Astérisque

MICHEL RAYNAUD
LUC ILLUSIE
J.-F. BOUTOT
H. CARAYOL
BAS EDIXHOVEN
SAN LING
JOSEPH OESTERLÉ
FRED DIAMOND
B. MAZUR
K. A. RIBET

Courbes modulaires et courbes de Shimura

Astérisque, tome 196-197 (1991)

<http://www.numdam.org/item?id=AST_1991__196-197__1_0>

196-197 ASTÉRISQUE

1991

COURBES MODULAIRES ET COURBES DE SHIMURA

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Classification AMS : M. Raynaud : 10D12, 14M40, 14K15, 14K30
L. Illusie : 14K30
J.-F. Boutot et H. Carayol : 10D45, 14L05
B. Edixhoven : 10D12, 10D23, 14H40, 14K15
S. Ling et J. Oesterlé : 10D12, 10D23, 14H40, 14K15
F. Diamond : 10D12, 10D23
B. Mazur et K. Ribet : 10D12, 10D23, 14H40, 14K15

Mots clefs : Courbes modulaires, courbes de Shimura, formes modulaires, représentations galoisiennes, jacobiennes, congruences, uniformisation *p*-adique.

Key-Words : Modular curves, modular forms, Shimura curves, Galois representations, Jacobians, congruences, p-adic uniformization.

Table des Matières

Introduction

Ce volume est issu d'un Séminaire intitulé *"Courbes modulaires, courbes de Shimura et représentations galoisiennes"*, organisé par K. Ribet et moi–même, en 1987–88, à l'Université de Paris–Sud (Orsay). Il s'agissait de comprendre les outils et résultats de l'article de K. Ribet [Ribet 1990a], alors sous forme de prépublication. Les orateurs furent H. Carayol, L. Illusie, R. Livne, J.–F. Mestre, J. Oesterlé, M. Raynaud, et les organisateurs. Les trois premiers articles de ce volume ont pour origine des conférences du Séminaire. Les autres articles offrent des résultats originaux obtenus depuis lors sur les thèmes abordés dans le Séminaire.

Pour décrire le fil conducteur et la teneur du présent volume, il nous faut brièvement décrire la substance de l'article cité. Il s'agit de la preuve, par B. Mazur et K. Ribet, du résultat suivant, conjecturé par Serre [Serre 1987]. On se donne un nombre premier ℓ impair et une $\overline{\mathbf{F}}_\ell$–représentation irréductible ρ de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, attachée à une forme modulaire parabolique de poids 2, primitive de niveau N et de caractère trivial, vecteur propre des opérateurs de Hecke. On considère un nombre premier p divisant N mais pas N/p. On suppose $p \not\equiv 1 \mod .\ell$ (Mazur) ou N non multiple de ℓ^2 (Ribet). On veut prouver que si ρ est **finie** en p (ce qui, si $p \neq \ell$, signifie que ρ est non ramifiée en p), alors ρ provient aussi d'une forme modulaire parabolique de poids 2, de caractère trivial et de niveau N/p.

Ce résultat a en particulier comme conséquence que la conjecture de Shimura–Taniyama–Weil, selon laquelle toute courbe elliptique sur $\mathbf{Q}$ est quotient d'une courbe modulaire $X_0(N)$, entraîne que l'équation de Fermat $X^n + Y^n = Z^n$ n'a pas de solutions en entiers X, Y, Z non nuls, pour $n \geq 3$ (voir [Frey 1987] et également, pour une introduction de nature élémentaire à ce cercle d'idées, l'article [Mazur 1991]).

Nous ne voulons pas commenter ici précisément la structure de la preuve. Celle–ci est décrite clairement dans l'introduction de [Ribet 1990a] et admirablement résumée dans l'exposé [Oesterlé 1988]. Nous n'en mentionnons ici que les aspects qui forment le fil conducteur du volume.

L'on procède en deux étapes. La première, due à Mazur, traite le cas où $p \not\equiv 1 \mod .\ell$. On note $T(N)$ l'algèbre des opérateurs de Hecke sur les formes paraboliques de poids 2 pour $\Gamma_0(N)$. On peut supposer que ρ est la (classe de) représentation attachée à un idéal maximal $\mathfrak{m}$ de $T(N)$, $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow GL_2(T(N)/\mathfrak{m})$, par les formules

$$tr\,\rho(\mathrm{Frob}_r) = T_r \mod .N$$

$$\det \rho(\mathrm{Frob}_r) = r \mod .N$$

pour tout nombre premier r ne divisant pas ℓN.

On regarde alors la représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur l'espace $J_0(N)[\mathfrak{m}]$ des points annulés par $\mathfrak{m}$ dans $J_0(N)(\overline{\mathbb{Q}})$, où $J_0(N)$ est la jacobienne de la courbe modulaire $X_0(N)$. On prouve facilement que cette représentation a une semisimplifiée isotypique de type ρ, mais on sait en outre maintenant qu'elle est semi–simple donc égale à sa semisimplifiée [Boston, Lenstra, Ribet 1991]. Prenons–en un composant simple V. Le point crucial est que V, puisque ρ est finie en p, se plonge dans la fibre en p du modèle de Néron de $J_0(N)$. Cela découle de la propriété universelle des modèles de Néron si $p \neq \ell$, puisqu'alors ρ est non ramifiée en p, et le lecteur trouvera à la fin de l'exposé de **Raynaud** la variante qui permet de traiter le cas $\ell = p$. Le même exposé donne la description du modèle de Néron sur $\mathbb{Z}_p$ de $J_0(N)$, avec son action de l'algèbre de Hecke. Un outil important est l'accouplement de monodromie, dont la réalisation ℓ-adique est détaillée dans le second exposé (**Illusie**), d'après Grothendieck. Le résultat de Mazur découle alors de l'action de Hecke sur la réduction modulo p de $J_0(N)$. En particulier, le module V a une image triviale dans le groupe Φ des composantes connexes de cette réduction, car l'action de Hecke sur ce groupe Φ est de type Eisenstein. L'article d'**Edixhoven** donne une démonstration de ce dernier fait pour $p|N$, $p > 3$ mais sans supposer que p^2 ne divise pas N ; la méthode est différente de celle de Mazur et Ribet. Dans un même ordre d'idées, l'article de **Ling** et **Oesterlé** décrit le sous–groupe de Shimura, noyau de l'homomorphisme $J_0(N) \longrightarrow J_1(N)$ (voir [Ribet 1983] pour le lien entre le groupe de Shimura et les applications $J_0(N) \longrightarrow J_0(Nq)$ où q est un nombre premier, $q \nmid N$).

La contribution de K. Ribet est le cas où $p \equiv 1 \mod .\ell$ et N premier à ℓ. Il commence par élever le niveau de la représentation ρ, c'est–à–dire prouver qu'il existe pour certains (nombreux) nombres premiers $q \not\equiv 1 \mod .\ell$, une forme parabolique de poids 2 pour $\Gamma_0(Nq)$, **nouvelle** en q, qui donne lieu à la représentation ρ (voir aussi [Ribet 1990b]). Dans le présent volume, la contribution de **F. Diamond** étend ce résultat aux formes de poids supérieur : il utilise la cohomologie des courbes modulaires plutôt que leur jacobienne.

Il s'agit alors de travailler avec la forme g obtenue, nouvelle à la fois en p et en q. Ribet introduit un corps de quaternions ramifié seulement en p et q et la courbe de Shimura C correspondant au niveau $M = N/p$. Cerednik et Drinfeld on décrit la fibre spéciale d'un modèle propre et plat de C sur $\mathbb{Z}_q$. C'est la méthode de Drinfeld pour établir ce résultat que vous trouverez exposée en détail (la rédaction de Drinfeld étant très elliptique) dans l'article de **Boutot** et **Carayol**. De cette description, Ribet déduit, et c'est là le point principal, que la composante neutre (du modèle de Néron) de la jacobienne de C, sur $\mathbb{F}_q$, est entièrement torique, un tore dont le groupe des caractères est isomorphe à celui de la partie q–nouvelle de la partie torique de $J_0(Mpq)$ sur $\mathbb{F}_p$. Noter l'échange de p et q qui est fondamental. Renvoyons à [Ribet

1990a] ou [Oesterlé 1989] pour les détails de l'ingénieux aller–retour vers C qui permet de conclure, mais mentionnons néanmoins qu'on ne peut conclure à la fin que parce qu'on a un résultat de multiplicité 1, à savoir que $J_0(Mpq)[\mathfrak{m}]$ est de dimension 2 sur $T(N)/\mathfrak{m}$. Dans la contribution de **Mazur** et **Ribet** ce résultat est généralisé au cas où l'on ne fait pas d'hypothèse sur la ramification de ρ en p, mais des exemples montrent qu'une restriction du genre $(p, M) = 1$ est nécessaire. Cette généralisation permet d'étendre le théorème de Ribet au cas où $p \equiv 1 \mod \ell$, $\ell | N$, $\ell^2 \nmid N$.

Mentionnons pour finir que c'est une version de ce théorème de multiplicité 1, utilisant la cohomologie cristalline, qui d'après l'annonce de [Jordan–Livne 1989] sert à obtenir la généralisation des résultats de Ribet aux poids supérieurs. Cependant l'usage du théorème de multiplicité 1 n'est pas toujours indispensable (cf. [Ribet 1991]) et on arrive à ramener le cas des formes de poids supérieurs à celui des formes de poids 2 (Ribet, courrier du 1er juillet 1991). Une autre généralisation consiste à examiner le cas où p^2 divise N : la conjecture de Serre correspondante est prouvée dans [Carayol 1989].

G. HENNIART

Bibliographie de l'introduction

[Boston–Lenstra–Ribet 1991] N. BOSTON, H. LENSTRA and K. RIBET. — *Quotients of group rings arising from two–dimensional representations*, C.R.A.S. Paris, t. 312, Série I, (1991), 323–328.

[Carayol 1989] H. CARAYOL. — *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. 59 (1989), 785–801.

[Frey 1987] *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. vol. 1, n° 1, 1986

[Jordan–Livne 1989] *Conjecture "epsilon" for weight $k > 2$*, B.A.M.S. 21 (1989), 51–56.

[Mazur 1991] *Number theory as gadfly*, Amer. Math. Monthly vol. 98 (1991), 593–610.

[Oesterlé 1988] *Nouvelles approches du théorème de Fermat*, Exposé n° 694 au Séminaire Bourbaki, Astérisque 161–162, (1988) 165–186.

[Ribet 1983] *Congruence relations between modular forms*, Pro-

ceeding ICM 83, Warsaw, t. 1, (1983), 503–514.

[Ribet 1990a] *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. 100 (1990), 431–476.

[Ribet 1990b] *Raising the levels of modular representations* in Séminaire de Théorie des Nombres de Paris, Progress in Math. 81 (1990), 259–271.

[Ribet 1991] *Lowering the levels of modular representations without multiplicity* 1, International Mathematics Research Notices (1991), 15–19.

[Serre 1987] *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. 54 (1987), 179–230.

1. Résumés des articles

M. Raynaud : *Jacobienne des courbes modulaires et opérateurs de Hecke*

Soit N un entier > 0. Nous considérons la courbe modulaire $X_0(N)_{\mathbb{Q}}$ de niveau N, définie sur $\mathbb{Q}$, et sa jacobienne $J_0(N)_{\mathbb{Q}}$. Il y a au moins deux façons naturelles d'étendre cette variété abélienne sur $\mathbb{Q}$ en un schéma en groupes sur $\mathbb{Z}$. On peut utiliser le modèle de Néron de $J_0(N)_{\mathbb{Q}}$ ou bien on peut d'abord, grâce à Drinfeld, étendre la courbe modulaire $X_0(N)_{\mathbb{Q}}$ en un modèle entier $X_0(N)$, puis introduire la jacobienne de ce modèle. Nous comparons ces deux schémas en groupes. En un nombre premier divisant exactement N le modèle de Néron a une réduction semi–stable et nous calculons le groupe des composantes connexes de sa fibre fermée. De plus, nous rappelons comment étendre les correspondances de Hecke de $\mathbb{Q}$ à $\mathbb{Z}_p$. Pour terminer, nous démontrons un analogue de la propriété universelle de Néron pour les schémas en groupes quasi–finis et plats, analogue qui est valable pour les schémas en groupes semi–abéliens, pourvu que la base ne soit pas trop ramifiée.

L. Illusie : *Réalisation ℓ–adique de l'accouplement de monodromie, d'après A. Grothendieck*

Pour une courbe propre et plate sur un trait strictement local, dont la fibre générale est lisse et les seules singularités de la fibre spéciale sont des points doubles ordinaires, on explicite, à l'aide de la formule de Picard–Lefschetz, la réalisation ℓ–adique ($\ell \neq$ caractéristique résiduelle) de l'accouplement de monodromie défini par Grothendieck dans (SGA 7 IX).

J.–F. Boutot et H. Carayol : *Uniformisation p–adique des courbes de Shimura : les théorèmes de Čerednik et Drinfeld*

Nous exposons, avec des démonstrations complètes et détaillées, la méthode de Drinfeld pour prouver les résultats de Čerednik sur l'uniformisation p–adique des courbes de Shimura. La construction, due à Drinfeld, d'une famille universelle de groupes formels sur le demi–plan analytique rigide est détaillée pour tout corps p–adique, et l'application globale au théorème de Čerednik est donnée pour les courbes de Shimura sur $\mathbb{Q}$.

B. Edixhoven : *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*

Pour un nombre entier $N \geq 1$, soit $X_0(N)_{\mathbb{Q}}$ la courbe modulaire sur $\mathbb{Q}$ paramétrant les N–isogénies cycliques entre courbes elliptiques, et $J_0(N)_{\mathbb{Q}}$ sa jacobienne. L'algèbre de Hecke agit sur $J_0(N)_{\mathbb{Q}}$ donc aussi sur son modèle de

Néron $J_0(N)$ sur $\mathbf{Z}$. Soit p un nombre premier et $\Phi_{N,p}$ le groupe de composantes connexes de la fibre géométrique $J_0(N)_p$ de $J_0(N)$ en caractéristique p. Nous démontrons que pour $p > 3$, l'action de l'algèbre de Hecke sur $\Phi_{N,p}$ est "Eisenstein".

S. Ling et J. Oesterlé : *The Shimura subgroup of* $J_0(N)$

Au morphisme naturel $X_1(N) \longrightarrow X_0(N)$ de courbes modulaires correspond par fonctorialité de Picard un homomorphisme $J_0(N) \longrightarrow J_1(N)$ entre leurs jacobiennes. Son noyau $\Sigma(N)$, appelé le sous—groupe de Shimura de $J_0(N)$, est fini. Nous déterminons la structure du groupe $\Sigma(N)$, ainsi que l'action sur ce groupe de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ et de l'algèbre de Hecke. Nous étudions également le comportement de ce groupe par les applications de dégénérescence. Cela généralise des travaux antérieurs de B. Mazur et K. Ribet.

F. Diamond : *Congruence primes for cusp forms of weight* $k \geq 2$

Soit f une forme primitive de conducteur N, et soit ℓ un nombre premier ne divisant pas N. On considère les nombres premiers de congruence entre f et des formes primitives de conducteur divisant $N\ell$ et divisible par ℓ. Pour les formes de poids 2, Ribet a calculé ces nombres premiers de congruence en étudiant certains sous–groupes des jacobiennes des courbes modulaires. En considérant, au lieu de jacobiennes, des groupes de cohomologie à coefficients dans des représentations tensorielles symétriques, on peut généraliser ses résultats aux poids plus grands.

B. Mazur et K.A. Ribet : *Two–dimensional representations in the arithmetic of modular curves*

Soit p un nombre premier et N un entier ≥ 1 premier à p. Soit f une forme nouvelle de poids 2 pour $\Gamma_0(Np)$, et soit ρ la représentation modulo p de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ attachée à f. Nous prouvons que si ρ est absolument irréductible, et n'est pas de niveau N, alors ρ intervient avec multiplicité 1 dans l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur les points d'ordre p de la jacobienne de $X_0(Np)$. Nous donnons des exemples montrant que ce résultat ne s'étend pas au cas où l'on remplace Np par Np^r, $r \geq 3$.

2. Résumés en anglais. English abstracts

M. Raynaud : *Jacobienne des courbes modulaires et opérateurs de Hecke*

Let N be a strictly positive integer. We consider the modular curve $X_0(N)_{\mathbb{Q}}$ of level N, defined over $\mathbb{Q}$ and its Jacobian $J_0(N)_{\mathbb{Q}}$. There are at least two natural ways to extend this $\mathbb{Q}$-abelian variety into a group-scheme over $\mathbb{Z}$. We can use the Néron model of $J_0(N)_{\mathbb{Q}}$ or we can first extend the modular curve $X_0(N)_{\mathbb{Q}}$ into an integral model $X_0(N)$, thanks to Drinfeld, and then introduce its Jacobian. We compare those two group-schemes. At a prime p such that $p\|N$, the Néron model has semi-abelian reduction and we compute the group of connected components of the closed fiber. Further we recall how to extend the Hecke correspondences from $\mathbb{Q}$ to $\mathbb{Z}_p$.

We end this lecture by an analogue of the Néron universal property for quasi-finite flat group-schemes, which is valid for semi-abelian group-schemes, when the base is not too ramified.

L. Illusie : *Réalisation ℓ-adique de l'accouplement de monodromie, d'après A. Grothendieck*

For a proper and flat curve over a strictly local discrete valuation ring, whose general fiber is smooth and whose special fiber has only ordinary double points as singularities, we describe, by means of the Picard–Lefschetz formula, the ℓ-adic realization ($\ell \neq$ residual characteristic) of the monodromy pairing defined by Grothendieck in (SGA 7 IX).

J.-F. Boutot et H. Carayol : *Uniformisation p-adique des courbes de Shimura : les théorèmes de Čerednik et Drinfeld*

We expound, with complete and detailed proofs, Drinfeld's method for proving results of Čerednik's on the p-adic uniformization of Shimura curves. Drinfeld's construction of a universal family of formal groups on the rigid analytic half-plane is detailed over any p-adic field, whereas the global application to Čerednik's theorem is given for Shimura curves over $\mathbb{Q}$.

B. Edixhoven : *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein".*

Let N be a positive integer and $X_0(N)_{\mathbb{Q}}$ the modular curve over $\mathbb{Q}$ parameterizing cyclic isogenies of degree N between elliptic curves. Let $J_0(N)_{\mathbb{Q}}$ be the Jacobian variety of $X_0(N)_{\mathbb{Q}}$. The Hecke algebra acts on $J_0(N)_{\mathbb{Q}}$ hence also on its Néron model $J_0(N)$ over $\mathbb{Z}$. Let p be a prime number and $\Phi_{N,p}$ the group of connected components of the geometric fiber $J_0(N)_p$

of $J_0(N)$ in characteristic p. We prove that for $p > 3$ the action of the Hecke algebra on $\Phi_{N,p}$ is "Eisenstein".

S. Ling et J. Oesterlé : *The Shimura subgroup of $J_0(N)$*

To the natural morphism $X_1(N) \longrightarrow X_0(N)$ of modular curves corresponds, by Picard functoriality, a morphism $J_0(N) \longrightarrow J_1(N)$ between their Jacobian varieties. Its kernel $\Sigma(N)$, called the Shimura subgroup of $J_0(N)$, is finite. We determine the group structure of $\Sigma(N)$ together with the action of Galois and the action of the Hecke algebra. This extends previous results obtained by B. Mazur and K. Ribet.

F. Diamond : *Congruence primes for cusp forms of weight $k \geq 2$*

Let f be a primitive newform of conductor N, and let ℓ be a prime number not dividing N. We consider congruence primes between f and newforms of level dividing $N\ell$ and divisible by ℓ. For weight 2 forms, Ribet computed those congruence primes by studying some subgroups of the Jacobian varieties of modular curves. Considering, instead of Jacobian varieties, cohomology groups with coefficients in symmetric power representations, we generalize his results to higher weights.

B. Mazur et K.A. Ribet : *Two-dimensional representations in the arithmetic of modular curves*

Let p be a prime number and N a positive integer prime to p. Let f be a new form of weight for $\Gamma_0(Np)$ and ρ the mod p representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ attached to f. We prove that if ρ is absolutely irreducible and is not of level N, then ρ occurs with multiplicity 1 in the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on points of order p of the Jacobian of $X_0(Np)$. We give examples showing that this does not extend to the case where Np is replaced by Np^r, $r \geq 3$.

Jacobienne des courbes modulaires et opérateurs de Hecke

Michel RAYNAUD (*)

ABSTRACT. Let N be a strictly positive integer. We consider the modular curve $X_0(N)_{\mathbb{Q}}$ of level N, defined over $\mathbb{Q}$ and its jacobian $J_0(N)_{\mathbb{Q}}$. There are at least two natural ways to extend this $\mathbb{Q}$-abelian variety into a group-scheme over $\mathbb{Z}$. We can use the Néron model of $J_0(N)_{\mathbb{Q}}$ or we can first extend the modular curve $X_0(N)_{\mathbb{Q}}$ into an integral model $X_0(N)$, thanks to Drinfeld, and then introduce its jacobian. We compare those two group-schemes. At a prime p such that $p\|N$, the Néron model has semi-abelian reduction and we compute the group of connected components of the closed fiber. Further we recall how to extend the Hecke correspondances from $\mathbb{Q}$ tout $\mathbb{Z}_p$.

We end this lecture by an analogue of the Néron universal property for quasi-finite flat group-schemes, which is valid for semi-abelian group-schemes, when the base is not too ramified.

Modèle de Néron de $J_0(N)_{\mathbb{Q}}$ et schéma de Picard de $X_0(N)$

Soient N un entier > 0.

Considérons la courbe modulaire $X_0(N)_{\mathbb{Q}}$. C'est le *"module grossier"* compactifié, associé au champ des couples (E, C_N) formés d'une courbe elliptique E et d'un sous-schéma en groupes étale C_N de E, cyclique d'ordre N. Alors $X_0(N)_{\mathbb{Q}}$ est une courbe propre et lisse sur $\mathbb{Q}$, géométriquement connexe. On note $J_0(N)_{\mathbb{Q}}$ sa jacobienne, qui est donc une variété abélienne sur $\mathbb{Q}$.

Comment prolonger $J_0(N)_{\mathbb{Q}}$ en un schéma en groupes sur $\mathbb{Z}$?

Une première méthode consiste à considérer le **modèle de Néron** $J_0(N)$ sur $\mathbb{Z}$ de $J_0(N)_{\mathbb{Q}}$. Alors $J_0(N)$ est un schéma en groupes lissé et séparé sur $\mathbb{Z}$, de fibre générique $J_0(N)_{\mathbb{Q}}$ et c'est le **"meilleur"** possible dans le sens, où tout autre prolongement lisse s'envoie dans $J_0(N)$. Cette approche présente un inconvénient : il n'est pas évident d'interpréter la réduction de $J_0(N)$ en un nombre premier p, en particulier lorsque p divise le conducteur N.

Une autre méthode consiste à introduire d'abord le modèle $X_0(N)$ de $X_0(N)_{\mathbb{Q}}$ sur $\mathbb{Z}$ que l'on obtient comme suit :

On part de $X_0(1)$ défini comme la droite projective sur $\mathbb{Z}$, complétée de la droite affine ayant pour coordonnée l'invariant j. On dispose du morphisme fini canonique

$$X_0(N)_{\mathbb{Q}} \longrightarrow X_0(1)_{\mathbb{Q}},$$

(*) Unité Associée au CNRS URA D0752

qui, au niveau des champs, consiste à oublier la structure de niveau C_N, et on définit $X_0(N)$ comme étant la normalisée de $X_0(1)$ dans $X_0(N)_{\mathbb{Q}}$. Par construction $X_0(N)$ est donc une courbe relative sur $\mathbb{Z}$, propre et normale, finie sur $X_0(1)$.

On note d'abord que $X_0(N)$ est **lisse** au-dessus de l'ouvert de $\mathbb{Z}$ où le conducteur N **est inversible** comme module grossier associé au champ lisse compactifié des couples (E, C_N) comme plus haut (on doit vérifier la lissité à l'infini par une étude locale, cf. [12] Appendice).

Soit maintenant p un nombre premier qui **divise strictement** N et $N' = N/p$. Deligne et Rapoport ([3] cf. th. 6.9) ont montré que au voisinage de p, $X_0(N)$ est le module grossier compactifié associé au champ (E, C_N), où $C_N = C_p C_{N'}$ avec C_p un sous-schéma en groupes de E, fini et plat, de rang p. La fibre au-dessus de p de $X_0(N)$ est constituée de deux copies de $X_0(N')_{\mathbb{F}_p}$ (donc géométriquement irréductibles) qui se coupent transversalement aux points supersinguliers. En particulier la réduction de $X_0(N)$ en p est semi-stable.

Lorsque $p^2|N$, la fibre en p de $X_0(N)$ est plus compliquée, et certaines composantes irréductibles apparaissent avec des multiplicités > 1. Ce n'est que grâce à l'interprétation modulaire donnée par Drinfeld et étudiée dans [7] que l'on a pu obtenir un certain contrôle sur $X_0(N)$. En effet, $X_0(N)$ peut encore être défini comme le module grossier compactifié associé au champ des couples (E, C_N) où C_N est un sous-schéma en groupes cyclique d'ordre N du schéma elliptique E, mais toute la subtilité est cachée dans la définition de cyclique. Dire que C_N est cyclique d'ordre N signifie maintenant que, localement pour la topologie plate, il existe une section P de E, telle que C_N soit un sous-schéma en groupes de E, ayant pour schéma sous-jacent le diviseur $[P] + [2P] + \cdots + [NP]$. Une propriété fondamentale de ce champ est d'être **régulier** sur $\mathbb{Z}$ ([7] chap. 5). Cela se traduit de la façon suivante : partons d'un point fermé x de $X_0(N)$, de corps résiduel k_x au-dessus de $\mathbb{F}_p$. Il lui correspond une courbe elliptique (du moins à distance finie) E_x sur k_x et une structure cyclique de Drinfeld $C_{N,x}$. Alors l'anneau R de la déformation verselle du champ de Drinfeld au voisinage de $(E_x, C_{N,x})$ est un anneau régulier complet, de dimension 2, plat sur $\mathbb{Z}$. De plus on obtient le complété $\widehat{O}_{X,x}$ de l'anneau local de $X_0(N)$ en x en passant au quotient par le groupe fini G des automorphismes exceptionnels de $(E_x, C_{N,x})$. Le groupe G est, comme d'habitude, d'ordre divisant 12.

Ceci étant, à la courbe $X_0(N)$, on peut associer un foncteur en groupes sur $\mathbb{Z}$, le foncteur de Picard relatif de $X_0(N)$ sur $\mathbb{Z}$ ([4] et aussi [1] chap. 8) :

$$P = \mathrm{Pic}_{X_0(N)/\mathbb{Z}}$$

dont la formation à l'avantage sur le modèle de Néron, de commuter au

passage aux fibres. Pour tout corps premier $\mathbf{k}$, on a donc :

$$P_{\mathbf{k}} = \mathrm{Pic}_{X_0(N)_k/k}$$

THÉORÈME 1. — *Le foncteur de Picard P est représentable par un schéma en groupes lisse sur $\mathbf{Z}$ (non nécessairement séparé).*

Notons d'abord que P est formellement lisse sur $\mathbf{Z}$ car, sur une courbe relative, il n'y a pas d'obstruction infinitésimale à relever un faisceau inversible en raison de la nullité du H^2 d'un faisceau cohérent. On dispose alors d'un sous-foncteur ouvert P^0 de P : la composante neutre, qui est associée au foncteur des faisceaux inversibles sur $X_0(N)$ de degré nul sur toutes les composantes irréductibles des fibres ([1] chap. 9.2 Cor. 13) et P^0 a ses fibres connexes.

La difficulté du théorème ci-dessus dépend de la complexité des singularités des fibres de $X_0(N)/\mathbf{Z}$:

— Là où N est inversible, $X_0(N)$ est une courbe projective et lisse et on peut invoquer Grothendieck ([4] th. 3.1)..

— Au voisinage d'un nombre premier p qui divise strictement le conducteur N, (i.e. p^2 ne divise pas N) les fibres de $X_0(N)$ sont géométriquement réduites et les composantes irréductibles sont géométriquement irréductibles. la représentabilité résulte alors d'un résultat non publié de Mumford. On peut aussi invoquer Deligne ([2] chap. V Prop. 4.3). Une autre méthode consiste à adapter la construction de Weil des jacobiennes, étendue par Rosenlicht et Serre aux jacobiennes généralisées ([12] chap. V). Pour plus de détails, on pourra consulter ([1] chap. 9.3).

— Lorsque p^2 divise le conducteur N, la fibre en p n'est plus réduite. Toutefois certaines composantes sont encore (géométriquement) réduites ([7] p. 417) : celles qui correspondent à une structure de niveau cyclique C_N de degré N qui est soit de type multiplicatif, soit étale (composantes contenant la pointe 0 ou ∞). Ce fait joint à la normalité de $X_0(N)$ assurent la représentabilité de P^0 par un schéma en groupes lisse et séparé ([1] chap. 9.4 th. 2). Comme par ailleurs les composantes irréductibles de $X_0(N)_{\mathbb{F}_p}$ sont géométriquement irréductibles (si $N = p^m N'$, avec $(p, N') = 1$, chaque composante irréductible de $X_0(N)_{\mathbb{F}_p}$ se projette homéomorphiquement sur $X_0(N')_{\mathbb{F}_p}$ (cf. [7] prop. 13.4.5), P est recouvert par des ouverts qui sont des torseurs étales sous P^0 et ceux-ci sont représentables comme on le voit par descente ([1] chap. 6.5 th. 1).

Comparaison de P et de $J_0(N)$

On dispose d'un morphisme de groupes naturel $P \longrightarrow \mathbb{Z}$, donné par le degré total des faisceaux inversibles. Soit $\widetilde{P}$ son noyau qui est un sous-schéma en groupes ouvert et fermé de P, contenant P^0. Alors $\widetilde{P}$ est un prolongement sur $\mathbb{Z}$ de la jacobienne $J_0(N)_{\mathbb{Q}}$.

D'après la propriété universelle des modèles de Néron, on a donc un morphisme de groupes canonique :

$$c : \widetilde{P} \longrightarrow J_0(N)$$

qui prolonge l'isomorphisme naturel sur la fibre générique.

THÉORÈME 2. — *Le morphisme c induit un isomorphisme sur les composantes neutres, au voisinage de p, dans les cas suivants :*

i) p^2 ne divise pas N.

ii) $p \geq 5$.

iii) En tout point fermé x de $X_0(N)_{\mathbb{F}_p}$, le groupe G des automorphismes exceptionnels considéré plus haut est d'ordre premier à p.

Démonstration : Si p^2 ne divise pas N, on verra plus loin que $P^0_{\mathbb{F}_p}$ est semi-abélien. L'assertion i) résulte alors du lemme suivant :

LEMME 3. — *Soit R un anneau de valuation discrète, de corps des fractions K, de corps résiduel k et soit A_K une K-variété abélienne, qui se prolonge en un R-schéma en groupes semi-abélien B. Alors B^0 est la composante neutre du R-modèle de Néron A de A_K.*

Considérons le morphisme canonique $c : B^0 \longrightarrow A^0$ et montrons que c'est un isomorphisme.

On peut supposer R strictement hensélien. Soit n entier premier à la caractéristique résiduelle p. Le noyau ${}_nB^0$ (resp. ${}_nA^0$) de la multiplication par n dans B^0 (resp. A^0) est étale sur R et par suite $c|_nB^0$ est injectif. Considérons alors $H = \mathrm{Ker}(c)$. Vu ce qui précède H_k ne contient pas de points d'ordre n non nuls avec $(n,p) = 1$. Comme B^0_k est semi-abélien, donc extension d'une variété abélienne par un tore, il en est de même de tout sous-groupe lisse connexe et les points de torsion d'ordre premier à p, d'un tel groupe sont schématiquement denses. On en déduit que H_k est fini et donc c est quasi-fini. On conclut par le Main theorem de Zariski, que c'est une immersion ouverte.

Vu ce qui a été rappelé sur G, ii) est un cas particulier de iii). D'autre part, il est démontré dans ([1] chap. 9.7) que c induit un isomorphisme sur les composantes neutres lorsque les singularités de $X_0(N)$ sont rationnelles. Pour étudier la rationalité de la singularité de $X_0(N)$ en un point

fermé x, on peut remplacer l'anneau local O_x par son complété $\widehat{O}_x$ qui est donc un quotient d'un anneau régulier $\widehat{O}_y$ par un groupe fini G. Soit $f : X' \longrightarrow \mathrm{Spec}(\widehat{O}_x)$ une désingularisation de $\widehat{O}_x$ et soit Y' le normalisé de $X' \times_{\mathrm{Spec}(\widehat{O}_x)} \mathrm{Spec}(\widehat{O}_y)$ $g : Y' \longrightarrow \mathrm{Spec}(\widehat{O}_y)$ la projection canonique. Notons π le morphisme fini naturel $Y' \longrightarrow X'$. Comme $\widehat{O}_y$ est régulier, on a $H^1(Y', O_{Y'}) = 0$, comme on le voit en dominant Y' par Y'' déduit de $\mathrm{Spec}(\widehat{O}_y)$ par une suite d'éclatements de points fermés. Lorsque le groupe G est d'ordre premier à p, le morphisme trace réalise $O_{X'}$ comme facteur direct de $\pi_*(O_{Y'})$. A fortiori $H^1(X', O_{X'}) = 0$ et donc $\widehat{O}_x$ a une singularité rationnelle.

Remarque : en caractéristique 2 et 3, j'ignore si c est un isomorphisme en restriction aux composantes neutres. Si ce n'était pas le cas, cela laisserait mal augurer du contrôle des quotients elliptiques de $J_0(N)$ et donc de la conjecture de Manin [9].

Dans la suite on considère un nombre premier p qui divise strictement le conducteur N. On note simplement k le corps premier $\mathbb{F}_p$, R le localisé de $\mathbb{Z}$ en p, $K = \mathbb{Q}$ le corps des fractions de R, $\pi = p$ une uniformisante de R, X la courbe modulaire $X_0(N)_R$, X_0 et X_∞ les deux composantes irréductibles de X_k, de jacobiennes respectives J_0 et J_∞, x_i, $i \in I$, les points communs aux deux composantes, k_i le corps résiduel en x_i.

Commençons par déterminer la jacobienne J_k de X_k. La normalisée $\widetilde{X}_k$ de X_k est la somme disjointe $X_0 \coprod X_\infty$ et a pour jacobienne $J_0 \underset{k}{\times} J_\infty$. Notons $x_{i,0}$(resp. $x_{i,\infty}$) le point de $\widetilde{X}_k$ au-dessus de x_i, situé sur la composante X_0 (resp. X_∞). On a une suite exacte de faisceaux d'unités :

$$(*) \qquad 0 \longrightarrow \mathcal{O}^*_{X_k} \longrightarrow \mathcal{O}^*_{\widetilde{X}_k} \longrightarrow \mathcal{U} \longrightarrow 0,$$

où $\mathcal{U}$ est concentré en les points x_i, $i \in I$. Plus précisément la fibre de $\mathcal{U}$ en x_i s'insère dans la suite exacte :

$$0 \longrightarrow k_i^* \longrightarrow k_{i,0}^* \times k_{i,\infty}^* \longrightarrow \mathcal{U}(x_i) \longrightarrow 0.$$

Ainsi le choix d'une composante, par exemple X_0, permet d'identifier $\mathcal{U}(x_i)$ à k_i^*, via la première projection $k_{i,0}^* \times k_{i,\infty}^* \longrightarrow \mathcal{U}(x_i)$.

De la suite exacte (*), on déduit la suite exacte de cohomologie :

$$0 \longrightarrow k^* \longrightarrow k_0^* \times k_\infty^* \longrightarrow \Pi_i \mathcal{U}(x_i) \longrightarrow \mathrm{Pic}(X_k) \longrightarrow \mathrm{Pic}(\widetilde{X}_k) \longrightarrow 0.$$

Par restriction aux faisceaux de degré 0, on obtient la suite exacte :

$$0 \longrightarrow k^* \longrightarrow k_0^* \times k_\infty^* \longrightarrow \Pi_i \mathcal{U}(x_i) \longrightarrow J_k(k) \longrightarrow (J_0 \times J_\infty)(k) \longrightarrow 0.$$

On en déduit que J_k est extension de la variété abélienne $J_0 \times J_\infty$ par un tore T qui s'insère dans la suite exacte :

$$(**) \qquad 0 \longrightarrow k^* \longrightarrow k_0^* \times k_\infty^* \longrightarrow \Pi_i \mathcal{U}(x_i) \longrightarrow T(k) \longrightarrow 0.$$

Comme plus haut, le choix d'une des composantes de X_k détermine un isomorphisme :

$$T(k) \approx \Pi_i k_i^*/k^*,$$

k^* étant plongé diagonalement dans $\Pi_i k_i^*$.

Autrement dit, si T_i désigne le tore restriction de Weil de $\mathbb{G}_m$ de k_i à k, le choix d'une composante de X_k fournit un isomorphisme canonique :

$$T \approx (\Pi_i T_i)/\mathbb{G}_m.$$

Remarque : les corps résiduels des points supersinguliers de X sur le corps premiers $\mathbb{F}_p$ sont au pire des extensions quadratiques de $\mathbb{F}_p$ (cf. [7] 12.5.4).

Pour décrire T, on peut aussi passer à une clôture algébrique $\overline{k}$ de k. Le groupe de Galois $\mathfrak{G} = \mathrm{Gal}(\overline{k}/k)$ opère sur l'ensemble $\overline{x}_j$, $j \in J$, des points doubles de $X_{\overline{k}}$. Pour tout $j \in J$, considérons le groupe libre $\mathbb{Z}\overline{x}_{j,0} \oplus \mathbb{Z}\overline{x}_{j,\infty}$ et soit $\mathbb{Z}_j$ le noyau de l'augmentation :

$$(a_{j,0}, a_{j,\infty}) \longrightarrow a_{j,0} + a_{j,\infty}.$$

Il résulte alors de la suite exacte (**) que le groupe M des caractères du tore T est canoniquement isomorphe (avec l'action de Galois), au sous-groupe de $\oplus \mathbb{Z}_j$, noyau de l'augmentation $\sum_j a_{j,0}$.

Le choix d'une composante (par exemple X_0) fournit un isomorphisme canonique entre M et le groupe D_0 formé des diviseurs de X_0 à support dans la réunion des $\overline{x}_{j,0}$ et de degré nul. On a de même un isomorphisme entre M et D_∞. L'isomorphisme composé $D_0 \longrightarrow D_\infty$ est induit par l'application $\overline{x}_{j,0} \longrightarrow -\overline{x}_{j,\infty} \forall j \in J$.

Pour décrire complètement la jacobienne de X_k, on devrait encore décrire l'extension de $J_0 \times J_\infty$ par T. Identifions comme d'habitude J_0 et J_∞ à leur variété duale. Une extension de $J_0 \times J_\infty$ par T est alors décrite par des morphismes $j_0 : M \longrightarrow J_0$ et $j_\infty : M \longrightarrow J_\infty$. Ceux-ci devraient s'obtenir en composant l'isomorphisme $M \approx D_0$ avec l'application canonique $D_0 \longrightarrow J_0(k)$ et de même avec la composante ∞, mais je ne l'ai pas vérifié.

Reprenons le morphisme canonique $c : \widetilde{P} \longrightarrow J = J_0(N)$, provenant de la propriété universelle des modèles de Néron. Nous avons vu que c induit un isomorphisme sur les composantes neutres. Soit $\{0\}$ l'adhérence

schématique dans $\widetilde{P}$ de la section unité. C'est un sous-schéma en groupes étale de $\widetilde{P}$ qui rencontre P^0 suivant la section unité, et qui mesure le défaut de séparation de $\widetilde{P}$. On en déduit immédiatement la représentabilité du quotient $J' = \widetilde{P}/\{\widetilde{0}\}$ et le fait que c se factorise à travers J' et une immersion ouverte $c' : J' \longrightarrow J$.

Notons Φ le groupe des composantes connexes de la fibre J_k et Φ' celui de J'_k. On a donc une injection $\Phi' \longrightarrow \Phi$, **qui, en général, n'est pas un isomorphisme.**

Pour mesurer le défaut de surjectivité, on peut remplacer R par un hensélisé strict. D'après la propriété universelle du modèle de Néron J, l'application canonique :

$$J(R) \longrightarrow J(K)$$

est une bijection. Par ailleurs on a évidemment une bijection $\widetilde{P}(K) \approx J'(K) \approx J(K)$. Le noyau de $\widetilde{P} \longrightarrow J'$ est un R-schéma en groupes étale et comme R est strictement hensélien, tout R-torseur sous ce groupe est trivial. Il en résulte que $\widetilde{P}(R) \longrightarrow J'(R)$ est surjectif. Le défaut de surjectivité de c' provient donc d'un défaut de surjectivité de $\widetilde{P}(R) \longrightarrow \widetilde{P}(K)$. Comme X possède une section (par exemple la pointe ∞) et que les sections globales de O_X sont les constantes, un élément de $\widetilde{P}(R)$ (resp. $\widetilde{P}(K)$) correspond à un faisceau inversible L sur X de degré total zéro (resp. L_K sur X_K de degré 0)) ([4] corollaire 2.4). Un tel faisceau inversible L_K sur X_K ne se prolonge pas nécessairement en un faisceau inversible L sur X, car X n'est pas nécessairement régulier aux points doubles de la fibre spéciale X_k.

Plus précisément, en un point double ordinaire x de la fibre spéciale X_k, à extension résiduelle triviale, l'hensélisé de $O_{X,x}$ est isomorphe à l'hensélisé de l'anneau $R[[x,y]]/xy - \pi^e$ et son complété est isomorphe à $R[[x,y]]/xy - \pi^e$ où e est un entier ≥ 1 bien déterminé : "l'épaisseur" de la singularité. Ce complété est aussi l'anneau des séries de Laurent $\sum_{-\infty}^{+\infty} a_i T^i$, $a_i \in K$, qui convergent dans la couronne $0 < v(T) < e$ et sont de valuation ≥ 0. La correspondance entre ces deux réalisations envoie par exemple x sur T et y sur π^e/T.

L'anneau des séries de Laurent, après tensorisation par K est principal ; par contre l'anneau $R[[x,y]]/(xy-\pi^e)$ a ses deux branches mod. π qui sont des diviseurs de Weil exactement d'ordre e. Ce n'est que lorsque $e = 1$ que l'anneau local est régulier, donc factoriel. Par descente fidèlement plate, on en conclut que le groupe de Picard local de $O_{X,x}$ est cyclique d'ordre e.

Dans le cas de la courbe modulaire X et après hensélisation stricte de R, l'anneau local $O_{X,x}$ en un point double x est le quotient par le

groupe G des automorphismes exceptionnels du modèle de Drinfeld qui lui est régulier et donc correspond à une épaisseur $e = 1$. Un argument de norme montre alors que l'épaisseur de la singularité en x n'est autre que le cardinal de G (cf. [12] Appendice).

PROPOSITION 4. — *Supposons R strictement hensélien. Soit $\overline{x}_j$, $j \in J$, la famille des points doubles de $X_{\overline{k}}$ et e_j l'épaisseur de la singularité de X en $\overline{x}_j$. Notons e le ppcm des e_j, $i \in I$.*

1) Le groupe Φ/Φ' est annulé par e.

2) Le groupe Φ' est cyclique d'ordre $e(\sum_j 1/e_j)$.

L'assertion 1) résulte du fait que pour tout diviseur ≥ 0 D_K sur X_K, eD_K a une adhérence schématique dans X qui est un diviseur de Cartier, comme il résulte des remarques précédentes.

Prouvons 2). Les composantes X_0 et X_∞ de X_k sont des diviseurs de Weil de X ; eX_0 et eX_∞ sont des diviseurs de Cartier ; enfin $eX_0 \equiv -eX_\infty$ car $X_0 + X_\infty = (\pi)$. Parodiant la construction de Mumford, ([10]), il est commode d'introduire des multiplicités d'intersections locales fractionnaires entre diviseurs de Weil en posant :

$$(X_0 \cdot X_\infty)_{\bar{x}_j} = (1/e_j)(e_j X_0 \cdot X_\infty)_{\bar{x}_j}.$$

Dans l'anneau $R[[u,v]]/(uv - \pi^{e_j})$, $(e_j X_0 \cdot X_\infty)_{\bar{x}_j}$ est la multiplicité d'intersection du diviseur de Cartier $e_j X_0$ d'équation disons $u = 0$, avec le cycle X_∞ d'équations $v = \pi = 0$. Cette multiplicité d'intersection vaut donc 1. D'où $(X_0 \cdot X_\infty)_{\bar{x}_j} = 1/e_j$. On en déduit $(X_0 \cdot X_\infty) = \sum_j 1/e_j$.

Ceci étant, le groupe des composantes connexes de la fibre spéciale de P est isomorphe à $\mathbb{Z}^2$, formé des couples (a_0, a_∞) d'entiers correspondant aux degrés des faisceaux inversibles sur les composantes X_0 et X_∞. Le sous-groupe des composantes de $\widetilde{P}_k$ est isomorphe à $\mathbb{Z}$ et correspond aux couples vérifiant $a_0 + a_\infty = 0$. L'adhérence schématique dans $\widetilde{P}$ de $\{0\}$ correspond aux diviseurs de Cartier verticaux. Elle est formée des multiples de eX_0, dont le degré d'intersection avec X_∞ est $e(\sum_j 1/e_j)$, d'où le résultat.

Remarque : Sur le corps premier $\mathbb{F}_p$, l'action de Galois sur Φ' est triviale, car l'action de Galois sur $\widetilde{P}/P^0$ est triviale, les composantes X_0 et X_∞ étant géométriquement irréductibles.

Structure de Φ

Soient $\overline{x}_j, j \in J$ les points doubles de $X_{\overline{k}}$, où $\overline{k}$ est une clôture algébrique de k. Considérons le groupe $\oplus_j \mathbb{Z}\overline{x}_j$ avec son action naturelle de Galois. Le noyau de l'augmentation canonique $b : \oplus_j \mathbb{Z}\overline{x}_j \longrightarrow \mathbb{Z}$ s'identifie au groupe

M des caractères du tore T, une fois choisie l'une des deux composantes X_0 ou X_∞.

Définissons un produit scalaire sur $\oplus_j \mathbb{Z}\overline{x}_j$ en posant

$$< \overline{x}_j, \overline{x}_{j'} >= \delta_{j,j'} e_j,$$

où e_j est l'épaisseur de la singularité de X en $\overline{x}_j$ et $\delta_{j,j'}$ le symbole de Kronecker. Notons que ce produit scalaire ne dépend pas du choix d'une composante.

Par restriction, on en déduit un produit scalaire sur M, d'où une inclusion naturelle compatible avec les actions naturelles de Galois :

$$M \longrightarrow M^* = \mathrm{Hom}(M, \mathbb{Z}).$$

THÉORÈME 5. — *Le groupe Φ, avec son action de Galois, est isomorphe au groupe quotient M^*/M.*

Ce théorème est énoncé dans SGA 7 I chap. IX et repose sur plusieurs étapes.

— Soit A_K une K-variété abélienne, à réduction semi-stable sur R. Notons A son R-modèle de Néron, et M le groupe des caractères du tore maximal de la fibre spéciale. Considérons la variété abélienne duale A'_K de A_K, son R-modèle de Néron A', le groupe M' des caractères du tore de la fibre spéciale.

— Grothendieck définit un accouplement canonique de monodromie $M \times M' \longrightarrow \mathbb{Z}$ (cf. th. 10.4), non dégénéré, et le groupe des composantes connexes de A_k est canoniquement isomorphe au conoyau $\mathrm{Hom}(M, \mathbb{Z})/M'$ (th. 11.5).

— Le choix d'une polarisation principale de A_K ramène cet accouplement à la donnée d'une forme quadratique sur M, d'ailleurs positive non dégénérée, et Φ se décrit comme le quotient M/M^* avec $M^* = \mathrm{Hom}(M, \mathbb{Z})$.

Si de plus, A_K est la jacobienne canoniquement principalement polarisée de la fibre générique X_K d'une courbe X semi-stable sur R, la forme quadratique est celle induite par le produit scalaire décrit plus haut (th. 12.5).

Ces diverses assertions conduisent au th. 5.

Ceci étant, le plan suivi par Grothendieck est plus imbriqué. L'accouplement de monodromie n'est pas directement défini au niveau des entiers, mais d'abord au niveau ℓ-adique (ℓ premier, distinct de p) par voie cohomologique. Quant au calcul de la monodromie dans le cas d'une courbe semi-stable, il se déduit de la formule de Picard-Lefschetz (chap. XV). Comme l'application précise que Grothendieck avait en vue ne figure pas explicitement dans l'exposé de Deligne, le détail de la démonstration est présenté ici dans l'exposé d'Illusie.

COROLLAIRE 6. — *Soit n le cardinal de l'ensemble J des points singuliers de X_k. Pour toute partie H de l'ensemble J, posons $e_H = \Pi_{h\in H} e_h$.*
Alors le groupe $\Phi(\bar{k})$ est isomorphe au groupe :

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_{n-2}\mathbb{Z} \oplus \mathbb{Z}/d_{n-1}\mathbb{Z}.$$

Avec $d_m = pgcd(e_H)$, pour $H \subset J$, card $H = m$, ceci pour $m = 1, \cdots, n-2$ et

$$d_{n-1} = \sum_{H\subset J, \mathrm{card}(H)=n-1} e_H.$$

Démonstration : Les éléments $a_i = x_1 - x_i$, $i = 2, \cdots, n$ forment une base de M. La matrice $< a_i, a_j >$ prend la forme :

$$\begin{pmatrix} e_1+e_2 & e_1 & \cdots & e_1 \\ e_1 & e_1+e_3 & \cdots & e_1 \\ & & & \\ e_1 & & \cdots & e_1+e_n \end{pmatrix}$$

On obtient alors la structure de Φ à l'aide des facteurs invariants de cette matrice (cf. [1] chap. 9.6, Prop. 10 pour une autre démonstration combinatoire). On trouvera également un calcul de Φ dû à Rapoport et Mazur pour $N = p$ dans ([8], Appendix).

Par exemple lorsque X est régulier, on a $\Phi = \Phi' = \mathbb{Z}/n\mathbb{Z}$.

Opérateurs de Hecke

Soit ℓ un nombre premier tel que $(\ell, N) = 1$. Nous allons définir une correspondance T_ℓ sur la courbe $X_0(N)$, puis lui associer un endomorphisme, noté encore T_ℓ, de $J_0(N)$. En fait nous allons simplement prolonger la correspondance de Hecke de $X_0(N)_{\mathbb{Q}}$ à $X_0(N)$ au-dessus de $\mathbb{Z}$ localisé en p, propriété bien connue des spécialistes (cf. [3] IV 3.19).

Nous allons construire des flèches finies :

$$\begin{array}{ccc} & X_0(\ell N) & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\beta} \\ X_0(N) & & X_0(N) \end{array}$$

au-dessus de $R = (\mathbb{Z}$ localisé en $p)$.

La courbe modulaire $X_0(N)$, à distance finie, est associée au champ dont les points à valeur dans un schéma S au-dessus de $\mathbb{Z}$ localisé en p sont les couples (E, C_N), où E est une S-courbe elliptique et C_N est un sous-schéma en groupes plat de E, "cyclique" d'ordre N. Plus précisément si $N = pN'$ avec $(p, N') = 1$, $C_N = C_p C_{N'}$, où $C_{N'}$ est, localement pour la topologie étale sur S isomorphe à $(\mathbb{Z}/N'\mathbb{Z})_S$ et C_p est fini et plat d'ordre p. De même $X_0(\ell N)$ est associée au champ des couples $(E, C_\ell C_N)$, où $C_\ell C_N$ est cyclique d'ordre ℓN, avec C_N comme plus haut et C_ℓ est cyclique d'ordre ℓ.

Le morphisme d'oubli de C_ℓ au niveau des champs :

$$(E, C_\ell C_N) \longmapsto (E, C_N)$$

induit sur les modules grossiers le morphisme

$$\alpha : X_0(\ell N) \longrightarrow X_0(N).$$

Ce morphisme est fini ; il factorise le morphisme fini canonique

$$X_0(\ell N) \longrightarrow X_0(1) = \text{ Droite projective.}$$

On définit de même β à partir du morphisme de champs :

$$(E, C_\ell C_N) \longmapsto (E/C_\ell, C_\ell C_N/C_\ell).$$

Soit w_ℓ l'involution de $X_0(\ell N)$ associée au morphisme de champs :

$$(E, C_\ell C_N) \longrightarrow (E/C_\ell, [\ell E/C_\ell].C_N),$$

(où ${}_\ell E$ désigne le noyau de la multiplication par ℓ dans E), alors $\beta = \alpha\ w_e$, donc est lui aussi fini.

Les morphismes α et β sont étales au-dessus d'un ouvert de $X_0(N)$ dense sur les fibres ; **ils peuvent être ramifiés à l'infini et au-dessus des points possédant des automorphismes exceptionnels.**

Soit $\mathcal{L}$ un faisceau inversible sur $X_0(N)$. Alors $\alpha^*(\mathcal{L})$ est un faisceau inversible sur $X_0(\ell N)$. L'application α^* induit un morphisme de groupes $\mathrm{Pic}_{X_0(N)/\mathbb{Z}} \longrightarrow \mathrm{Pic}_{X_0(\ell N)/\mathbb{Z}}$ qui commute aux changements de base, et donc un morphisme $i : J_0(N) \longrightarrow J_0(\ell N)$.

Si $\mathcal{M}$ est un faisceau inversible sur $X_0(\ell N)$, sa norme relativement à β, $\mathrm{Nor}_\beta(\mathcal{M})$ est définie, car les courbes modulaires sont normales ([6] 6.5), et est un faisceau inversible sur $X_0(N)$. Cette opération de norme existe plus généralement après tout changement de base lisse S sur $\mathbb{Z}$, car un tel changement conserve la normalité. Prenant $S = J_0(\ell N)$, et pour $\mathcal{M}$

le faisceau inversible universel de Poincaré, on obtient un morphisme de groupes :

$$j : J_0(\ell N) \longrightarrow J_0(N).$$

Par définition **la correspondance de Hecke relative à ℓ sur la jacobienne** $J_0(N)$ est l'endomorphisme : $\mathbf{T}_\ell = ji$ (cf. [8] p. 88).

Nous allons décrire $\mathbf{T}_\ell$ sur le tore de la fibre spéciale de $J_0(N)$.

Pour simplifier, ℓ étant fixé, notons $X' = X_0(\ell N)$, $J' = J_0(\ell N)$. Soient T (resp. T') le tore de J_k (resp. J'_k), M (resp. M') son groupe des caractères.

L'application $T \longrightarrow T'$, induite par i, provient de la contravariance de Pic appliquée au morphisme $\alpha_k : X'_k \longrightarrow X_k$. Elle s'insère donc dans un diagramme commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & \Pi k_x^* & \longrightarrow & T & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & k^* & \longrightarrow & \Pi_{x' \longrightarrow x} k_{x'}^* & \longrightarrow & T' & \longrightarrow & 1 \end{array}$$

où x parcourt les points singuliers de X_k.

L'application $T \longrightarrow T'$, correspond dualement à un morphisme $i^* : M' \longrightarrow M$. Pour le décrire, on passe à une clôture algébrique $\overline{k}$ de k et on considère le diagramme commutatif, à lignes exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & \oplus \mathbb{Z}\overline{x'} & \xrightarrow{\varepsilon'} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & \oplus \mathbb{Z}\overline{x} & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0, \end{array}$$

où l'application verticale centrale envoie $\overline{x'}$ sur $\alpha(\overline{x'})$ et où ε et ε' désignent les augmentations canoniques.

Passons au morphismes $T' \longrightarrow T$ induit par j. Il est associé à $j^* : M \longrightarrow M'$.

Au morphisme fini $\beta : X' \longrightarrow X$, entre schémas normaux est associée une application de norme. Elle induit une application de norme sur la fibre spéciale, (application qui n'est pas du type usuel, car $\beta_k : X'_k \longrightarrow X_k$ n'est ni un morphisme de schémas normaux, ni localement libre au voisinage

des points doubles ramifiés). On peut néanmoins préciser la norme en notant qu'elle est induite par la norme classique sur les courbes normalisées $\widetilde{X'_k} \longrightarrow \widetilde{X_k}$ et que, vu la nature particulière des singularités, on a des suites exactes :

$$1 \longrightarrow \mathbf{O}^*_{X'_k} \longrightarrow \mathbf{O}^*_{\widetilde{X'_k}} \longrightarrow \Pi k^*_{x'} \longrightarrow 1$$

$$1 \longrightarrow \mathbf{O}^*_{X_k} \longrightarrow \mathbf{O}^*_{\widetilde{X_k}} \longrightarrow \Pi k^*_{x} \longrightarrow 1$$

La norme induit un morphisme de la première ligne dans la seconde. On doit préciser l'application qui apparaît dans la dernière colonne. Elle envoie $k^*_{x'}$ dans k^*_x avec $x = \beta(x')$. Par hensélisation stricte de X en x, on se ramène au cas où $k^*_x = k^*_{x'}$, auquel cas apparaît l'élévation à la puissance $n_{x'}$, où $n_{x'}$ est l'indice de ramification de X' sur X en x'. Si e_x(resp. $e_{x'}$) est l'épaisseur de la singularité de X (resp. X') en x (resp. x'), on a $n_{x'} = e_x/e_{x'}$. Finalement, on voit que la norme de X' vers X, envoie $k^*_{x'}$ dans k^*_x par la norme résiduelle à la puissance $n_{x'}$.

Passant à une clôture algébrique de k et aux groupes des caractères, on trouve que j^* s'insère dans le diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & \oplus \mathbb{Z}\bar{x} & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & M' & \longrightarrow & \oplus \mathbb{Z}\bar{x}' & \xrightarrow{\varepsilon'} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

où la flèche verticale médiane envoie $\bar{x}$ sur $\sum_{\bar{x}' \longrightarrow \bar{x}} n_{\bar{x}'} \bar{x}'$.

Finalement, $\mathbb{T}_\ell$ induit un endomorphisme de T, associé au morphisme $i^*j^* : M \longrightarrow M$, qui s'insère dans le diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & \oplus \mathbb{Z}\bar{x} & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\ & & {\scriptstyle i^*j^*}\downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M & \longrightarrow & \oplus \mathbb{Z}\bar{x} & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

où la flèche médiane est l'application composée :

$$\overline{x} \longmapsto \sum_{\beta(\overline{x}')=\overline{x}} n_{\overline{x}'}\overline{x}'$$

$$\overline{x}' \longmapsto \alpha(\overline{x}').$$

En terme de champs, on peut la décrire ainsi. Soit (E, C_N) le couple, défini à isomorphisme près qui correspond au point supersingulier x. Alors son image par j^* est

$$\sum_{C_\ell}(E/C_\ell, {}_\ell E/C_\ell \cdot C_N),$$

où C_ℓ parcourt les $\ell+1$ sous-groupes cycliques d'ordre ℓ de ${}_\ell E$ et où l'on regroupe les termes du second membre par classes d'isomorphismes. Si la classe de $(E/C_\ell, {}_\ell E/C_\ell C_N)$ correspond au point $\overline{x}'$, elle apparaît avec la multiplicité $n_{\overline{x}'}$.

Finalement l'image de x par i^*j^* est la somme :

$$\sum_{C_\ell}(E/C_\ell,\ C_N).$$

Variante sur la propriété de prolongement des modèles de Néron

PROPOSITION 6. — *Soit R un anneau de valuation discrète de corps des fractions K, de corps résiduel k de caractéristique $p>0$. On suppose que l'indice de ramification absolu $e=v(p)$ de R est $<p-1$ (en particulier $p=2$ est exclu). Soit A un modèle de Néron semi-abélien sur R, d'une K-variété abélienne A_K. Alors pour tout R-schéma en groupes quasi-fini et plat G, l'application canonique :*

$$\mathrm{Hom}_{R-gr}(G, A) \longrightarrow \mathrm{Hom}_{K-gr}(G_K, A_K)$$

est bijective.

Si de plus on part d'une immersion $G_K \longrightarrow A_K$, son prolongement $G \longrightarrow A$ est une immersion.

Exemple : Prenons pour A le modèle de Néron de $J_0(N)_{\mathbb{Q}}$ et soit p un nombre premier qui divise strictement N. Soit G_K un sous-schéma en groupes fini de A_K, annulé par p, associé à une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $Gl_2(\mathbb{F}_{p^\infty})$. Supposons que G_K soit fini en p, c'est-à-dire se prolonge en un schéma en groupes G fini sur $\mathbb{Z}$ localisé en p. Alors si $p>2$, G se plonge dans A au-dessus de $\mathbb{Z}$ localisé en p.

Démonstration : Partons d'un morphisme de groupes $u_K : G_K \longrightarrow A_K$. Quitte à diviser G par l'adhérence schématique du noyau de u_K. On peut supposer que u_K est une immersion, et on doit alors montrer que G est un sous-schéma en groupes de A.

On peut supposer R hensélien et se borner au cas où G est annulé par une puissance de p, soit p^n.

Comme R est hensélien, G est extension d'un groupe étale G" par sa composante neutre G^0 qui est un groupe fini et plat à fibre spéciale radicielle.

De même $H = {}_{p^n}A$ est extension d'un groupe étale H" par sa composante neutre H^0.

Montrons d'abord que l'injection $u_K : G_K \longrightarrow {}_{p^n}A_K$ induit un morphisme sur les composantes neutres $u^0 : G^0 \longrightarrow H^0$.

Comme $e < p - 1$, l'application de restriction :

$$\mathrm{Hom}_{R-gr}(G', G'') \longrightarrow \mathrm{Hom}_{K-gr}(G'_K, G''_K),$$

de la catégorie des R-schémas en groupes finis, dans celle des K-schémas en groupes finis, est pleinement fidèle ([11] cor. 3.3.6). Il suffit donc de montrer que u_K envoie $(G^0)_K$ dans $(H^0)_K$, ou encore, que le morphisme composé $(G^0)_K \longrightarrow H_K \longrightarrow H''_K$ est nul. Or, d'après le théorème de monodromie de Grothendieck ([5] chap. IX prop. 5.6), l'action de $\mathrm{Gal}(\overline{K}/K)$ sur H''_K est non ramifiée, de sorte que H''_K se prolonge en un R-schéma en groupes fini étale $\widetilde{H}''$. Toujours en raison de la pleine fidélité que l'on vient de rappeler, $(G^0)_K \longrightarrow H''_K$ se prolonge en un R-morphisme $G^0 \longrightarrow \widetilde{H}''$. Comme $\widetilde{H}''$ est étale et G^0 connexe, ce morphisme est nul, donc u_K envoie G^0_K dans H^0_K.

Ceci étant, grâce au morphisme $G^0 \longrightarrow H^0 \longrightarrow A$, on construit le diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G^0 & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G'' & \longrightarrow & 0,
\end{array}$$

où E, extension d'un groupe étale par un groupe lisse, est lisse. La flèche $u_K : G_K \longrightarrow A_K$, induit une rétraction $E_K \longrightarrow A_K$ qui, d'après la propriété universelle usuelle des modèles de Néron se prolonge en un morphisme $E \longrightarrow A$. Le morphisme composé $G \longrightarrow E \longrightarrow A$ est le prolongement cherché u de u_K. Le fait que u soit une immersion se voit

par restriction aux parties finies de G et H et résulte encore de l'énoncé de pleine fidélité (cf. [11] 3.3.6).

BIBLIOGRAPHIE

[1] S. BOSCH, W. LÜTKEBOHMERT, M. RAYNAUD. — *Néron Models,* Ergebnisse, Springer-Verlag (1990).

[2] P. DELIGNE. — Le lemme de Gabber, *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell, édité par L. Szpiro, Asterisque* **127**, (1985), 131-150.

[3] P. DELIGNE et M. RAPOPORT. — *Les schémas de modules de courbes elliptiques. Modular Functions of one Variable II*, Lect. Notes Math. 349, 1973.

[4] A. GROTHENDIECK. — Fondements de la Géométrie Algébrique, *Sém. Bourbaki, V*, les schémas de Picard N° 232 (1962); *Benjamin*, New York (1966).

[5] A. GROTHENDIECK. — *Groupes de monodromie en Géométrie Algébrique : Sém. de Géométrie Algébrique [SGA 7]*, Lect. Notes Math. 225, 1971.

[6] A. GROTHENDIECK et J. DIEUDONNÉ. — *Etude globale élémentaire de quelques classes de morphismes : Eléments de Géométrie Algébrique, [EGA II]*, Pub. Math. IHES 8, 1961.

[7] N. KATZ et B. MAZUR. — *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies 108, Princeton University Press, Princeton, 1965.

[8] B. MAZUR. — Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47**, (1977), 33-186.

[9] B. MAZUR et P. SWINNERTON-DYER. — Arithmetic of Weil curves, *Invent. Math.* **25**, (1974), 1-61.

[10] D. MUMFORD. — The topology of normal singularities of an algebraic surface, *Pub. IHES* **9**, (1961), 5-22.

[11] M. RAYNAUD. — Schémas en groupes de type $(p, \cdots, p)$, *Bull. Soc. Math. France* **102**, (241-280), 1974.

[12] M. RAYNAUD. — *p-Groupes et réduction semi-stable des courbes, The Grothendieck Festschrift, Volume III*, Birkhäuser, 1991.

[13] J.-P. SERRE. — *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

Michel RAYNAUD
Département de Mathématique
Bâtiment 425
Université de Paris-Sud
91405 ORSAY Cedex

RÉALISATION ℓ-ADIQUE DE L'ACCOUPLEMENT DE MONODROMIE D'APRÈS A. GROTHENDIECK

Luc ILLUSIE

On explicite l'argument de Grothendieck dans (SGA 7 IX 12.7) pour déduire la partie relative à $\ell \neq p$ de son théorème 12.5 de la formule de Picard-Lefschetz de (SGA 7 XV). Voir Saito [5, § 1] pour un exposé voisin et divers compléments.

Je tiens à remercier vivement le rapporteur pour de judicieuses critiques et suggestions.

Je remercie également Mme Le Bronnec pour la parfaite saisie du manuscrit.

0. **Notations** (cf. (SGA 7 I § 0) et (SGA 7 IX § 12))

S : un trait strictement local
s (resp. η) : le point fermé (resp. générique) de S
p : l'exposant caractéristique de $k(s)$
v : la valuation de S
$\mathfrak{m}$: l'idéal maximal de S
$\overline{\eta}$: un point géométrique générique
ℓ : un nombre premier $\neq p$
$I = \mathrm{Gal}(\overline{\eta}/\eta)$
$t_\ell : I \longrightarrow \mathbb{Z}_\ell(1)$ la ℓ-composante de l'homorphisme canonique $I \longrightarrow \prod_{p' \neq p} \mathbb{Z}_{p'}(1)$
Λ : l'anneau $\mathbb{Z}_\ell$ (ou l'anneau des entiers d'une extension finie de $\mathbb{Q}_\ell$)
X : un S-schéma propre et plat, à fibres géométriques connexes de dimension 1, lisse hors d'un ensemble fini Σ de points fermés de X_s ; on suppose qu'au voisinage de chaque point $x \in \Sigma$, X est, localement pour la topologie étale, S-isomorphe au sous-schéma de $\mathbb{A}^2_S = S[t_1, t_2]$ d'équation $t_1 t_2 = a_x$, avec $a_x \in \mathfrak{m}$, $a_x \neq 0$; on note $e_x = v(a_x)$
$Y : X_s$

A : le modèle de Néron de $\mathrm{Pic}_{X_\eta/\eta}$; A^0 sa composante neutre
T : le tore maximal de A^0_s (= $\mathrm{Pic}^0_{Y/s}$ (SGA 7 IX 12.1.12))
$Z_{(\overline{x})}$: localisé strict du schéma Z en le point géométrique $\overline{x}$

Sommaire

1. Cycles évanescents et formule de Picard-Lefschetz

1.1. Pour $x \in \Sigma$, notons B_x l'ensemble des deux branches de Y en x (composantes irréductibles de $Y_{(x)}$), et définissons $\mathbb{Z}(x)$, $\mathbb{Z}'(x)$ par les suites exactes (duales l'une de l'autre)

$$0 \longrightarrow \mathbb{Z} \xrightarrow{(1)} \mathbb{Z}^{B_x} \longrightarrow \mathbb{Z}(x) \longrightarrow 0, \tag{1.1.1}$$

$$0 \longrightarrow \mathbb{Z}'(x) \longrightarrow \mathbb{Z}^{B_x} \xrightarrow{(2)} \mathbb{Z} \longrightarrow 0, \tag{1.1.2}$$

où (1) (resp. (2)) est l'application diagonale (resp. somme). Il peut être commode de choisir, pour chaque $x \in \Sigma$, un ordre sur B_x : ceci détermine une base $\delta'_x = (1, -1)$ de $\mathbb{Z}'(x)$, nous noterons δ_x la base de $\mathbb{Z}(x)$ duale de δ'_x.

$$\Lambda(x) = \mathbb{Z}(x) \otimes \Lambda, \quad \Lambda'(x) = \mathbb{Z}'(x) \otimes \Lambda \tag{1.1.3}$$

Nous noterons $\widetilde{Y}$ le normalisé de $Y = X_s$, et, pour $x \in \Sigma$, $\widetilde{Y_{(x)}}$ celui de $Y_{(x)}$, et $\tilde{x} = \{x_1, x_2\} = (\widetilde{Y_{(x)}})_x$ l'ensemble des deux points de $\widetilde{Y_{(x)}}$ au-dessus de x.

Rappelons quelques résultats de Deligne (SGA 7 XV) sur le complexe $R\Psi\Lambda$ relatif à $X \longrightarrow S$.

1.2. On a

$$R^i\Psi\Lambda = 0 \quad \text{pour } i \neq 0, 1 \; ; \quad R^0\Psi\Lambda = \Lambda. \tag{1.2.1}$$

Le triangle canonique

$$\Lambda \longrightarrow R\Psi\Lambda \longrightarrow R\Phi\Lambda \longrightarrow \tag{1.2.2}$$

donne lieu à un isomorphisme

$$\tau_{\geq 1} R\Psi\Lambda \xrightarrow{\sim} R\Phi\Lambda,$$

et le complexe $R\Phi\Lambda$ est concentré sur Σ (i.e. $R\Phi\Lambda | Y - \Sigma = 0$).

1.3. Soit $x \in \Sigma$. On a

$$H^i_x(Y, R\Psi\Lambda) = 0 \quad \text{pour } i \neq 1, 2. \tag{1.3.1}$$

Pour $i = 2$, on a un isomorphisme trace

$$Tr : H^2_x(Y, R\Psi\Lambda) \xrightarrow{\sim} \Lambda(-1). \tag{1.3.2}$$

Pour $i = 1$, il existe un unique isomorphisme

$$H^1_x(Y, R\Psi\Lambda) \xrightarrow{\sim} \Lambda(x) \tag{1.3.3}$$

rendant commutatif le diagramme

$$\begin{array}{ccc} H^0(\widetilde{Y_{(x)}}, \Lambda) & \xrightarrow{d} & H^1_x(Y, R\Psi\Lambda) \\ \simeq \downarrow & & \downarrow \simeq \\ \Lambda^{B_x} & \xrightarrow{(1.1.1)} & \Lambda(x), \end{array} \tag{1.3.4}$$

où la flèche verticale de gauche est l'isomorphisme évident, et d le composé

$$H^0(\widetilde{Y_{(x)}}, \Lambda) \xrightarrow{\sim} H^0(U_x, \Lambda) \xrightarrow{\sim} H^0(U_x, R\Psi\Lambda) \xrightarrow{\partial} H^1_x(Y, R\Psi\Lambda),$$

avec $U_x := Y_{(x)} - \{x\}$ (dans les termes de (SGA 7 XV 3.1.2, 3.3.3), (1.3.3) identifie $H^1_x(Y, R\Psi\Lambda)$ au quotient primitif du H^0 de la quadrique $\tilde{x}$). La base δ_x de $H^1_x(Y, R\Psi\Lambda)$ définie via (1.3.3) est pas définition le **cycle évanescent en** x.

La suite (1.1.1) s'identifie à un morceau de la suite exacte de cohomologie de $(Y_{(x)}, x)$ à valeurs dans $R\Psi\Lambda$:

(1.3.5)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(Y_{(x)}, R\Psi\Lambda) & \longrightarrow & H^0(U_x, R\Psi\Lambda) & \xrightarrow{d} & H^1_x(Y_{(x)}, R\Psi\Lambda) & \longrightarrow & 0 \\ & & {\scriptstyle (1.2.1)}\downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq {\scriptstyle (1.3.3)} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \Lambda^{B_x} & \longrightarrow & \Lambda(x) & \longrightarrow & 0. \end{array}$$

1.4.1 Soit $x \in \Sigma$. L'accouplement naturel

$$R^1\Psi(\Lambda)_x \times H^1_x(Y_{(x)}, R\Psi\Lambda) \longrightarrow \Lambda(-1), \quad (a, b) \longmapsto Tr(ab) \tag{1.4.1}$$

est une dualité parfaite entre modules libres de rang 1.

On a d'autre part un accouplement naturel entre $H^2_x(Y_{(x)}, \Lambda) = H^2_{\tilde{x}}(\widetilde{Y_{(x)}}, \Lambda)$ et $H^0(\widetilde{Y_{(x)}}, \Lambda)$,

$$H^2_x(Y_{(x)}, \Lambda) \times H^0(\widetilde{H_{(x)}}, \Lambda) \longrightarrow \Lambda(-1), \quad (a, b) \longmapsto Tr(ab), \tag{1.4.2}$$

qui est une dualité parfaite entre modules libres de rang 2.

LEMME 1.5. — (*a*) *La transposée de la flèche d de* (1.3.4) *pour les accouplements* (1.4.1) *et* (1.4.2) *est* $d'(1)$, d' *désignant la flèche composée*

$$d' : R^1\Psi(\Lambda)_x \longrightarrow H^1(U_x, R\Psi\Lambda) = H^1(U_x, \Lambda) \xrightarrow{-\partial} H^2_x(Y_{(x)}, \Lambda)$$

(où la première flèche est la restriction), en d'autres termes on a

$$Tr(d'(1)a \cdot b) = Tr(a \cdot db)$$

pour $a \in R^1\Psi(\Lambda)_x(1)$, $b \in H^0(\widetilde{Y_{(x)}}, \Lambda)$.

(*b*) *Notons* $i : \{x\} \longrightarrow Y_{(x)}$ *l'inclusion. La flèche* d' *de (a) est égale au composé*

$$R^1\Psi(\Lambda)_x \xrightarrow{(1)} R^1\Phi(\Lambda)_x \xrightarrow{(2)} H^1_x(Y_{(x)}, R\Phi\Lambda) \xrightarrow{(3)} H^2_x(Y_{(x)}, \Lambda)$$

où (1) *est la flèche canonique* (1.2.2), (2) *l'effet sur* H^1 *de l'isomorphisme inverse de*

$$i_*Ri^!R\Phi(\Lambda) \xrightarrow{\sim} R\Phi(\Lambda)_x$$

(venant de ce que $R\Phi(\Lambda)|U_x = 0$*), et* (3) *le bord de la suite exacte de cohomologie du triangle*

$$i_*Ri^!\Lambda \longrightarrow i_*Ri^!R\Psi\Lambda \longrightarrow i_*Ri^!R\Phi\Lambda$$

déduit de (1.2.2).

(*c*) *L'isomorphisme*

$$\Lambda'(x) \longrightarrow R^1\Psi(\Lambda)_x(1) \tag{1.5.1}$$

transposé de (1.3.3) *via l'accouplement* (1.4.1) *(et l'accouplement naturel entre* $\Lambda(x)$ *et* $\Lambda'(x)$*) rend commutatif le carré*

$$\begin{array}{ccc} \Lambda'(x) & \xrightarrow{(1.1.2)} & \Lambda^{B_x} \\ \simeq\downarrow & & \simeq\downarrow \\ R^1\Psi(\Lambda)_x(1) & \xrightarrow{d'(1)} & H^2_x(Y_{(x)}, \Lambda)(1), \end{array} \tag{1.5.2}$$

où la flèche verticale de droite est le transposé de l'isomorphisme $H^0(\widetilde{Y_{(x)}}, \Lambda) \longrightarrow \Lambda^{B_x}$ *via l'accouplement* (1.4.2).

(d) *La suite* (1.1.2) *s'identifie à un second morceau de la suite exacte de cohomologie de* $(Y_{(x)}, x)$ *à valeurs dans* $R\Psi\Lambda$:
(1.5.3)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(Y_{(x)}, R\Psi\Lambda)(1) & \longrightarrow & H^1(U_x, R\Psi\Lambda)(1) & \xrightarrow{-\partial} & H^2_x(Y_{(x)}, R\Psi\Lambda)(1) & \longrightarrow & 0 \\ & & \simeq \downarrow (1.5.2) & & \simeq \downarrow & & \simeq \downarrow Tr & & \\ 0 & \longrightarrow & \Lambda'(x) & \longrightarrow & \Lambda^{B_x} & \longrightarrow & \Lambda & \longrightarrow & 0. \end{array}$$

(la flèche vertical médiane étant duale de celle de (1.3.5) *via l'accouplement entre* $H^0(U_x, R\Psi\Lambda) = H^0(\widetilde{Y_{(x)}}, \Lambda)$ *et* $H^1(U_x, R\Psi\Lambda)(1) = H^1(U_x, \Lambda)(1) \xrightarrow[\simeq]{-\partial} H^2_x(Y_{(x)}, \Lambda)(1)$ *donné par* (1.4.2)*).*

L'assertion (c) découle de (a), et (d) s'en déduit. Prouvons (a). Il s'agit de voir que lorsqu'on identifie $H^1(U_x, R\Psi\Lambda)(1)$ au dual de $H^0(U_x, R\Psi\Lambda)$ par l'accouplement

$$H^1(U_x, R\Psi\Lambda)(1) \otimes H^0(U_x, R\Psi\Lambda) \xrightarrow{\text{cup-produit}} H^1(U_x, R\Psi\Lambda)(1) \xrightarrow{-Tr\partial} \Lambda,$$

et $R^1\psi(\Lambda)_x(1) = H^1(Y_{(x)}, R\Psi\Lambda(1)$ au dual de $H^1_x(Y_{(x)}, R\Psi\Lambda)$ par (1.4.1), alors la transposée de $\partial : H^0(U_x, R\Psi\Lambda) \longrightarrow H^1_x(Y_{(x)}, R\Psi\Lambda)$ est la flèche de restriction $H^1(Y_{(x)}, R\Psi\Lambda)(1) \longrightarrow H^1(U_x, R\Psi\Lambda)(1)$, en d'autres termes qu'on a

$$-Tr\partial(ab) = Tr(a \cdot \partial b)$$

pour $a \in H^1(Y_{(x)}, R\Psi\Lambda)(1)$, $b \in H^0(U_x, R\Psi\Lambda)$, le produit ab désignant par abus $\rho(a)b$, où $\rho(a) \in H^1(U_x, R\Psi\Lambda)$ est la restriction de a. Or on a

$$-\partial(ab) = a \cdot \partial b,$$

par les formules standard reliant cup-produit et cobord (cf. R. Godement, Théories des faisceaux, Hermann 1958, p. 255), d'où (a).

Prouvons (b). Notons $j : U_x \hookrightarrow Y_{(x)}$ l'inclusion. On déduit de (1.2.2) un

"diagramme des 9" (sur $Y_{(x)}$)

$$\begin{array}{ccccc}
i_*Ri^!\Lambda & \longrightarrow & i_*Ri^!R\Psi\Lambda & \longrightarrow & i_*Ri^!R\Phi\Lambda \\
\downarrow & & \downarrow & & \downarrow \\
\Lambda & \longrightarrow & R\Psi\Lambda & \longrightarrow & R\Phi\Lambda \\
\downarrow & & \downarrow & & \downarrow \\
Rj_*j^*\Lambda & \longrightarrow & Rj_*j^*R\Psi\Lambda & \longrightarrow & 0.
\end{array}$$

Il s'agit de voir que les composés

$$H^1(R\Psi\Lambda) \longrightarrow H^1(Rj_*j^*R\Psi\Lambda) \xrightarrow{\sim} H^1(Rj_*j^*\Lambda) \xrightarrow{\partial} H^2(i_*Ri^!\Lambda)$$

et

$$H^1(R\Psi\Lambda) \longrightarrow H^1(R\Phi\Lambda) \xrightarrow{\sim} H^1(i_*Ri^!R\Psi\Lambda) \xrightarrow{\partial} H^2(i_*Ri^!\Lambda)$$

sont opposés. Or cela résulte du lemme suivant, dont la vérification est laissée au lecteur :

LEMME 1.5.4. — *Soient $\mathcal{A}$ une catégorie abélienne, $D(\mathcal{A})$ sa catégorie dérivée, et*

$$\begin{array}{ccccc}
A' & \longrightarrow & B' & \longrightarrow & C' \\
\downarrow & & \downarrow & & \downarrow \\
A & \longrightarrow & B & \longrightarrow & C \\
\downarrow & & \downarrow & & \downarrow \\
A'' & \longrightarrow & B'' & \longrightarrow & C''
\end{array}$$

un diagramme des 9 de $D(\mathcal{A})$ (triangle distingué de triangles distingués associé à une suite exacte courte de suites exactes courtes de complexes). On suppose que $C'' = 0$ (donc $A'' \xrightarrow{\sim} B''$ et $C' \xrightarrow{\sim} C$). Alors les composés

$$B \longrightarrow B'' \xrightarrow{\sim} A'' \longrightarrow A'[1] \quad \text{et} \quad B \longrightarrow C \xrightarrow{\sim} C' \longrightarrow A'[1]$$

sont opposés.

1.6. Considérons la partie centrale de la suite exacte de cohomologie de $R\Gamma(Y,-)$ appliquée à (1.2.2)(1) ("suite exacte de spécialisation")

$$\begin{aligned} 0 \longrightarrow H^1(Y,\Lambda)(1) \xrightarrow{sp} H^1(Y,R\Psi\Lambda)(1) \xrightarrow{(1)} \bigoplus_{x\in\Sigma} R^1\Phi(\Lambda)_x(1) \\ \xrightarrow{(2)} H^2(Y,\Lambda)(1) \xrightarrow{sp} H^2(Y,R\Psi\Lambda)(1) \longrightarrow 0. \end{aligned} \tag{1.6.1}$$

La flèche (1) est composée de la restriction $H^1(Y,R\Psi\Lambda)(1) \longrightarrow \oplus H^1(Y_{(x)},R\Psi\Lambda)(1)$ et de la somme des flèches canoniques $H^1(Y_{(x)},R\Psi\Lambda)(1) \xrightarrow{\sim} H^1(Y_{(x)},R\Phi\Lambda)(1)$. La flèche (2) est composée de la somme des flèches bord (3) envisagées en 1.5 (b) et de la flèche naturelle $\oplus H^2_x(Y,\Lambda)(1) \longrightarrow H^2(Y,\Lambda)(1)$ (oubli des supports). Il résulte de 1.5 (b) que l'on a un carré commutatif

$$\begin{array}{ccc} \oplus\Lambda'(x) & \longrightarrow & \Lambda^B \\ \simeq\downarrow & & \simeq\downarrow Tr^{-1} \\ \oplus R^1\Phi(\Lambda)_x(1) & \xrightarrow[(2)]{} & H^2(Y,\Lambda)(1), \end{array} \tag{1.6.2}$$

où B est l'ensemble des composantes irréductibles de Y, $Tr : H^2(Y,\Lambda)(1) \xrightarrow{\sim} \Lambda^B$ l'isomorphisme trace, la flèche verticale de gauche la somme des isomorphismes (1.5.1), et la flèche horizontale supérieure composée de la somme des flèches canoniques $\Lambda'(x) \longrightarrow \Lambda^{B_x}$ et des flèches évidentes $\Lambda^{B_x} \longrightarrow \Lambda^B$ (i.e., avec les conventions de 1.1, envoyant δ'_x sur $C_{x_1} - C_{x_2}$, où C_{x_i} est la composante contenant x_i).

Notons qu'on a un isomorphisme canonique

$$H^2(Y,R\Psi\Lambda)(1) \xrightarrow{\sim} H^2(X_{\overline{\eta}},\Lambda)(1) \xrightarrow[Tr]{\simeq} \Lambda \tag{1.6.3}$$

Les Λ-modules libres $H^1(Y,R\Psi\Lambda)(1)$ $(\simeq H^1(X_{\overline{\eta}},\Lambda)(1))$, $\bigoplus_{x\in\Sigma} R^1\Phi(\Lambda)_x(1)$, $H^2(Y,\Lambda)(1)$ sont duaux respectivement de $H^1(Y,R\Psi\Lambda)$ $(\simeq H^1(X_{\overline{\eta}},\Lambda))$, $\bigoplus_{x\in\Sigma} H^1_x(Y,R\Psi\Lambda)$, $H^0(\widetilde{Y},\Lambda)$ via les accouplements naturels donnés par $(a,b) \longmapsto Tr(ab)$. Comme le conoyau de la flèche (2) de (1.6.1) est un Λ-module libre (de rang 1) d'après (1.6.3), la suite transposée

$$H^1(Y,R\Psi\Lambda) \xleftarrow{(1)'} \bigoplus_{x\in\Sigma} H^1_x(Y,R\Psi\Lambda) \xleftarrow{(2)'} H^0(\widetilde{Y},\Lambda), \tag{1.6.4}$$

est exacte. Il résulte de 1.5 (a) et (b) que la flèche (2)' est composée de la restriction $H^0(\widetilde{Y},\Lambda) \longrightarrow \oplus H^0(U_x,\Lambda)$ (où $U_x := Y_{(x)} - \{x\}$) et de la somme des flèches bord $H^0(U_x,\Lambda) = H^0(U_x, R\Psi\Lambda) \xrightarrow{d} H^1_x(Y, R\Psi\Lambda)$ de (1.3.5). On a par suite un carré commutatif

$$\begin{array}{ccc} \bigoplus\limits_{x\in\Sigma} H^1_x(Y,R\Psi\Lambda) & \xleftarrow{(2)'} & H^0(\widetilde{Y},\Lambda) \\ \downarrow \simeq & & \downarrow \simeq \\ \bigoplus\limits_{x\in\Sigma} \Lambda(x) & \longleftarrow & \Lambda^B, \end{array} \tag{1.6.5}$$

où la flèche verticale de gauche est la somme des isomorphismes (1.3.3), celle de droite l'isomorphisme naturel (dual de l'isomorphisme trace figurant dans (1.6.2)), et la flèche horizontale inférieure composée de la flèche évidente $\Lambda^B \longrightarrow \oplus \Lambda^{B_x}$ et de la somme des flèches canoniques $\Lambda^{B_x} \longrightarrow \Lambda(x)$ (1.1.1). La flèches (1)' est somme des flèches d'oubli des supports. Notons que la flèche $\Lambda \longrightarrow R\Psi\Lambda$ donne un carré commutatif

$$\begin{array}{ccc} H^1(Y,\Lambda) & \longleftarrow & \bigoplus\limits_{x\in\Sigma} H^1_x(Y,\Lambda) \\ {\scriptstyle sp}\downarrow & & \downarrow \simeq \\ H^1(Y,R\Psi\Lambda) & \xleftarrow{(1)'} & \bigoplus\limits_{x\in\Sigma} H^1_x(Y,R\Psi\Lambda), \end{array} \tag{1.6.6}$$

où la flèche verticale de gauche est injective, et celle de droite un isomorphisme (car $H^0_x(Y,R\Phi\Lambda) = 0$, et $\partial : H^1_x(Y,R\Phi\Lambda) \longrightarrow H^2_x(Y,\Lambda)$ est injectif d'après 1.5 (b)). En particulier, l'image de (1)' est contenue dans $H^1(Y,\Lambda)$.

On pourrait – mais nous n'en aurons pas besoin – interpréter (1.6.4) comme un morceau de la suite exacte "de cospécialisation" (définie par le triangle transposé de $\Lambda \longrightarrow R\Psi\Lambda \longrightarrow R\Phi\Lambda$ par application de $R\mathrm{Hom}(-,K)$ où K est un complexe dualisant sur Y).

1.7. Rappelons enfin que, pour $x \in \Sigma$ et $\sigma \in I$, le morphisme **variation** en x

$$Var(\sigma)_x : R^1\Phi(\Lambda)_x \longrightarrow H^1_x(Y,R\Psi\Lambda)$$

est donné par

$$Var(\sigma)_x(a) = -e_x t_\ell(\sigma)(a\delta_x)\delta_x \tag{1.7.1}$$

(SGA 7 XV 3.3.5) (cf. §0, 1.3 et 1.5 pour les notations; $(a\delta_x) \in \Lambda(-1)$ est la coordonnée de a par rapport à δ'_x). Il est commode d'introduire

$$N_x : R^1\Phi(\Lambda)_x(1) \longrightarrow H^1_x(Y, R\Psi\Lambda)$$

("logarithme de la monodromie en x"), défini par la formule

$$N_x(t_\ell(\sigma)a) = Var(\sigma)_x(a) \tag{1.7.2}$$

pour $a \in R^1\Phi(\Lambda)_x$ et $\sigma \in I$. On a un carré commutatif

$$\begin{array}{ccccc} R^1\Phi(\Lambda)_x(1) & \xrightarrow[\simeq]{(1.5.1)} & \Lambda'(x) & \delta'_x \\ \Big\downarrow{\scriptstyle N_x} & & \Big\downarrow & \Big\downarrow \\ H^1_x(Y, R\Psi\Lambda) & \xrightarrow[\simeq]{(1.3.3)} & \Lambda(x) & -e_x\delta_x. \end{array}$$

Il résulte de ce qui précède et de la factorisation de $\sigma - 1 : H^1(X_{\overline{\eta}}, \Lambda) \longrightarrow H^1(X_{\overline{\eta}}, \Lambda)$ en somme des $Var(\sigma)_x$ (SGA 7 XIII 2.4.6) qu'il existe un unique homomorphisme

$$N : H^1(X_{\overline{\eta}}, \Lambda)(1)(= H^1(Y, R\Psi\Lambda)(1)) \longrightarrow H^1(X_{\overline{\eta}}, \Lambda)\ (= H^1(Y, R\Psi\Lambda))$$

("logarithme de la monodromie")

$$N(t_\ell(\sigma)a) = (\sigma - 1)a \tag{1.7.3}$$

pour $a \in H^1(X_{\overline{\eta}}, \Lambda)$ et $\sigma \in I$, et que N rend commutatif le carré

$$\begin{array}{ccc} H^1(X_{\overline{\eta}}, \Lambda)(1) = H^1(Y, R\Psi\Lambda)(1) & \xrightarrow{(1)} & \bigoplus_{x\in\Sigma} R^1\Phi(\Lambda)_x(1) \\ \Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle \oplus N_x} \\ H^1(X_{\overline{\eta}}, \Lambda) = H^1(Y, R\Psi\Lambda) & \xleftarrow{(1)'} & \bigoplus_{x\in\Sigma} H^1_x(Y, R\Psi\Lambda), \end{array} \tag{1.7.4}$$

avec les notations de (1.6.1) et (1.6.4).

2. Application à l'accouplement de monodromie

2.1. Soit B l'ensemble des composantes irréductibles de Y. Si $B = \{C_1, \ldots, C_n\}$, le noyau de l'application somme $\mathbb{Z}^B \longrightarrow \mathbb{Z}$ a pour base les $C_1 - C_i$ $(2 \leq i \leq n)$. C'est donc l'image de l'application $\bigoplus_{x \in \Sigma} \mathbb{Z}'(x) \longrightarrow \mathbb{Z}^B$ envoyant δ'_x sur $C_{x_1} - C_{x_2}$, avec les notations de 1.1, C_{x_i} désignant la composante irréductible correspondant au point x_i. Nous définirons M par la suite exacte

$$0 \longrightarrow M \longrightarrow \bigoplus_{x \in \Sigma} \mathbb{Z}'(x) \longrightarrow \mathbb{Z}^B \longrightarrow \mathbb{Z} \longrightarrow 0, \tag{2.1.1}$$

où les flèches sont celles qu'on vient de considérer. C'est donc un $\mathbb{Z}$-module libre de rang fini. Par transposition (pour les dualités évidentes sur $\mathbb{Z}$, $\mathbb{Z}^B$ et les $\mathbb{Z}^{B_x}$), on obtient une suite exacte

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}^B \longrightarrow \bigoplus_{x \in \Sigma} \mathbb{Z}(x) \longrightarrow M^\vee \longrightarrow 0, \tag{2.1.2}$$

où $\mathbb{Z}^B \longrightarrow \mathbb{Z}(x)$ est composé des projections $\mathbb{Z}^B \longrightarrow \mathbb{Z}^{B_x}$ et $\mathbb{Z}^{B_x} \longrightarrow \mathbb{Z}(x)$ (1.1.1).

Par analogie avec (SGA 7 IX 12.4.5), notons

$$u : M \otimes_{\mathbb{Z}} M \longrightarrow \mathbb{Z} \tag{2.1.3}$$

l'accouplement défini par l'homomorphisme composé

$$\begin{array}{ccccc} M & \longrightarrow & \bigoplus_{x \in \Sigma} \mathbb{Z}'(x) & & \delta'_x \\ {\scriptstyle u_*}\downarrow & & \downarrow & & \downarrow \\ M^\vee & \longleftarrow & \bigoplus_{x \in \Sigma} \mathbb{Z}(x) & & -e_x \delta_x, \end{array}$$

avec les notations de §0 et 1.1 (le signe diffère de celui de (loc. cit.), où il est supposé par ailleurs que $e_x = 1$ pour tout x). En d'autres termes, u est la forme bilinéaire symétrique induite sur M par la forme quadratique $-\Sigma e_x \delta_x^2$ sur $\oplus \mathbb{Z}'(x)$. Elle est donc définie négative; en particulier, u_* est injectif et $u_* \otimes \mathbb{Q}$ est un isomorphisme.

2.2. Les considérations de 1.6 montrent que, si l'on identifie $H^2(Y,\Lambda)(1)$ à Λ^B par l'isomorphisme trace, et, pour $x \in \Sigma$, $R^1\Phi(\Lambda)_x(1)$ à $\Lambda'(x)$ par l'isomorphisme (1.5.1), alors $M \otimes \Lambda$ apparaît comme noyau de (2) dans la suite exacte de spécialisation (1.6.1) :

(2.2.1)

$$\begin{array}{ccccc} H^1(X_{\overline{\eta}},\Lambda)(1) & \longrightarrow & \bigoplus_{x\in\Sigma} R^1\Phi(\Lambda)_x(1) & \xrightarrow{(2)} & H^2(Y,\Lambda)(1) \\ & \searrow^{c} \quad \nearrow & & & \\ & M\otimes\Lambda & & & \\ & \nearrow \quad \searrow & & & \\ 0 & & 0 & & \end{array}$$

Dualement, $M^\vee \otimes \Lambda$ apparaît comme conoyau de la flèche $(2)'$ de la suite exacte de cospécialisation (1.6.4) :

(2.2.2)

$$\begin{array}{ccccc} H^1(X_{\overline{\eta}},\Lambda) & \longleftarrow & \bigoplus_{x\in\Sigma} H^1_x(Y,R\Psi\Lambda) & \xleftarrow{(2)'} & H^0(\widetilde{Y},\Lambda) \\ & \nwarrow^{c'} \quad \swarrow & & & \\ & M^\vee\otimes\Lambda & & & \\ & \swarrow \quad \nwarrow & & & \\ 0 & & 0 & & \end{array}$$

La flèche c' est transposée de c. Enfin, par définition de u_*, il résulte de (1.7.4)

que l'on a un diagramme commutatif

$$
\begin{array}{ccccc}
H^1(X_{\overline{\eta}},\Lambda)(1) & \xrightarrow{\ c\ } & M\otimes\Lambda & \hookrightarrow & \underset{x\in\Sigma}{\oplus} R^1\Phi(\Lambda)_x(1) \\
\downarrow{\scriptstyle N} & & \downarrow{\scriptstyle u_*\otimes\Lambda} & & \downarrow{\scriptstyle \oplus N_x} \\
H^1(X_{\overline{\eta}},\Lambda) & \xleftarrow{\ c'\ } & M^\vee\otimes\Lambda & \twoheadleftarrow & \underset{x\in\Sigma}{\oplus} H^1_x(Y,R\Phi\Lambda).
\end{array}
\tag{2.2.3}
$$

2.3. Soit T le tore maximal de $\mathrm{Pic}^0_{Y/s}$ (cf. §0). Rappelons (SGA 7 IX 12.3) comment on identifie M, défini par (2.1.1), au groupe des caractères de T, ou, dualement, T à $M^\vee\otimes\mathbb{G}_m$, $M^\vee$ étant défini par (2.1.2). Soit $\pi:\widetilde{Y}\longrightarrow Y$ la projection canonique. Considérons la suite exacte de faisceaux (étales) sur Y

$$
0\longrightarrow \mathbb{G}_{mY}\longrightarrow \pi_*\mathbb{G}_{m\widetilde{Y}}\longrightarrow \underset{x\in\Sigma}{\oplus}\mathbb{Z}(x)\otimes\mathbb{G}_m\longrightarrow 0. \tag{2.3.1}
$$

Par définition, T apparaît comme noyau (ou conoyau) dans la suite exacte de cohomologie correspondante

$$
\begin{array}{ccccccccc}
0\longrightarrow\mathbb{G}_m & \longrightarrow & \mathbb{Z}^B\otimes\mathbb{G}_m & \longrightarrow & \underset{x\in\Sigma}{\oplus}\mathbb{Z}(x)\otimes\mathbb{G}_m & \longrightarrow & \mathrm{Pic}_{Y/s} & \longrightarrow & \mathrm{Pic}_{\widetilde{Y}/s}\longrightarrow 0 \\
 & & & & & \searrow\ \nearrow & & & \\
 & & & & & T & & & \\
 & & & & & \nearrow\ \searrow & & & \\
 & & & & 0 & & 0 & &
\end{array}
\tag{2.3.2}
$$

Comme le début de (2.3.2), jusqu'à $\oplus\mathbb{Z}(x)\otimes\mathbb{G}_m$, se déduit du début de (2.1.2) (jusqu'à $\oplus\mathbb{Z}(x)$) par tensorisation avec $\mathbb{G}_m$, on a donc canoniquement

$$
M^\vee\otimes\mathbb{G}_m\xrightarrow{\sim}T. \tag{2.3.3}
$$

Par application du foncteur de Tate T_ℓ et tensorisation avec $\Lambda(-1)$, on en déduit un isomorphisme

$$
M^\vee\otimes\Lambda\xrightarrow{\sim}T_\ell(T)\otimes\Lambda(-1), \tag{2.3.4}
$$

et $M^\vee \otimes \Lambda$ apparaît comme conoyau dans la suite exacte déduite de (2.3.2)

(2.3.5)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \Lambda^B & \longrightarrow & \underset{x\in\Sigma}{\oplus}\Lambda(x) & \longrightarrow & H^1(Y,\Lambda) \\ & & & & & \searrow & & \nearrow_{\gamma'} & \\ & & & & & & M^\vee\otimes\Lambda & & \\ & & & & & \nearrow & & \searrow & \\ & & & & & 0 & & 0 & \end{array}$$

Rappelons que, d'après (1.6.6), l'image de la flèche c' figurant dans (2.2.2) est contenue dans $H^1(Y,\Lambda) \subset H^1(Y,R\Psi\Lambda) = H^1(Y_{\overline{\eta}},\Lambda)$.

LEMME 2.4. — *On a* $c' = -\gamma' : M^\vee \otimes \Lambda \longrightarrow H^1(Y,\Lambda)$.

Il suffit de montrer que les flèches composées, qu'on notera encore c' et γ', de $\oplus\Lambda(x)$ dans $H^1(Y,\Lambda)$ sont opposées. Soit $can : \oplus H^1_x(Y,\Lambda) \longrightarrow H^1(Y,\Lambda)$ la flèche canonique. La flèche c' (resp. γ') s'obtient en composant can avec une somme de flèches

$$c'_x \text{ (resp. } \gamma'_x) : \Lambda(x) \longrightarrow H^1_x(Y,\Lambda)$$

(cf. (1.6.6)). Notons

$$\partial_x \text{ (resp. } \delta_x) : \Lambda^{B_x} \longrightarrow H^1_x(Y,\Lambda)$$

la composée de c'_x (resp. γ'_x) avec la projection canonique $\Lambda^{B_x} \longrightarrow \Lambda(x)$ (1.1.1). Notons $i : \{x\} \longrightarrow Y_{(x)}$, $j : U_x = Y_{(x)} - \{x\} \longrightarrow Y_{(x)}$ les inclusions, et $\pi : \widetilde{Y}_{(x)} \longrightarrow Y_{(x)}$ la projection de la normalisée. Si l'on identifie Λ^{B_x} à $H^0(U_x,\Lambda)$ de la façon évidente, δ_x est un opérateur bord dans la suite exacte de cohomologie associée au triangle distingué

$$(*) \qquad i_*Ri^!\Lambda \longrightarrow \Lambda \longrightarrow Rj_*j^*\Lambda \longrightarrow$$

(cf. (1.3.4), (1.6.6)). D'autre part, γ'_x est un opérateur bord dans la suite exacte de cohomologie associée au triangle distingué

$$(**) \qquad i_*Ri^!\Lambda \longrightarrow \pi_*\pi^*i_*Ri^!\Lambda \longrightarrow \Lambda(x) \longrightarrow,$$

variante de (2.3.1). Or (*) et (**) s'insèrent dans un diagramme des neuf (où $\pi_*\Lambda = \Lambda^{B_x}$)

$$\begin{array}{ccccc}
i_*Ri^!\Lambda & \longrightarrow & \Lambda & \longrightarrow & Rj_*j^*\Lambda \\
\downarrow & & \downarrow & & \| \\
\pi_*\pi^*i_*Ri^!\Lambda & \longrightarrow & \pi_*\Lambda & \longrightarrow & Rj_*j^*\Lambda \\
\downarrow & & \downarrow & & \downarrow \\
\Lambda(x) & = & \Lambda(x) & \longrightarrow & 0.
\end{array}$$

Les opérateur ∂_x et δ_x qui s'en déduisent sont donc opposés (1.5.4).

2.5. Soit

$$\gamma : H^1(X_{\overline{\eta}}, \Lambda)(1)\ (= H^1(Y, R\Psi\Lambda)(1)) \longrightarrow M \otimes \Lambda \tag{2.5.1}$$

la transposée de la flèche composée de γ' (2.3.5) et de la flèche canonique de $H^1(Y, \Lambda)$ dans $H^1(Y, R\Psi\Lambda)$. Comme les flèches c et c' figurant dans (2.2.1) et (2.2.2) sont transposées, il résulte de 2.4 que

$$\gamma = -c. \tag{2.5.2}$$

2.6. Rappelons maintenant la définition de **l'accouplement de monodromie** u_ℓ envisagé par Grothendieck dans (SGA 7 IX 9.1.2). Posons, comme en (SGA 7 IX 2.5.3),

$$\begin{aligned}
&U = T_\ell(A_{\overline{\eta}}) \otimes \Lambda = H^1(X_{\overline{\eta}}, \Lambda)(1) \\
&V = U^I = \text{partie fixe de } U \\
&W = \text{partie torique de } U = T_\ell(T) \otimes \Lambda.
\end{aligned} \tag{2.6.1}$$

Rappelons que les quotients successifs de la filtration $U \supset V \supset W$ sont libres sur Λ et que, pour l'accouplement canonique

$$U \otimes U(-1) \longrightarrow \Lambda, \quad (a, b) \longmapsto Tr(ab),$$

on a le **théorème d'orthogonalité** (SGA 7 IX 2.5.2)

$$V^\perp = W, \tag{2.6.2}$$

d'où

$$(U/V)^\vee = W(-1). \tag{2.6.3}$$

Considérons, comme dans (SGA 7 IX 9.2), la factorisation naturelle

$$\begin{array}{ccc} U & \twoheadrightarrow & U/V \\ {\scriptstyle N}\downarrow & & \downarrow \\ U(-1) & \hookrightarrow & W(-1) \end{array} \tag{2.6.4}$$

de N (défini par (1.7.3)). Les flèches horizontales de ce carré sont transposées. Lorsqu'on identifie $W(-1)$ à $M^\vee \otimes \Lambda$ par (2.3.4), l'inclusion $W(-1) \hookrightarrow U(-1)$ est donnée par la flèche γ' de (2.3.5) (plus précisément est composée de γ' et de l'inclusion de $H^1(Y, \Lambda)$ dans $H^1(Y, R\Psi\Lambda) = U$). Dualement, la projection $U \longrightarrow U/V$ s'identifie alors à γ (2.5.1), et le carré (2.6.4) se récrit

$$\begin{array}{ccc} U & \overset{\gamma}{\twoheadrightarrow} & M \otimes \Lambda \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle \varphi_*} \\ U(-1) & \overset{\gamma'}{\hookrightarrow} & M^\vee \otimes \Lambda \end{array} \tag{2.6.5}$$

La flèche φ_* correspond à un accouplement

$$\varphi : (M \otimes \Lambda) \otimes (M \otimes \Lambda) \longrightarrow \Lambda. \tag{2.6.6}$$

Pour $\Lambda = \mathbb{Z}_\ell$, φ est l'accouplement noté u_ℓ par Grothendieck dans (SGA 7 IX 2.5.3). Comme $\gamma = -c$ (2.5.2) et $\gamma' = -c'$ (2.4), la commutativité de (2.2.3) et (2.6.5) entraîne :

THÉORÈME 2.7. — *Avec les notations* (2.1.3) *et* (2.6.6), *on a*

$$\varphi = u \otimes \Lambda.$$

C'est, avec le signe opposé, la partie relative à ℓ du résultat de Grothendieck (SGA 7 IX 9.1.2).

Remarque 2.8 : La formule d'orthogonalité (2.6.2) résulte immédiatement de (2.2.3) et (2.4). En effet, par définition $U^I = \mathrm{Ker}\, N$. Donc, par (2.2.3) (et l'injectivité de $u_* \otimes \Lambda$), $U^I = \mathrm{Ker}\, c$. Mais, d'après (2.4), $Im\ c' = W(-1)$. Donc, comme c et c' sont transposées, $\mathrm{Ker}\, c$ est l'orthogonal de $W(-1)$. Notons aussi que, d'après (1.6.1), on a

$$U^I = H^1(Y, \Lambda)(1).$$

Remarque 2.9 : On a $N^2 = 0$, et la filtration $(U \supset V \supset W) \otimes \mathbb{Q}$ est la **filtration de monodromie** de $U \otimes \mathbb{Q}$, caractérisée par $N(U \otimes \mathbb{Q}) \subset W(-1) \otimes \mathbb{Q}$, $N(V \otimes \mathbb{Q}) = 0$, et $N : (U/V) \otimes \mathbb{Q} \xrightarrow{\sim} W(-1) \otimes \mathbb{Q}$, cf. [2, 1.6, 1.7]. Le logarithme N de la partie unipotente de la monodromie et la filtration de monodromie sont définis plus généralement pour tout $\overline{\mathbb{Q}}_\ell$-représentation $\rho : I \longrightarrow GL(H)$ dont la restriction à un sous-groupe d'indice fini I_1 de I est unipotente. Un accouplement $H' \otimes H'' \longrightarrow \overline{\mathbb{Q}}_\ell$ donne lieu à un accouplement entre les gradués associés pour les filtrations de monodromie correspondantes. Changeant les notations de § 0, supposons en particulier que X soit un schéma propre et plat sur S, de fibre générique lisse, de dimension relative n, et prenons $H = H^n(X_{\overline{\eta}}, \overline{\mathbb{Q}}_\ell)$. D'après le théorème de monodromie locale, la représentation H de I est quasi-unipotente, i.e. vérifie la condition ci-dessus (SGA 7 I 1.3). La filtration de monodromie, centrée en n,

$$H = M_{2n}H \supset \cdots \supset M_nH \supset \cdots M_0H \supset M_{-1}H = 0,$$

est dans l'intervalle $[0, 2n]$, N envoie M_i dans $M_{i-2}(-1)$, et $N^i : gr^M_{n+i}H \xrightarrow{\sim} gr^M_{n-i}H(-i)$. De plus, la dualité de Poincaré

$$H \otimes H \longrightarrow \overline{\mathbb{Q}}_\ell(-n), \quad (a, b) \longmapsto < a, b > := Tr(ab)$$

permet d'identifier $gr^M_{n-i}H(-n)$ au dual de $gr^M_{n+i}H$. En particulier, pour $i = n$, on trouve un accouplement

$$u_n : gr^M_{2n}H \otimes gr^M_{2n}H \longrightarrow \overline{\mathbb{Q}}_\ell, \quad (a, b) \longmapsto < a, N^n b >, \tag{2.9.1}$$

qui généralise l'accouplement (2.1.3). Cet accouplement est symétrique : en effet,

$$\begin{aligned} < a, N^n b > &= (-1)^n < N^n a, b > \quad \text{(par [2, 1.6.9])} \\ &= < b, N^n a > . \end{aligned}$$

On peut se demander s'il provient d'un accouplement défini sur $\mathbb{Q}$ (voire sur $\mathbb{Z}$) et ayant une propriété de positivité (ou négativité, suivant les conventions···) analogue à celle satisfaite par (2.1.3). J'ignore ce qu'il en est en général.

Dans le cas semi-stable, on peut toutefois préciser la question. Supposons que X soit régulier, et que la fibre spéciale Y soit un diviseur à croisements normaux réduit, somme de diviseurs lisses. Grâce à Rapoport-Zink [3], on dispose alors d'une suite spectrale "de Steenbrink" (cf. [6])

$$E_1^{ij} = H^{i+j}(Y, gr_{-i}^W R\Psi \mathbb{Q}_\ell) \Longrightarrow H^*(X_{\overline{\eta}}, \mathbb{Q}_\ell), \tag{2.9.2}$$

où

$$E_1^{-r,q+r} = \bigoplus_{\substack{k\geq 0\\ k\geq -r}} H^{q-r-2k}(Y^{(r+2k+1)}, \mathbb{Q}_\ell(-r-k)),$$

$Y^{(m)}$ désignant la somme disjointe des intersections m à m des composantes de Y. Cette suite spectrale dégénère en E_2 si S est localisé strict d'une courbe lisse sur un corps fini (pour des raisons de poids, grâce à la conjecture de Weil [1], [2]), ou si S est localisé strict d'une courbe lisse sur un corps de caractéristique nulle (grâce à Steenbrink [6]), et il est plausible qu'elle dégénère en E_2 sans hypothèse supplémentaire. On conjecture de plus que la filtration aboutissement est la filtration de monodromie. C'est le cas si $n \leq 2$ ([3, 2.13]), ou si S est localisé strict d'une courbe lisse sur un corps fini (d'après Deligne [2, 1.8, 3.3.1]). C'est aussi le cas si S est localisé strict d'une courbe lisse sur un corps de caractéristique nulle et X est projectif sur S, d'après Steenbrink [6, 5.9] (dont l'argument est corrigé par Saito dans [4]).

Admettons que (2.9.2) dégénère en E_2 et que la filtration aboutissement soit la filtration de monodromie. Il est alors facile de décrire $gr_{2n}H$ et $N^n : gr_{2n}H \xrightarrow{\sim} gr_0 H(-n)$. On a (en degré total n)

$$\begin{aligned} W_{2n}E_1 = E_1^{-n,2n} &= H^0(Y^{(n+1)}, \mathbb{Q}_\ell(-n)), \\ W_0 E_1 = E_1^{n,0} \quad &= H^0(Y^{(n+1)}, \mathbb{Q}_\ell), \end{aligned}$$

d'où

$$gr_{2n}H = W_{2n}E_2 = \mathrm{Ker}(H^0(Y^{(n+1)}, \mathbb{Q}_\ell(-n)) \xrightarrow{d_*} H^2(Y^{(n)}, \mathbb{Q}_\ell(-n+1)))$$

$$gr_0 H \ = W_0 E_2 \ = \mathrm{Coker}\ (H^0(Y^{(n)}, \mathbb{Q}_\ell) \xrightarrow{d^*} H^0(Y^{(n+1)}, \mathbb{Q}_\ell)),$$

où d^* (resp. d_*) est une somme alternée d'homomorphismes de Gysin (resp. de restriction). Les opérateurs d_* et d^* ont des descriptions combinatoires simples, qui permettent de définir sur $gr_{2n}H(n)$ et $gr_0 H$ une $\mathbb{Z}$-structure naturelle. Il est plausible que l'accouplement u_n (2.9.1) provienne par extension des scalaires à $\overline{\mathbb{Q}}_\ell$ de la restriction à un sous-réseau de la forme quadratique $\pm\Sigma_{\alpha\in A} x^2$ sur $\mathbb{Z}^A$, où $A = Y^{(n+1)}(k)$. C'est ce qui est suggéré par l'analogue transcendant [6].

BIBLIOGRAPHIE

[1] P. Deligne. — La conjecture de Weil I, Pub. IHES 43, (1974), 273-307.

[2] P. Deligne. — La conjecture de Weil II, Pub. IHES 52, (1980), 137-252.

[3] M. Rapoport et Th. Zink. — Uber die lokale Zetafunktion von Shimuravarietäten, Monodromiefiltration und verschwindende Zyklen in ungleicher Charakteristik, Inv. Math. 68, (1982), 21-101.

[4] M. Saito. — Modules de Hodge polarisables, Pub. RIMS 553, (1986).

[5] T. Saito. — Vanishing cycles and geometry of curves over a discrete valuation ring, Amer. J. of Math., 109, (1987), 1043-1085.

[6] J. Steenbrink. — Limits of Hodge structures, Inv. Math. 31, (1976), 229-257.

[SGA 7] Groupes de monodromie en géométrie algébrique, Séminaire de Géométrie Algébrique du Bois-Marie 67-69, I par A. Grothendieck, SLN 288, (1972), II par P. Deligne et N. Katz, SLN 340, (1973).

L. ILLUSIE
Université de Paris-Sud
Arithmétique et Géométrie
Algébrique (URA D 0752)
Bâtiment 425
91405 ORSAY CEDEX

UNIFORMISATION P-ADIQUE DES COURBES DE SHIMURA : LES THÉORÈMES DE ČEREDNIK ET DE DRINFELD

J.-F. BOUTOT et H. CARAYOL

Table des matières

S.M.F.
Astérisque 196-197 (1991)

III. Le théorème de Čerednik-Drinfeld

Introduction

Soit Δ une algèbre de quaternions indéfinie de centre $\mathbf{Q}$. Il lui correspond un système projectif, indexé par les sous-groupes compacts ouverts U de $\Delta(\mathbf{A}_f)^*$, de *courbes de Shimura* S_U : ce sont des courbes algébriques (complètes si Δ est un corps gauche), définies sur $\mathbf{Q}$, dont les composantes connexes absolues sont définies sur des extensions cyclotomiques de $\mathbf{Q}$. L'exemple le plus connu d'une telle situation est le cas où Δ est déployée : les courbes obtenues alors sont les habituelles courbes modulaires. On a étudié depuis longtemps la réduction modulo p de ces dernières, et l'on sait bien que la nature de cette réduction dépend de l'exposant en p du niveau, c'est-à-dire de la composante U_p en p du sous-groupe U (supposant pour simplifier que celui-ci se décompose en un produit) : en particulier — prenant U assez petit pour éviter quelques problèmes techniques liés à la non-représentabilité — notre courbe a bonne réduction en p si U_p est maximal, c'est-à-dire si p ne divise pas le niveau. On renvoie à [De-Ra] et [K-M] pour l'étude de la mauvaise réduction, dans les cas où U_p n'est pas maximal : cette réduction est décrite en termes d'un problème de modules (où interviennent les fameuses bases de Drinfeld), lequel permet en particulier l'étude de la fibre spéciale et de la singularité obtenue. Dans le cas d'une algèbre Δ plus générale, *en une place p où Δ est déployée*, la situation est formellement isomorphe à celle rencontrée dans le cas des courbes modulaires : la courbe de Shimura a bonne réduction lorsque U_p est maximal, et les cas de mauvaise réduction sont décrits de façon analogue au cas modulaire; tout cela se généralise même au cadre plus général des courbes associées à des algèbres de quaternions sur des corps totalement réels ([Ca 1]).

Toute autre est la situation que l'on rencontre *en une place p où l'algèbre Δ est ramifiée* : dans ce cas, supposant que U_p est *maximal*, Čerednik a

découvert que la courbe de Shimura S_U admettait en p une *uniformisation p-adique*, c'est-à-dire que $S_U \otimes \mathbf{Q}_p$ était la réunion de (formes tordues galoisiennes de) *quotients à la Mumford* du "demi-plan p-adique" par des sous-groupes de Schottky de $PGL(2, \mathbf{Q}_p)$; ces derniers sous-groupes sont liés à l'algèbre $\overline{\Delta}$ déduite de Δ en échangeant les invariants locaux aux places p et ∞ (i.e. $\overline{\Delta}$ est définie et déployée en p). On peut ensuite, si besoin est, utiliser cette uniformisation pour décrire la fibre spéciale en p, laquelle apparaît donc comme le quotient par un groupe fini d'un graphe de droites projectives (cette fibre est en général singulière).

Čerednik a obtenu son résultat par une habile méthode indirecte, dont le principe est de considérer a priori la courbe de Mumford, et de la comparer à la courbe de Shimura en étudiant de part et d'autre l'action du groupe fondamental : cette méthode, qui repose sur des travaux antérieurs d'Ihara, est proche — ce qui ne saurait surprendre — de celle utilisée par Kazhdan pour traiter de la conjugaison des variétés de Shimura.

Deligne et Kazhdan ont vite remarqué que le résultat de Čerednik laissait soupçonner l'existence d'une famille universelle de *groupes formels* sur le "demi-plan" rigide - analytique $\Omega_{\mathbf{Q}_p} = \mathbf{P}^1(\widehat{\overline{\mathbf{Q}}}_p) - \mathbf{P}^1(\mathbf{Q}_p)$; c'est là le théorème fondamental que Drinfeld a alors su démontrer : de manière un peu plus précise, il a prouvé que $\widehat{\Omega}_{\mathbf{Q}_p} \widehat{\otimes} \widehat{\mathbf{Z}}_p^{nr}$ — où $\widehat{\Omega}_{\mathbf{Q}_p}$ est un schéma formel sur $\mathbf{Z}_p$ dont $\Omega_{\mathbf{Q}_p}$ est la fibre générique — paramétrait une famille de groupes formels, de dimension 2 et de hauteur 4, munis d'une action de l'ordre maximal du corps de quaternions D de centre $\mathbf{Q}_p$, et d'une "rigidification". Le théorème local de Drinfeld est d'ailleurs valide aussi bien en dimension supérieure (où $\Omega_{\mathbf{Q}_p}$ est remplacé par $\mathbf{P}^{n-1}(\widehat{\overline{\mathbf{Q}}}_p)$ privé de tous ses hyperplans rationnels : on obtient alors un espace de modules pour des groupes formels de dimension n et de hauteur n^2, munis d'une action de l'ordre maximal du corps gauche d'invariant 1/n), ainsi que pour les $\Omega_K = \mathbf{P}^1(\widehat{\overline{K}}) - \mathbf{P}^1(K)$ (où K est un corps local non archimédien) et leurs analogues en dimension supérieure. La méthode utilisée par Drinfeld pour démontrer son théorème repose sur la théorie de Dieudonné-Cartier : elle consiste à effectuer d'ingénieuses constructions algébriques sur les modules de Dieudonné des groupes formels considérés, leur associant de cette façon des structures que l'on sait (d'après Deligne) être représentables par le schéma formel $\widehat{\Omega}_{\mathbf{Q}_p} \widehat{\otimes} \widehat{\mathbf{Z}}_p^{nr}$, puis à montrer que l'on obtient ainsi un isomorphisme de foncteurs.

Une fois prouvé le théorème local, Drinfeld parvient assez facilement à en déduire le résultat originel de Čerednik : on sait en effet que S_U paramétrise une famille de variétés abéliennes, dont il compare les complétés formels aux groupes formels classifiés par $\widehat{\Omega}_{\mathbf{Q}_p} \widehat{\otimes} \widehat{\mathbf{Z}}_p^{nr}$. Le théorème de Drin-

feld révèle donc, en quelque sorte, la structure profonde du résultat de Čerednik. Outre cela, ce théorème local permet de définir naturellement un système projectif de revêtements étales Σ_n de $\Omega_{\mathbb{Q}_p} \otimes \mathbb{Q}_p^{nr}$: ces revêtements, un peu mystérieux, permettent d'uniformiser p-adiquement les courbes S_U en une place p où Δ est ramifiée et où U_p n'est pas maximal, une situation qui n'était pas abordable par les méthodes originelles de Čerednik. On peut également appliquer le théorème local à d'autres cas que celui des courbes de Shimura sur $\mathbb{Q}$, et obtenir d'autres résultats d'uniformisation p-adique : par exemple, uniformiser les courbes de Shimura définies sur des corps totalement réels (cas d'ailleurs déjà traité dans l'article de Čerednik) ; les spécialistes du sujet savent en principe comment le faire, mais nul à notre connaissance ne l'a encore écrit. De même, Rapoport et Zink savent, partant du théorème local en dimension supérieure, uniformiser des variétés de Shimura associées à certains groupes unitaires. Signalons enfin que Drinfeld sait uniformiser ses "Modules elliptiques II" par les revêtements Σ_n.

Drinfeld a exposé son théorème dans un très bref article ([Dr 2]), très concentré et difficilement abordable ; notre but ici est d'expliquer la méthode qu'il utilise, et de donner des démonstrations détaillées. Le présent travail est divisé en trois chapitres bien distincts. Le premier traite du demi-plan non archimédien, de ses différents aspects (rigide-analytique ou formel), des divers problèmes de modules qu'il représente. Le second chapitre constitue à la fois le coeur et la partie la plus substantielle de cet article : le théorème local y est énoncé et prouvé. L'essentiel de la méthode utilisée par Drinfeld dans cette preuve nous a été expliqué par Thomas Zink, qui nous a fait à Strasbourg de nombreux exposés sur le sujet. Notre dette à son égard est difficilement estimable : nous lui exprimons ici tous nos remerciements, dans l'espoir que notre rédaction le satisfasse. Après avoir longtemps hésité, nous avons fait le choix, peut-être discutable, de ne rédiger ce théorème local que dans le cas du "demi-plan", c'est-à-dire en dimension 1 (sur un corps p-adique arbitraire, toutefois) ; ce choix nous permet de raccourcir quelque peu nos diagrammes, et de mieux expliciter les différents cas qui se présentent (toutefois les idées nécessaires à la démonstration en dimension supérieure sont pour l'essentiel similaires). Le troisième et dernier chapitre enfin traite de la situation globale : nous y énonçons, commentons et prouvons le théorème de Čerednik (dans le cas où le corps de base est $\mathbb{Q}$).

Chapitre I : Le "demi-plan" non archimédien.

Soient K un corps local non archimédien et C le complété de la clôture algébrique de K. Le "demi-plan" non archimédien Ω sur K est défini ensemblistement par $\Omega = \mathbf{P}^1(C) - \mathbf{P}^1(K)$.

Nous rappelons tout d'abord au §1 la construction de l'arbre I associé à $PGL(2,K)$ [Se] et de sa réalisation géométrique $I_{\mathbb{R}}$. Puis (§2) nous définissons une application $\lambda : \Omega \to I_{\mathbb{R}}$ qui permet de décrire la structure d'espace analytique rigide, au sens de Tate [Ta 1], de Ω par recollement des images réciproques par λ des arêtes de l'arbre. Cette description donnée par Drinfeld [Dr 1] a été reprise en détail (en dimension quelconque) par Deligne et Husemöller [De-Hu]. Pour les bases de la géométrie analytique rigide, on peut consulter [B-G-R] et [Fr-VdP].

Nous définissons ensuite (§3) un modèle formel, au sens de Raynaud [Ra 1], de l'espace analytique rigide Ω. C'est un schéma formel $\widehat{\Omega}$ au-dessus de l'anneau des entiers de K que nous construisons également par recollement de schémas formels $\widehat{\Omega}_{[s,s']}$ correspondants aux arêtes [s,s'] de l'arbre I. Ce modèle formel fut introduit par Mumford [Mu 2] dans son article sur l'analogue non archimédien de l'uniformisation de Schottky des surfaces de Riemann.

Le §4 explique la description fonctorielle donnée par Deligne (non publié) des schémas formels $\widehat{\Omega}_{[s,s']}$ en terme des réseaux adjacents correspondants aux sommets s et s' de I. Par recollement de ces réseaux en des faisceaux constructibles, on obtient au §5 la description fonctorielle de $\widehat{\Omega}$ qu'utilise Drinfeld [Dr 2]. On trouvera un autre compte-rendu de cette description dans l'article récemment paru de Teitelbaum [Te].

Pour clore ce chapitre (§6), nous décrivons l'action du groupe $PGL(2,K)$ sur le schéma formel $\widehat{\Omega}$ et sur le foncteur correspondant.

1. L'immeuble de $PGL(2,K)$.

(1.0) Soient K un corps local non archimédien, $\mathcal{O}$ l'anneau des entiers de K et π une uniformisante de $\mathcal{O}$. Soient $k = \mathcal{O}/\pi\mathcal{O}$ le corps résiduel,

p la caractéristique de k et q son ordre. On note C le complété de la clôture algébrique de K et $|\ |$ la norme sur C normalisée par $|\pi| = q^{-1}$. La valuation v est donnée par : $v(x) = \log_q |x|$.

(1.1) Un *réseau* M de K^2 est un sous-$\mathcal{O}$-module libre de rang 2 de K^2. Deux réseaux M et M' sont homothétiques s'il existe $\lambda \in K^*$ tel que $M' = \lambda M$. On note S l'ensemble des classes d'homothétie de réseaux et [M] la classe d'un réseau dans S.

L'immeuble de $PGL(2, K)$ est le graphe I dont S est l'ensemble des sommets et tel que $s = [M]$ est joint par une arête à s' s'il existe un représentant M' de s' tel que $\pi M \subsetneqq M' \subsetneqq M$. Ainsi I est un arbre dont chaque sommet a $q+1$ voisins : les arêtes issues du sommet $s = [M]$ sont en bijection avec les droites de $M/\pi M$, autrement dit avec $\mathbf{P}^1(k)$.

(1.2) Les points de la réalisation géométrique $I_{\mathbf{R}}$ de I s'identifient aux classes de proportionnalité de *normes* sur le K-espace vectoriel K^2 (*cf.* [G-Iw]) :

a) A un sommet $s = [M]$ correspond la classe de la norme $|\ |_M$ dont la boule unité est M. Si (e_1, e_2) est une base de M et si $v = a_1 e_1 + a_2 e_2$, on a

$$|v|_M = \sup\{|a_1|, |a_2|\}.$$

b) Si s et s' sont deux sommets adjacents et si $s = [M]$ et $s' = [M']$, avec $\pi M \subset M' \subset M$, il existe une base (e_1, e_2) de M telle que $(e_1, \pi e_2)$ soit une base de M'. Pour $v = a_1 e_1 + a_2 e_2$, on a

$$|v|_M = \sup\{|a_1|, |a_2|\},$$
$$|v|_{M'} = \sup\{|a_1|, q|a_2|\}.$$

A un point $x = (1-t)s + ts'$, $0 < t < 1$, situé sur l'arête joignant s ets' correspond la classe de la norme $|\ |_t$ définie par

$$|v|_t = \sup\{|a_1|, q^t |a_2|\}.$$

On a

$$M = \{v \in K^2, |v|_t \leq \lambda\} \text{ pour } q^t \leq \lambda < q,$$
$$M' = \{v \in K^2, |v|_t \leq \lambda\} \text{ pour } 1 \leq \lambda < q^t.$$

c) Réciproquement soit $|\ |$ une norme sur K^2. Pour λ réel > 0, l'ensemble $M_\lambda = \{v \in K^2, |v| \leq \lambda\}$ est un réseau de K^2. On a $M_{\lambda'} \subset M_\lambda$ si $\lambda' \leq \lambda$ et $M_{q^{-1}\lambda} = \pi M_\lambda$, donc $[M_\lambda]$ prend au plus deux valeurs dans S lorsque λ varie.

Si $[M_\lambda] = s$ est constant, c'est que $|\ |$ correspond à s.

Sinon $[M_\lambda] = s$ ou s' pour deux sommets adjacents s et s'. Quitte à remplacer la norme $|\ |$ par une norme proportionnelle, on a $[M_\lambda] = s$ pour $q^t \leq \lambda < q$ et $[M_\lambda] = s'$ pour $1 \leq \lambda < q^t$, avec $0 < t < 1$. Alors $|\ |$ correspond au point $x = (1-t)s + ts'$ de l'arête joignant s et s'.

2. L'espace analytique rigide Ω.

(2.1) On notera $\Omega = \mathbf{P}^1(C) - \mathbf{P}^1(K)$. Si l'on identifie $\mathbf{P}^1(C)$ à l'ensemble des classes de C^*-homothétie d'applications K-linéaires non nulles de K^2 dans C, $\mathbf{P}^1(K)$ correspond aux applications de K-rang un. Ainsi Ω s'identifie à l'ensemble des classes de C^*-homothétie d'applications K-linéaires *injectives* de K^2 dans C.

(2.2) En composant une application K-linéaire injective $z : K^2 \to C$ avec la norme sur C, on obtient une norme $|\ |_z$ sur K^2 :

$$|v|_z = |z(v)| \qquad \text{pour} \qquad v \in K^2.$$

Ceci définit une application $\lambda : \Omega \to I_{\mathbb{R}}$

$$\lambda\ (\text{classe de } z) = \textit{classe de } |\ |_z.$$

On peut vérifier que l'image de λ est $I_{\mathbb{Q}}$.

(2.3) Soient $s = [M]$ et $s' = [M']$ deux sommets adjacents de I et (e_1, e_2) une base de M telle que $(e_1, \pi e_2)$ soit une base de M'. Identifions Ω à $C - K$ en choisissant pour représentant d'un point de Ω l'application z telle que $z(e_2) = 1$ et $z(e_1) = \zeta \in C - K$. Alors on a

$$\lambda^{-1}(s) = \{\zeta \in C, |\zeta| \leq 1\} - \bigcup_{\substack{a \in \mathcal{O} \\ \bmod \pi\mathcal{O}}} \{\zeta \in C, |\zeta - a| < 1\},$$

$$\lambda^{-1}(x) = \{\zeta \in C, |\zeta| = q^{-t}\} \text{ si } x = (1-t)s + ts', 0 < t < 1,$$

$$\lambda^{-1}(s') = \{\zeta \in C, |\zeta| \leq q^{-1}\} - \bigcup_{\substack{b \in \pi\mathcal{O} \\ \bmod \pi^2\mathcal{O}}} \{\zeta \in C, |\zeta - b| < q^{-1}\},$$

$$\lambda^{-1}([s, s']) = \{\zeta \in C, |\zeta| \leq 1\} - \bigcup_{\substack{a \in \mathcal{O} - \pi\mathcal{O} \\ \bmod \pi\mathcal{O}}} \{\zeta \in C, |\zeta - a| < 1\}$$
$$- \bigcup_{\substack{b \in \pi\mathcal{O} \\ \bmod \pi^2\mathcal{O}}} \{\zeta \in C, |\zeta - b| < q^{-1}\}.$$

Autrement dit $\lambda^{-1}(s)$ [resp. $\lambda^{-1}(s')$] est le disque fermé de rayon 1 [resp. q^{-1}] centré en 0 privé des q disques ouverts de rayon 1 [resp. q^{-1}] à

centres K-rationnels qu'il contient, tandis que $\lambda^{-1}(]s, s'[)$ est la couronne ouverte de petit rayon q^{-1} et grand rayon 1 centrée en 0.

Démonstration. — Les normes $|\ |_z = |\zeta a_1 + a_2|$ et $|\ |_t = \sup\{|a_1|, q^t|a_2|\}$ sont proportionnelles sur K^2 si et seulement si $|\ |_z = q^{-t}|\ |_t$. Cette égalité est satisfaite si et seulement si elle l'est pour $a_1 = 1$, c'est-à-dire si

$$(*) \qquad |\zeta + a_2| = \sup\{q^{-t}, |a_2|\} \text{ pour } a_2 \in K.$$

Si $0 < t < 1$, on a $|a_2| \neq q^{-t}$ pour tout $a_2 \in K$, donc $(*)$ équivaut à $|\zeta| = q^{-t}$.

Par contre si $t = 0$, $(*)$ équivaut à $|\zeta| = 1$ et $|\zeta + a_2| = 1$ pour tout $a_2 \in K$ tel que $|a_2| = 1$, ou encore $|\zeta| \leq 1$ et $|\zeta - a| \geq 1$ pour $a \in \mathcal{O}$.

De même si $t = 1$, $(*)$ équivaut à $|\zeta| = q^{-1}$ et $|\zeta + a_2| = q^{-1}$ pour tout $a_2 \in K$ tel que $|a_2| = q^{-1}$, ou encore $|\zeta| \leq q^{-1}$ et $|\zeta - b| \geq q^{-1}$ pour $b \in \pi\mathcal{O}$.

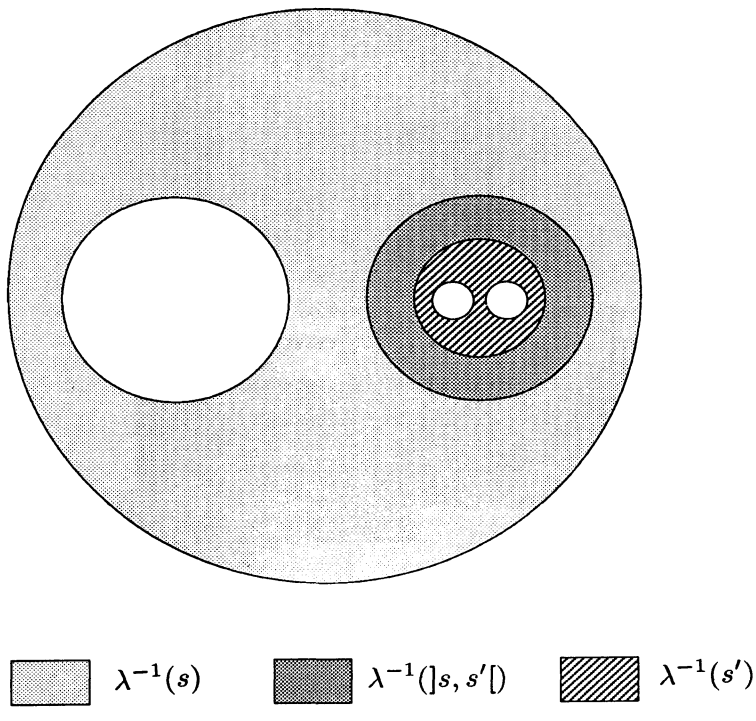


Figure 1 : $\lambda^{-1}([s, s'])$, $q = 2$.

(2.4) Les ensembles $\lambda^{-1}(s)$, $\lambda^{-1}(s')$ et $\lambda^{-1}([s,s'])$ ont des structures naturelles d'espaces analytiques rigides définis sur K ; ce sont des sous-ensembles affinoïdes connexes de $\mathbf{P}^1_K$, c'est-à-dire les complémentaires dans $\mathbf{P}^1_K$ d'un nombre fini de disques ouverts. De plus $\lambda^{-1}(s)$ et $\lambda^{-1}(s')$ sont des ouverts de $\lambda^{-1}([s,s'])$.

Plus généralement, si T est un sous-arbre fini de I, $\lambda^{-1}(T)$ est un sous-ensemble affinoïde connexe de $\mathbf{P}^1_K$; il est obtenu par recollement suivant la relation d'incidence définie par T des $\lambda^{-1}([s,s'])$ en les $\lambda^{-1}(s)$, pour $[s,s']$ arête de T et s sommet intérieur de T.

Ainsi $\Omega = \bigcup \lambda^{-1}(T)$, pour T sous-arbres finis de I, est muni d'une structure naturelle d'*espace analytique rigide* défini sur K ; c'est un sous-espace analytique connexe de $\mathbf{P}^1_K$.

(2.5) D'aucuns aiment s'imaginer intuitivement Ω comme le bord d'un voisinage tubulaire de $I_{\mathbb{R}}$.

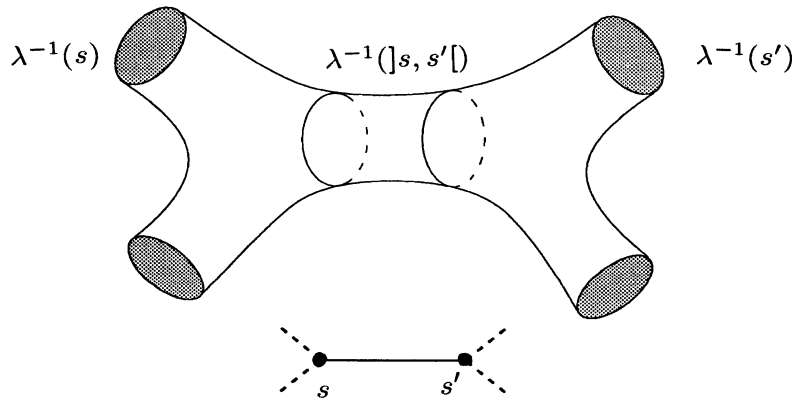


Figure 2.

3. Le schéma formel $\widehat{\Omega}$.

(3.1) Si M est un réseau de K^2, la fibre générique de la droite projective $\mathbb{P}(M)$ au-dessus de $\mathcal{O}$ est canoniquement identifiée à $\mathbf{P}^1_K$. De plus, si M_1 est un réseau homothétique, l'homothétie de M à M_1 définit un unique $\mathcal{O}$-isomorphisme entre $\mathbb{P}(M)$ et $\mathbb{P}(M_1)$ induisant l'identité sur les fibres génériques. Il est donc légitime de noter $\mathbb{P}_s$, où $s = [M]$ est le sommet de I correspondant à M, cette droite projective au-dessus de $\mathcal{O}$ munie de l'identification de sa fibre générique à $\mathbf{P}^1_K$.

Les points de $\lambda^{-1}(s)$ sont exactement ceux des points de $\mathbf{P}^1_K(C)$ qui ne se spécialisent pas en un point k-rationnel de la fibre spéciale de $\mathbf{P}_s$. On notera Ω_s l'ouvert de $\mathbf{P}_s$ complémentaire des points rationnels de la fibre spéciale et $\widehat{\Omega}_s$ le schéma formel complété de Ω_s le long de la fibre spéciale. Les bijections canonique $\mathbf{P}^1_K(C) = \mathbf{P}_s(\mathcal{O}_C) = \widehat{\mathbf{P}}_s(\mathcal{O}_C)$ induisent une bijection $\lambda^{-1}(s) = \widehat{\Omega}_s(\mathcal{O}_C)$; plus précisément l'espace analytique rigide $\lambda^{-1}(s)$ est la fibre générique (au sens de Raynaud) du schéma formel $\widehat{\Omega}_s$. S'agissant d'un schéma formel affine, cela veut simplement dire que l'algèbre de Tate correspondant à $\lambda^{-1}(s)$ est $\Gamma(\widehat{\Omega}_s) \otimes_{\mathcal{O}} K$.

(3.2) Un sommet s' de I adjacent à s définit un point k-rationnel de la fibre spéciale de $\mathbf{P}_s$: si $s = [M]$ et $s' = [M']$ avec $\pi M \subset M' \subset M$, ce point est défini par l'application $M \to M/M' \simeq k$. Le $\mathcal{O}$-schéma $\mathbf{P}_{[s,s']}$ obtenu par éclatement de $\mathbf{P}_s$ en ce point est également l'éclaté de $\mathbf{P}_{s'}$, en le point défini par s. Sa fibre générique, identique à celle de $\mathbf{P}_s$ et $\mathbf{P}_{s'}$, est canoniquement identifiée à $\mathbf{P}^1_K$.

On notera $\Omega_{[s,s']}$ l'ouvert de $\mathbf{P}_{[s,s']}$ complémentaire des points rationnels de la fibre spéciale à l'exception du point singulier et $\widehat{\Omega}_{[s,s']}$ le complété formel de $\Omega_{[s,s']}$ le long de la fibre spéciale. L'identification de la fibre générique de $\mathbf{P}_{[s,s']}$ avec $\mathbf{P}^1_K$ induit une bijection $\lambda^{-1}([s,s']) = \widehat{\Omega}_{[s,s']}(\mathcal{O}_C)$; en particulier les points de la couronne $\lambda^{-1}(]s,s'[)$ sont ceux qui se spécialisent au point singulier de la fibre spéciale de $\mathbf{P}_{[s,s']}$. En effet, en reprenant les notations de (2.3), les coordonnées naturelles le long des deux composantes de la fibre spéciale sont ζ et ζ/π (modulo l'idéal maximal), le point singulier correspondant sur l'une à l'annulation de la réduction de ζ, et sur l'autre au fait que ζ/π admet pour réduction ∞.

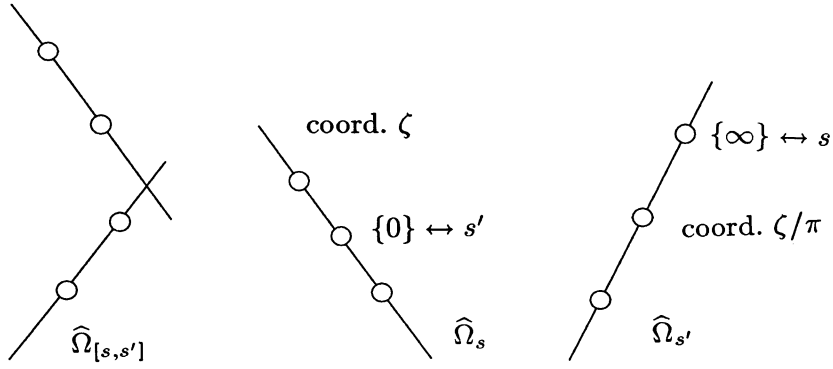


Figure 3.

On peut ici encore dire plus précisément que l'espace analytique rigide

$\lambda^{-1}([s,s'])$ est la fibre générique du schéma formel $\widehat{\Omega}_{[s,s']}$. De plus les applications canoniques induisent des immersions ouvertes de $\widehat{\Omega}_s$ et $\widehat{\Omega}_{s'}$ dans $\widehat{\Omega}_{[s,s']}$ correspondant sur les fibres génériques (ou sur les points à valeur dans $\mathcal{O}_C$) aux inclusions de $\lambda^{-1}(s)$ et $\lambda^{-1}(s')$ dans $\lambda^{-1}([s,s'])$.

(3.3) Plus généralement, si T est un sous-arbre fini de I, on obtient, par recollement suivant la relation d'incidence définie par T des schémas formels $\widehat{\Omega}_{[s,s']}$ en les $\widehat{\Omega}_s$ pour $[s,s']$ arête de T et s sommet intérieur de T, un schéma formel $\widehat{\Omega}_T$ dont la fibre générique est canoniquement identifiée à $\lambda^{-1}(T)$.

Si $T \subset T'$, l'immersion ouverte $\widehat{\Omega}_T \subset \widehat{\Omega}_{T'}$ induit sur les fibres génériques l'inclusion $\lambda^{-1}(T) \subset \lambda^{-1}(T')$. On construit ainsi un schéma formel $\widehat{\Omega} = \bigcup_T \widehat{\Omega}_T$ dont la fibre générique est Ω; en particulier on a $\widehat{\Omega}(\mathcal{O}_C) = \Omega$. La fibre spéciale de $\widehat{\Omega}$ est un arbre de droites projectives sur k se coupant en leurs points k-rationnels, dual de l'arbre I.

4. Le foncteur $\widehat{\Omega}$ à la Deligne.

Nous décrivons, en suivant Deligne, les foncteurs sur la catégorie *Compl* des $\mathcal{O}$-algèbres séparées complètes pour la topologie π-adique qui sont représentés par les schémas formels $\widehat{\Omega}_s$ et $\widehat{\Omega}_{[s,s']}$.

(4.1) DÉFINITION. — *On note F_s le foncteur qui, à $R \in \mathrm{Ob}$ Compl, associe l'ensemble des classes d'isomorphie de couples $(\mathcal{L}, \alpha)$, où $\mathcal{L}$ est un R-module libre de rang un et $\alpha : M \to \mathcal{L}$ un homomorphisme de $\mathcal{O}$-modules vérifiant la condition :*

$$(*) \begin{cases} \text{pour tout } x \in \mathrm{Spec}(R/\pi R), \text{ l'application} \\ \alpha(x) : M/\pi M \to \mathcal{L} \otimes_R k(x) \text{ est injective.} \end{cases}$$

(4.2) PROPOSITION. — *Le foncteur F_s est représenté par le schéma formel $\widehat{\Omega}_s$.*

Démonstration. — La condition sur α implique que $\alpha(u)$ est un générateur de $\mathcal{L}$ pour tout $u \in M - \pi M$, en particulier l'application $\alpha \otimes \mathrm{id}_R : M \otimes_{\mathcal{O}} R \to \mathcal{L}$ est surjective. Ainsi F_s est un sous-foncteur du foncteur $\widehat{\mathbf{P}}_s$: droite projective formelle sur $\mathcal{O}$ définie par $s = [M]$.

Pour décrire ce sous-foncteur, choisissons une base (e_1, e_2) de M, ce qui détermine un repère projectif $\{0, 1, \infty\}$ de $\widehat{\mathbf{P}}_s$. Le couple $(\mathcal{L}, \alpha)$ est déterminé à isomorphisme près par le rapport $\alpha(e_1)/\alpha(e_2) = \zeta \in R$. Ainsi F_s s'identifie à un sous-foncteur de la droite affine formelle $\widehat{\mathbf{P}}_s - \{\infty\}$.

La condition sur α s'exprime en terme de l'image $\overline{\zeta}$ de ζ dans $R/\pi R$: quel que soit $a \in k$, $\overline{\zeta} - a$ ne s'annule en aucun point de $\mathrm{Spec}(R/\pi R)$, autrement dit $\overline{\zeta} - a$ est inversible dans $R/\pi R$. Ainsi F_s est le sous-foncteur de $\widehat{\mathbf{P}}_s - \{\infty\}$ qui représente l'ouvert complémentaire des points k-rationnels de la fibre spéciale, c'est-à-dire $\widehat{\Omega}_s$.

(4.3) DÉFINITION. — *On note $F_{[s,s']}$ le foncteur qui, à $R \in \mathrm{Ob}\,Compl$, associe l'ensemble des classes d'isomorphie de diagrammes commutatifs :*

$$\begin{array}{ccccc} \pi M & \hookrightarrow & M' & \hookrightarrow & M \\ \downarrow{\scriptstyle \alpha/\pi} & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} \\ \mathcal{L} & \xrightarrow{c} & \mathcal{L}' & \xrightarrow{c'} & \mathcal{L} \end{array}$$

où $\mathcal{L}$ et $\mathcal{L}'$ sont des R-modules libres de rang un, α et α' des homomorphismes de $\mathcal{O}$-modules, c et c' des homomorphismes de R-modules, vérifiant la condition :

$$(*) \quad \begin{cases} \textit{pour tout } x \in \mathrm{Spec}(R/\pi R), \textit{ on a} \\ \mathrm{Ker}\{\alpha(x) : M/\pi M \to \mathcal{L} \otimes_R k(x)\} \subset M'/\pi M \\ \mathrm{Ker}\{\alpha'(x) : M'/\pi M' \to \mathcal{L}' \otimes_R k(x)\} \subset \pi M/\pi M'. \end{cases}$$

(4.4) PROPOSITION. — *Le foncteur $F_{[s,s']}$ est représenté par le schéma formel $\widehat{\Omega}_{[s,s']}$.*

Démonstration. — Soit (e_1, e_2) une base de M telle que $(e_1, \pi e_2)$ soit une base de M'. La condition $(*)$ implique que $\alpha(e_2)$ engendre $\mathcal{L}$ et $\alpha'(e_1)$ engendre $\mathcal{L}'$. Identifions $\mathcal{L}$ avec R en posant $\alpha(e_2) = 1$ et $\mathcal{L}'$ avec R en posant $\alpha'(e_1) = 1$. Soient $\zeta = \alpha(e_1)$ et $\eta = \alpha'(\pi e_2)$. La commutativité du diagramme entraîne $c = \eta$, $c' = \zeta$ et $\zeta\eta = \pi$.

Ainsi le choix de (e_1, e_2) permet d'identifier $F_{[s,s']}$ à un sous-foncteur du schéma formel $\mathrm{Spf}(\mathcal{O}\{\zeta, \eta\}/\zeta\eta - \pi)$. Ce même choix identifie $\mathrm{Spf}(\mathcal{O}\{\zeta, \eta\}/\zeta\eta - \pi)$ à l'ouvert de $\widehat{\mathbf{P}}_{[s,s']}$ complémentaire des points à l'infini $\overline{\zeta} = \infty$ et $\overline{\eta} = \infty$ des deux composantes de la fibre spéciale.

La condition $(*)$ s'exprime en termes des images $\overline{\zeta}$ et $\overline{\eta}$ de ζ et η dans $R/\pi R$: quel que soit $a \in k - \{0\}$, $\overline{\zeta} - a$ et $\overline{\eta} - a$ sont inversibles dans $R/\pi R$. Ainsi $F_{[s,s']}$ est le sous-foncteur de $\widehat{\mathbf{P}}_{[s,s']} - (\{\overline{\zeta} = \infty\} \cup \{\overline{\eta} = \infty\})$ qui représente l'ouvert complémentaire des points k-rationnels des deux

composantes de la fibre spéciale $\mathrm{Spec}(k[\overline{\zeta},\overline{\eta}]/\overline{\zeta}\overline{\eta})$ à l'exception du point singulier $\overline{\zeta}=\overline{\eta}=0$, c'est-à-dire $\widehat{\Omega}_{[s,s']}$.

(4.5) L'immersion ouverte $\widehat{\Omega}_s \hookrightarrow \widehat{\Omega}_{[s,s']}$ est, avec les identifications faites ci-dessus, la restriction de l'immersion ouverte $\mathrm{Spf}(\mathcal{O}\{\zeta,\zeta^{-1}\}) \hookrightarrow \mathrm{Spf}(\mathcal{O}\{\zeta,\eta\}/\zeta\eta-\pi)$. Fonctoriellement, la flèche $F_s \to F_{[s,s']}$ définie en associant à $\alpha : M \to \mathcal{L}$ le diagramme commutatif

$$\begin{array}{ccccc} \pi M & \hookrightarrow & M' & \hookrightarrow & M \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \alpha} \\ \mathcal{L} & \xrightarrow{\pi} & \mathcal{L} & \xrightarrow{\mathrm{id}} & \mathcal{L} \end{array}$$

identifie F_s au sous-foncteur de $F_{[s,s']}$ consistant en les diagrammes où c' est inversible.

De même l'immersion ouverte $\widehat{\Omega}_{s'} \hookrightarrow \widehat{\Omega}_{[s,s']}$ est la restriction de l'immersion $\mathrm{Spf}(\mathcal{O}\{\eta,\eta^{-1}\}) \hookrightarrow \mathrm{Spf}(\mathcal{O}\{\zeta,\eta\}/\zeta\eta-\pi)$. Fonctoriellement, en associant à $\alpha' : M' \to \mathcal{L}'$ le diagramme commutatif

$$\begin{array}{ccccc} \pi M & \hookrightarrow & M' & \hookrightarrow & M \\ \downarrow & & \downarrow{\scriptstyle \alpha'} & & \downarrow \\ \mathcal{L}' & \xrightarrow{\mathrm{id}} & \mathcal{L}' & \xrightarrow{\pi} & \mathcal{L}' \end{array}$$

on identifie $F_{s'}$ au sous-foncteur de $F_{[s,s']}$ consistant en les diagrammes où c est inversible.

5. Le foncteur $\widehat{\Omega}$ à la Drinfeld.

Au moyen des foncteurs F_s et $F_{[s,s']}$ ci-dessus définis, on obtient donc une description "modulaire" de chacun des ouverts affines $\widehat{\Omega}_s$ et $\widehat{\Omega}_{[s,s']}$ qui composent le schéma formel $\widehat{\Omega}$. La variante due à Drinfeld, que nous allons maintenant exposer, permet de décrire directement $\widehat{\Omega}$ au moyen d'un unique foncteur F défini sur la catégorie $Nilp$ des $\mathcal{O}$-algèbres où l'image de π est nilpotente.

Si B est une $\mathcal{O}$-algèbre, nous noterons $B[\Pi]$ le quotient de l'algèbre de polynômes $B[X]$ par l'idéal engendré par $X^2-\pi$: c'est donc un B-module libre de rang 2, engendré par 1 et un élément Π (l'image de X), qui vérifie $\Pi^2=\pi$. L'algèbre $B[\Pi]$ est munie d'une graduation à valeurs dans $\mathbb{Z}/2\mathbb{Z}$, telle que les éléments de B soient de degré 0, et Π de degré 1.

5.1 DÉFINITION. — *Soit $B \in \mathrm{Ob}\, Nilp$, et $S = \mathrm{Spec}\, B$. On définit $F(B)$ – parfois aussi noté $F(S)$ – comme l'ensemble des classes d'isomorphie de quadruplets (η, T, u, r) constitués comme suit :*

(i) *η est un faisceau en $\mathcal{O}[\Pi]$-modules plats, $(\mathbb{Z}/2\mathbb{Z})$-gradué, constructible, sur S muni de la topologie de Zariski.*

(ii) *T est un faisceau en $\mathcal{O}_S[\Pi]$ modules, $(\mathbb{Z}/2\mathbb{Z})$-gradué, tel que les composantes homogènes T_0, T_1 soient des faisceaux inversibles sur S.*

(iii) *u est un homomorphisme $\mathcal{O}[\Pi]$-linéaire de degré 0 de η vers T, tel que $u \otimes_{\mathcal{O}} \mathcal{O}_S : \eta \otimes_{\mathcal{O}} \mathcal{O}_S \to T$ soit surjectif.*

(iv) r est un isomorphisme K-linéaire du faisceau constant $\underline{K}^2$ vers le faisceau $\eta_0 \otimes_{\mathcal{O}} K$.

Ces données sont de plus astreintes à vérifier les conditions suivantes :

[C1] *Notons $S_i \subset S$ le lieu d'annulation du morphisme $\Pi : T_i \to T_{i+1}$ $(i = 0, 1)$; alors la restriction $\eta_i | S_i$ est un faisceau constant de fibre isomorphe à $\mathcal{O}^2$.*

[C2] *Pour tout point géométrique x de S, notons $T(x) = T \otimes_B k(x)$; alors l'application $\eta_x / \Pi\eta_x \to T(x)/\Pi T(x)$ induite par u est injective.*

[C3] $(\bigwedge^2 \eta_i)_{|S_i} = \pi^{-i}(\bigwedge^2(\Pi^i r \underline{\mathcal{O}}^2))_{|S_i}$ *(pour $i = 0, 1$).*

Complétons cette définition par quelques remarques :

(a) Il est clair que la définition ci-dessus de $F(S)$ vaut non seulement pour S affine, mais aussi pour tout $\mathcal{O}$-schéma S où l'image de π est nilpotente (i.e. un $(\mathcal{O}/\pi^n\mathcal{O})$-schéma).

(b) De la platitude de η comme $\mathcal{O}[\Pi]$-module, et de l'existence de r, on déduit que les composantes homogènes η_0 et η_1 sont des faisceaux en $\mathcal{O}$-modules plats dont toutes les fibres sont (libres) de rang 2. L'action de Π définit des applications injectives $\cdots \eta_0 \xrightarrow{\Pi} \eta_1 \xrightarrow{\Pi} \eta_0 \longrightarrow \cdots$, de composé $\Pi^2 = \pi$.

(c) La donnée du triplet (η, T, u) revient à la donnée d'un diagramme commutatif et périodique de période 2 :

$$\begin{array}{ccccccc} \cdots & \eta_0 & \longrightarrow & \eta_1 & \longrightarrow & \eta_0 & \cdots \\ & \downarrow{\scriptstyle u_0} & & \downarrow{\scriptstyle u_1} & & \downarrow{\scriptstyle u_0} & \\ \cdots & T_0 & \longrightarrow & T_1 & \longrightarrow & T_0 & \cdots \end{array}$$

(d) Utilisant r, on définit comme suit des sous-faisceaux N_0 et N_1 du

faisceau constant $\underline{K}_S^2$:

$$N_0 = r^{-1}\eta_0$$
$$N_1 = r^{-1}(\Pi \otimes \mathbb{Q})^{-1}(\eta_1) = \pi^{-1}r^{-1}(\Pi(\eta_1)).$$

Ce sont des sous-faisceaux en $\mathcal{O}$-modules de rang maximal (des "réseaux") isomorphes respectivement à η_0 et η_1. En chaque point géométrique x de S, on a les inclusions :

$$N_{0,x} \subset N_{1,x} \subset \pi^{-1}N_{0,x} \subset K^2,$$

d'où un simplexe (sommet ou arête) de l'arbre. Plus précisément, on voit en utilisant la condition [C2] que :

– Si $\Pi|T_0(x)$ est inversible, alors $N_{0,x} = N_{1,x}$. De plus la condition de normalisation [C3] nous donne : $\bigwedge^2 N_{1,x} = \pi^{-1}\bigwedge^2(\mathcal{O}^2)$.

– Si $\Pi|T_1(x)$ est inversible, alors $N_{1,x} = \pi^{-1}N_{0,x}$. D'après [C3] on a dans ce cas : $\bigwedge^2 N_{0,x} = \bigwedge^2(\mathcal{O}^2)$.

– Il reste le cas où $\Pi|T_0(x)$ et $\Pi|T_1(x)$ sont toutes deux nulles. On trouve alors (utilisant la surjectivité des $u_i \otimes_{\mathcal{O}} \mathcal{O}_S$) qu'on obtient une arête $[N_{0,x} \subsetneq N_{1,x} \subsetneq \pi^{-1}N_{0,x}]$, avec :

$$\bigwedge^2 N_{0,x} = \bigwedge^2(\mathcal{O}^2) \text{ et } \bigwedge^2 N_{1,x} = \pi^{-1}\bigwedge^2(\mathcal{O}^2).$$

(5.2) Notre but est de prouver la :

PROPOSITION. — *Le foncteur F est représentable par le schéma formel $\widehat{\Omega}$.*

Pour cela, nous allons définir pour chaque sommet s (resp. pour chaque arête $[s, s']$) un morphisme de foncteurs $F_s \to F$ (resp. $F_{[s,s']} \to F$), de façon compatible aux recollements, c'est-à-dire aux morphismes d'immersions ouvertes $F_s \hookrightarrow F_{[s,s']}$ et $F_{s'} \hookrightarrow F_{[s,s']}$. D'où un morphisme de foncteurs $\widehat{\Omega} \to F$, dont nous montrerons ensuite qu'il est un isomorphisme.

Commençons par remarquer que tout sommet s de l'arbre peut être représenté par un réseau $M \subset K^2$ tel que l'on ait ou bien $\bigwedge^2 M = \bigwedge^2(\mathcal{O}^2)$, ou bien $\bigwedge^2 M = \pi^{-1}\bigwedge^2(\mathcal{O}^2)$; un tel représentant M est unique, et les deux possibilités s'excluent mutuellement : cela définit une partition dans l'ensemble des sommets, entre sommets pairs (représentés par M vérifiant $\bigwedge^2 M = \bigwedge^2(\mathcal{O}^2)$) et sommets impairs (admettant un représentant M tel que $\bigwedge^2 M = \pi^{-1}\bigwedge^2(\mathcal{O}^2)$). Noter qu'un sommet voisin d'un sommet pair

(resp. impair) est impair (resp. pair). Nous supposerons toujours dans la suite les représentants M des sommets choisis de manière à vérifier $\bigwedge^2 M = \bigwedge^2(\mathcal{O}^2)$ ou $\pi^{-1}\bigwedge^2(\mathcal{O}^2)$. De même, nous orienterons toujours les arêtes $[s, s']$ de sorte que s soit impair et s' pair : d'où deux réseaux M et M' qui vérifient : $\bigwedge^2 M = \pi^{-1}\bigwedge^2(\mathcal{O}^2), \bigwedge^2 M' = \bigwedge^2(\mathcal{O}^2)$, et $\pi M \subset M' \subset M$.

(5.3) Le plus simple est de définir les morphismes $F_s \to F$. Distinguons deux cas, suivant que s est pair ou impair :

5.3.1. — *Définition de $F_s \to F$ pour $s = [M]$ impair.* $[\bigwedge^2 M = \pi^{-1}\bigwedge^2 \mathcal{O}^2]$.

La donnée d'un point de $F_s(B)$ correspond à la donnée d'un faisceau inversible $\mathcal{L}$ sur $S = \operatorname{Spec} B$ et d'un morphisme $\alpha : M \to \mathcal{L}$, $\mathcal{O}$-linéaire, tel que l'application $\alpha(x) : M/\pi M \to \mathcal{L} \otimes_B k(x)$ soit injective en chaque point x de S.

On fait alors correspondre à ce point le point de $F(B)$ défini par le diagramme suivant :

$$\begin{array}{ccccc} \eta_0 = \underline{M} & \xrightarrow{\Pi=\mathrm{id}} & \eta_1 = \underline{M} & \xrightarrow{\Pi=\pi} & \eta_0 = \underline{M} \\ \downarrow{\scriptstyle u_0=\alpha} & & \downarrow{\scriptstyle u_1=\alpha} & & \downarrow{\scriptstyle u_0=\alpha} \\ T_0 = \mathcal{L} & \xrightarrow{\Pi=\mathrm{id}} & T_1 = \mathcal{L} & \xrightarrow{\Pi=\pi} & T_0 = \mathcal{L} \end{array}$$

et par l'isomorphisme $r : \underline{K}^2 \xrightarrow{\sim} \underline{M} \otimes K$ qui correspond à l'inclusion $M \hookrightarrow K^2$. Il est immédiat de constater que toutes les conditions de la définition (5.1) sont satisfaites.

5.3.2. — *Définition de $F_{s'} \to F$ pour $s' = [M']$ pair* ($\bigwedge^2 M' = \bigwedge^2(\mathcal{O}^2)$).

A un point de $F_{s'}(B)$, représenté par $\alpha' : M' \to \mathcal{L}'$, on associe maintenant le point de $F(B)$ défini par le diagramme :

$$\begin{array}{ccccc} \eta_0 = \underline{M'} & \xrightarrow{\Pi=\pi} & \eta_1 = \underline{M'} & \xrightarrow{\Pi=\mathrm{id}} & \eta_0 = \underline{M'} \\ \downarrow{\scriptstyle u_0=\alpha'} & & \downarrow{\scriptstyle u_1=\alpha'} & & \downarrow{\scriptstyle u_0=\alpha'} \\ T_0 = \mathcal{L}' & \xrightarrow{\Pi=\pi} & T_1 = \mathcal{L}' & \xrightarrow{\Pi=\mathrm{id}} & T_0 = \mathcal{L}' \end{array}$$

et par l'isomorphisme $r : \underline{K}^2 \xrightarrow{\sim} \underline{M'} \otimes K$ qui correspond à l'inclusion $M' \hookrightarrow K^2$.

(5.4) *Le cas d'une arête.*

Il nous reste à définir $F_{[s,s']} \to F$ pour une arête $[s, s']$. Supposons l'orientation, et des représentants M et M' choisis comme expliqué en (5.2). La donnée d'un point de $F_{[s,s']}(R)$ correspond à la donnée d'une classe d'isomorphie de diagrammes commutatifs vérifiant les conditions (*) de (4.3) :

$$\begin{array}{ccccc} \pi M & \hookrightarrow & M' & \hookrightarrow & M \\ \downarrow{\scriptstyle \alpha/\pi} & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} \\ \mathcal{L} & \xrightarrow{c} & \mathcal{L}' & \xrightarrow{c'} & \mathcal{L}. \end{array}$$

On voit que $S = \operatorname{Spec} R$ est la réunion de deux fermés S_0 et S_1, où S_0 (resp. S_1) est le lieu des points où c' (resp. c) s'annule. Notons $\mathcal{U} \subset S_1$ [resp. $\mathcal{U}' \subset S_0$] l'ouvert où c' (resp. c) est inversible.

Sur $\mathcal{U}$, le point de $F_{[s,s']}$ que nous considérons provient du point de F_s défini par $\alpha : M \to \mathcal{L}$. La construction (5.3.1) lui associe alors le point suivant de $F(\mathcal{U})$:

$$\begin{array}{ccccc} \underline{M} & \xrightarrow{\mathrm{id}} & \underline{M} & \xrightarrow{\pi} & \underline{M} \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\ \mathcal{L} & \xrightarrow[\mathrm{id}]{} & \mathcal{L} & \xrightarrow[\pi]{} & \mathcal{L}, \end{array}$$

r défini par l'inclusion $M \hookrightarrow K^2$.

Ou, ce qui revient au même en utilisant l'isomorphisme $c' : \mathcal{L}' \xrightarrow{\sim} \mathcal{L}$, le point défini par le diagramme :

$$\begin{array}{ccccc} \underline{M} & \xrightarrow{\mathrm{id}} & \underline{M} & \xrightarrow{\pi} & \underline{M} \\ \downarrow{\scriptstyle (c')^{-1}\alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle (c')^{-1}\alpha} \\ \mathcal{L}' & \xrightarrow[c']{\sim} & \mathcal{L} & \xrightarrow[c]{} & \mathcal{L}', \end{array} \qquad (*)$$

Noter que $(c')^{-1}\alpha$ est un prolongement à M de la flèche $\alpha' : M' \to \mathcal{L}'$ (il n'est défini qu'au-dessus de $\mathcal{U}$).

De même, au-dessus de $\mathcal{U}'$, le point considéré correspond au point de $F_{s'}$ défini par $\alpha' : M' \to \mathcal{L}'$. On doit alors lui associer le point de $F(\mathcal{U}')$ défini par :

$$\begin{array}{ccccc} \underline{M'} & \xrightarrow{\pi} & \underline{M'} & \xrightarrow{\mathrm{id}} & \underline{M'} \\ {\scriptstyle\alpha'}\downarrow & & {\scriptstyle\alpha'}\downarrow & & {\scriptstyle\alpha'}\downarrow \\ \mathcal{L}' & \xrightarrow[\pi]{} & \mathcal{L}' & \xrightarrow[\mathrm{id}]{} & \mathcal{L}' \end{array}$$

(avec r défini par l'inclusion $M' \hookrightarrow K^2$).

Soit encore (utilisant $c : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$) :

$$\begin{array}{ccccc} \underline{M'} & \xrightarrow{\pi} & \underline{M'} & \xrightarrow{\mathrm{id}} & \underline{M'} \\ {\scriptstyle\alpha'}\downarrow & & {\scriptstyle c^{-1}\alpha'}\downarrow & & {\scriptstyle\alpha'}\downarrow \\ \mathcal{L}' & \xrightarrow[c']{} & \mathcal{L} & \xrightarrow[c]{\sim} & \mathcal{L}' \end{array} \qquad (**)$$

où $c^{-1}\alpha'$ prolonge à M' la flèche $\alpha/\pi : \pi M \longrightarrow \mathcal{L}$.

Enfin, le complémentaire de la réunion $\mathcal{U} \cup \mathcal{U}'$ est égal à l'intersection $J = S_0 \cap S_1$. On vérifie immédiatement qu'on peut définir un point de $F(J)$ par le diagramme :

$$\begin{array}{ccccc} \underline{M'} & \hookrightarrow & \underline{M} & \xrightarrow{\pi} & \underline{M'} \\ {\scriptstyle\alpha'}\downarrow & & {\scriptstyle\alpha}\downarrow & & {\scriptstyle\alpha'}\downarrow \\ \mathcal{L}' & \xrightarrow[c']{} & \mathcal{L} & \xrightarrow[c]{} & \mathcal{L}' \end{array} \qquad (***)$$

avec r correspondant encore à l'inclusion $M' \hookrightarrow K^2$.

Nous avons ainsi trois points de F à valeurs respectivement dans les schémas $\mathcal{U}$, $\mathcal{U}'$, et J, et décrits par les trois diagrammes $(*)$ $(**)$ et $(***)$ ci-dessus. Il nous faut maintenant expliquer comment ils se recollent en un point (η, T, u, r) de $F(S)$.

Le plus simple à définir est T : On prendra sur S tout entier $T_0 = \mathcal{L}'$, $T_1 = \mathcal{L}$, les morphismes Π étant donnés par c' et c.

Passons ensuite à la définition du faisceau η : Partons du faisceau sur la réunion disjointe $S_0 \coprod S_1$, qui est constant de valeur M sur S_1 et constant de valeur M' sur S_0. Son image directe par le morphisme $S_0 \coprod S_1 \to S$, que nous notons ϕ, est telle que sa restriction à J soit constante de valeur $M \oplus M'$. Nous définissons alors le faisceau η_0 (resp. η_1) comme le sous-faisceau des sections de ϕ qui, au-dessus de J, sont à valeurs dans le sous-module M', plongé dans $M \oplus M'$ par l'application $m' \to (m', m')$ (resp. dans le sous-module M, plongé par $m \to (m, \pi m)$). Les morphismes $\Pi : \eta_0 \to \eta_1$ et $\eta_1 \to \eta_0$ s'obtiennent par restriction à partir des morphismes de ϕ dans ϕ définis respectivement par :

$$\begin{cases} M \xrightarrow{\text{id}} M \\ M' \xrightarrow{\pi} M' \end{cases} \quad \text{et} \quad \begin{cases} M \xrightarrow{\pi} M \\ M' \xrightarrow{\text{id}} M'. \end{cases}$$

Si l'on préfère, la définition de η est résumée par le diagramme suivant :

$$\begin{array}{lccccc} & \eta_0 & \xrightarrow{\Pi} & \eta_1 & \xrightarrow{\Pi} & \eta_0 \\ \text{restriction à } \mathcal{U} : & M & \xrightarrow{\text{id}} & M & \xrightarrow{\pi} & M \\ S_1 & \uparrow & & \uparrow{\scriptstyle \text{id}} & & \uparrow \\ \text{restriction à } J : & M' & \hookrightarrow & M & \xrightarrow{\pi} & M' \\ S_0 & \downarrow{\scriptstyle \text{id}} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \text{id}} \\ \text{restriction à } \mathcal{U}' : & M' & \xrightarrow{\pi} & M' & \xrightarrow{\text{id}} & M' \end{array}$$

On notera en particulier que $\eta_0|S_0$ est constant de valeur M' et que $\eta_1|S_1$ est constant de valeur M.

L'isomorphisme $r : \underline{K}^2 \xrightarrow{\sim} \eta_0 \otimes_{\mathcal{O}} K$ est celui défini par les inclusions (compatibles) de M et M' dans K^2.

Enfin, le morphisme u_0 est donné par α' sur $S_0 = \mathcal{U}' \cup J$ et par $(c')^{-1}\alpha$ sur $\mathcal{U}$. De même, u_1 est égal à α sur $S_1 = \mathcal{U} \cup J$ et à $c^{-1}\alpha'$ sur $\mathcal{U}'$.

Il est bien clair que nous avons ainsi construit un point (η, T, u, r) de $F(S)$, d'où le morphisme $F_{[s,s']} \to F$ cherché. De plus, notre construction

met en évidence le fait que ces morphismes se recollent suivant les morphismes $F_s \to F$ et $F_{s'} \to F$ définis en (5.3).

D'où un morphisme de foncteurs : $\widehat{\Omega} \to F$.

(5.5) Il nous reste à voir qu'on a ainsi obtenu un *isomorphisme* de foncteurs : autrement dit, qu'un point arbitrairement donné de $F(R)$ provient toujours d'un (unique) point de $\widehat{\Omega}(R)$.

Supposons donc fixé un tel point $(\eta, T, u, r) \in F(R)$. On associe alors à chaque arête $[s, s']$ de l'arbre, que l'on peut supposer représentée par deux réseaux M et M' vérifiant $\pi M \subsetneq M' \subsetneq M$ et les conventions de (5.2), un sous-ensemble $S_{[s,s']}$ de $S = \operatorname{Spec} R$ défini comme suit : c'est le lieu des points x où sont vérifiées, avec les notations de la remarque (d) de (5.1), les inclusions :

$$M' \subset N_{0,x} \quad \text{et} \quad M \subset N_{1,x}.$$

Si l'on préfère distinguer les cas, en utilisant toujours cette remarque, cela revient à :

$$\begin{cases} \text{cas où } \Pi | T_0(x) \text{ est inversible : } N_{0,x} = N_{1,x} = M \\ \text{cas où } \Pi | T_1(x) \text{ est inversible : } N_{0,x} = \pi N_{1,x} = M' \\ \text{cas où aucun n'est inversible : } N_{0,x} = M', N_{1,x} = M. \end{cases}$$

Vérifions que $S_{[s,s']}$ est un ouvert de Zariski de S : Il suffit pour cela de vérifier que les intersections $S_{[s,s']} \cap S_0$ et $S_{[s,s']} \cap S_1$ sont des ouverts de Zariski, respectivement dans S_0 et S_1. L'intersection $S_{[s,s']} \cap S_0$ est le lieu des points de S_0 qui vérifient :

$$N_{0,x} = M' \quad \text{et} \quad N_{1,x} = M \quad \text{ou} \quad \pi^{-1} M'.$$

Or le faisceau η_0 est constant sur S_0, et donc N_0 est localement constant. La première condition définit donc un sous-ensemble à la fois ouvert et fermé $\mathcal{A} \subset S_0$. Sur l'ouvert de $\mathcal{A}$ où $\Pi | T_1$ est inversible, on a alors automatiquement $N_{1,x} = \pi^{-1} M'$. Autrement dit, le complémentaire de $S_{[s,s']} \cap S_0$ dans $\mathcal{A}$ est contenu dans $S_0 \cap S_1$. Ce complémentaire est défini dans $S_0 \cap S_1$ par la condition $N_{1,x} \neq M$, laquelle est fermée (aussi bien, d'ailleurs, qu'ouverte) car le faisceau $N_{1,x}$ est localement constant sur S_1.

Il en résulte que $S_0 \cap S_{[s,s']}$ est ouvert dans S_0 ; on vérifie de même que $S_1 \cap S_{[s,s']}$ est ouvert dans S_1. Et donc $S_{[s,s']}$ est ouvert dans S.

Utilisant toujours la remarque (d) de (5.1), on voit que *les $S_{[s,s']}$ recouvrent S*. Si $[s, s']$ et $[s, s'']$ sont deux arêtes distinctes d'intersection

s, alors $S_{[s,s']} \cap S_{[s,s'']}$ est l'ouvert S_s, lieu des points qui vérifient $N_{0,x} = N_{1,x} = M$; on remarquera que S_s peut aussi être défini dans $S_{[s,s']}$ ou dans $S_{[s,s'']}$ par la condition : $\Pi|T_0(x)$ inversible. De même, pour deux arêtes $[s,s']$ et $[s'',s']$ d'intersection s', l'intersection $S_{[s,s']} \cap S_{[s'',s']}$ est l'ouvert $S_{s'}$ "constitué" des points x qui vérifient $N_{0,x} = \pi N_{1,x} = M'$, et qui peut aussi être défini dans $S_{[s,s']}$ ou dans $S_{[s'',s']}$ par la condition : $\Pi|T_1(x)$ inversible.

Le diagramme composé suivant définit un point du foncteur $F_{[s,s']}$ à valeurs dans $S_{[s,s']}$:

$$\begin{array}{ccccc}
\pi M & \hookrightarrow & M' & \hookrightarrow & M \\
\downarrow & & \downarrow & & \downarrow \\
\pi N_1 & \hookrightarrow & N_0 & \hookrightarrow & N_1 \\
\downarrow \iota & & r \downarrow \iota & & \downarrow \iota \\
\eta_1 & \xrightarrow{\Pi} & \eta_0 & \xrightarrow{\Pi} & \eta_1 \\
u_1 \downarrow & & u_0 \downarrow & & u_1 \downarrow \\
T_1 & \xrightarrow{\Pi} & T_0 & \xrightarrow{\Pi} & T_1
\end{array}$$

Il est clair que les points ainsi obtenus se recollent : Sur S_s par exemple, on obtient le point du foncteur F_s défini par le composé $M = N_1 \xrightarrow{\sim} \eta_1 \longrightarrow T_1$. On obtient donc par ce recollement un point de $\widehat{\Omega}(R)$, et il est facile de vérifier qu'il a pour image le point initial (η, T, u, r). On vérifie également sans peine que c'est le seul antécédent possible.

6. Action du groupe $PGL(2,K)$.

(6.1) Le groupe $GL(2,K)$ agit naturellement, via son quotient $PGL(2,K)$, sur l'arbre I : un élément $g \in GL(2,K)$ transforme le sommet $[M]$ (resp. l'arête $[[M],[M']]$) en le sommet $[gM]$ (resp. l'arête $[[gM],[gM']]$).

On a d'autre part une action évidente de ce même groupe $PGL(2,K)$ sur l'ensemble $\Omega = \mathbf{P}^1(C) - \mathbf{P}^1(K)$. Il est clair que l'application $\lambda : \Omega \to I_{\mathbb{R}}$ est équivariante, d'où il résulte que le groupe opère en fait par automorphismes de la structure rigide-analytique de Ω : cette action permute les différents ouverts affinoïdes définis au §2. On voit sans peine que toutes

les constructions des §§1–4 sont équivariantes, et que notre action provient d'une action sur le schéma formel $\widehat{\Omega}$. Cette dernière admet une évidente description en termes des foncteurs à la Deligne : pour $s = [M]$ et $gs = [gM]$, on a un morphisme de foncteurs :

$$g : F_s \to F_{gs},$$

donné par : $g \cdot (\mathcal{L}, \alpha) = (\mathcal{L}, \beta)$, où β désigne le composé $gM \xrightarrow{g^{-1}}_{\sim} M \xrightarrow{\alpha} \mathcal{L}$. De même, pour $s' = [M']$ tel que $[s, s']$ constitue une arête, le morphisme $g : F_{[s,s']} \to F_{[gs,gs']}$ est donné par : $g \cdot (\mathcal{L}, \mathcal{L}', c, c', \alpha, \alpha') = (\mathcal{L}, \mathcal{L}', c, c', \alpha \circ g^{-1}, \alpha' \circ g^{-1})$.

Il est un peu moins évident d'exprimer cette action de $PGL(2, K)$ sur $\widehat{\Omega}$ en termes du foncteur F à la Drinfeld. Une telle description est fournie par la proposition suivante :

(6.2) PROPOSITION. — *L'action d'un élément g de $GL(2, K)$ sur le foncteur F est donnée par la formule suivante :*

$$g \cdot (\eta, T, u, r) = (\eta[n], T[n], u[n], \Pi^n \circ r \circ g^{-1}),$$

où n désigne la valuation de $\det(g)$, *et $[n]$ le décalage de n (modulo 2) de la graduation de (η, T, u).*

Remarquer que le décalage effectué assure que la condition de normalisation [C3] de la définition (5.1) est satisfaite pour l'image. En effet, notons r_1 le composé :

$$r_1 : \underline{K}^2 \xrightarrow{g^{-1}} \underline{K}^2 \xrightarrow{r} \eta_0 \otimes_{\mathcal{O}} K \xrightarrow{\Pi^n} \eta[n]_0 \otimes_{\mathcal{O}} K.$$

Le lieu d'annulation du morphisme $\Pi : T[n]_i \to T[n]_{i+1}$ est $S_{i'}$, avec $i' \equiv i + n \pmod 2$, au-dessus duquel on a :

$$\begin{aligned} \bigwedge^2 \eta[n]_i = \bigwedge^2 \eta_{i'} &= \pi^{-i'}\left(\bigwedge^2 (\Pi^{i'} r \underline{\mathcal{O}}^2)\right) = \\ &= \pi^{-i-n} \bigwedge^2 (\Pi^{i+n} r \underline{\mathcal{O}}^2) = \\ &= \pi^{-i} \bigwedge^2 (\Pi^{i+n} r g^{-1} \underline{\mathcal{O}}^2) = \pi^{-i} \bigwedge^2 (\Pi^i r_1 \underline{\mathcal{O}}^2). \end{aligned}$$

Il est clair alors que la formule de la proposition définit bien un morphisme de F dans lui-même. Pour montrer que c'est bien celui que

nous voulons, vérifions par exemple que, pour $s = [M]$ et $g \in GL(2, K)$, le diagramme suivant est commutatif :

$$\begin{array}{ccc} F_s(B) & \longrightarrow & F(B) \\ \Big\downarrow{\scriptstyle g} & & \Big\downarrow{\scriptstyle g} \\ F_{gs}(B) & \longrightarrow & F(B) \end{array}$$

(cette vérification sera d'ailleurs suffisante, car la réunion des images des F_s constitue un ouvert dense).

Partant de $(\mathcal{L}, \alpha) \in F_s(B)$, on a : $g \cdot (\mathcal{L}, \alpha) = (\mathcal{L}, \alpha \circ g^{-1})$. On peut exprimer dans une même formule les deux cas (5.3.1) et (5.3.2) : l'image de $(\mathcal{L}, \alpha)$ dans $F(B)$ est donnée par le diagramme suivant :

$$\begin{array}{ccccc} \eta_e = \underline{M} & \xrightarrow{\Pi = \pi} & \eta_{e+1} = \underline{M} & \xrightarrow{\Pi = \mathrm{id}} & \eta_e = \underline{M} \\ \Big\downarrow{\scriptstyle \alpha} & & \Big\downarrow{\scriptstyle \alpha} & & \Big\downarrow{\scriptstyle \alpha} \\ T_e = \mathcal{L} & \xrightarrow{\Pi = \pi} & T_{e+1} = \mathcal{L} & \xrightarrow{\Pi = \mathrm{id}} & T_e = \mathcal{L} \end{array}$$

où $e = \log_q[\bigwedge^2 M : \bigwedge^2 \mathcal{O}^2]$ désigne l'exposant de l'indice (virtuel) de $\mathcal{O}^2$ dans M (on ne suppose plus ici M normalisé pour que $e \in \{0, 1\}$). La "rigidification" r est le composé du morphisme $\underline{K}^2 \xrightarrow{\sim} \eta_e \otimes K$ associé à l'inclusion $M \subset K^2$ et de $\Pi^{-e} : \eta_e \otimes K \xrightarrow{\sim} \eta_0 \otimes K$.

De même, l'image de $(\mathcal{L}, \alpha \circ g^{-1})$ correspond au diagramme :

$$\begin{array}{ccccc} \eta'_{e-n} = g\underline{M} & \xrightarrow{\Pi = \pi} & \eta'_{e-n+1} = g\underline{M} & \xrightarrow{\Pi = \mathrm{id}} & \eta'_{e-n} = g\underline{M} \\ \Big\downarrow{\scriptstyle \alpha \circ g^{-1}} & & \Big\downarrow{\scriptstyle \alpha \circ g^{-1}} & & \Big\downarrow{\scriptstyle \alpha \circ g^{-1}} \\ T'_{e-n} = \mathcal{L} & \xrightarrow{\Pi = \pi} & T'_{e-n+1} = \mathcal{L} & \xrightarrow{\Pi = \mathrm{id}} & T'_{e-n} = \mathcal{L} \end{array}$$

et à $r' = \underline{K}^2 \xrightarrow{\sim} \eta'_0 \otimes K$ obtenu comme le composé de $\underline{K}^2 \simeq \eta'_{e-n}$ (associé à l'inclusion $gM \hookrightarrow K^2$) et de Π^{-e+n}.

On voit alors que, via l'isomorphisme $g : \underline{M} \xrightarrow{\sim} g\underline{M}$, le point (η', T', u', r') s'obtient bien à partir de (η, T, u, r) comme prédit par la proposition (6.2).

Chapitre II : Le théorème de Drinfeld

On suppose désormais que le corps local K est de *caractéristique zéro.*

On considère dans ce chapitre certains groupes formels p-divisibles munis d'une action de l'anneau des entiers $\mathcal{O}_D$ d'un corps de quaternions D de centre K : les *$\mathcal{O}_D$-modules formels spéciaux de hauteur* 4 (définis au §2). Sur une clôture algébrique $\overline{k}$ de k, ils forment une seule classe d'isogénie ; on choisit l'un d'entre eux noté Φ. Le théorème de Drinfeld (énoncé précisément au §8) établit que le schéma formel $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$ paramètre les $\mathcal{O}_D$-modules formels spéciaux X de hauteur 4 munis d'une quasiisogénie de hauteur zéro $\rho : \Phi \to X$.

Autrement dit le foncteur $\overline{G}$, sur la catégorie $\overline{Nilp}$ des $\mathcal{O}^{nr}$-algèbres B où π est nilpotent, qui à B associe l'ensemble $\overline{G}(B)$ des classes d'isomorphie de tels couples (X, ρ) au-dessus de B, est isomorphe au foncteur $\overline{H}$ représenté par $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$. Le foncteur $\overline{H}$ est la restriction à $\overline{Nilp}$ du foncteur F classifiant les quadruplets (η, T, u, r) définis au §5 du chapitre I. Il s'agit donc de construire un isomorphisme de foncteurs $\overline{\xi} : \overline{G} \to \overline{H}$, en particulier d'associer à (X, ρ) un quadruplet (η, T, u, r). On pose $T = \mathrm{Lie}(X)$; la difficulté est de trouver le faisceau constructible η et l'application $u : \eta \to T$.

Plutôt qu'avec le groupe p-divisible X lui-même, on travaille avec son module de Cartier (-Dieudonné) M. Ceci revient au même grâce à la théorie de Cartier (brièvement rappelée au §1), dont le grand avantage ici est d'être valable quelle que soit l'algèbre de base B. L'action de $\mathcal{O}_D$ sur X permet au §2 de munir M, ainsi que $T = \mathrm{Lie}(X)$, d'une $\mathbb{Z}/2\mathbb{Z}$-graduation et d'un opérateur Π de degré 1 tel que $\Pi^2 = \pi$. Les habituels opérateurs F et V sont également de degré 1 et l'identification de T avec M/VM est compatible à la graduation et à l'action de Π.

On dit que l'indice $i \in \mathbb{Z}/2\mathbb{Z}$ est *critique* si Π est nul sur T_i, autrement dit si $\Pi M_i \subset VM_i$. Sur $\overline{k}$, il existe toujours au moins un indice critique i ; alors M_i muni de l'opérateur $V^{-1}\Pi$ est un "cristal unité" et les invariants $M_i^{V^{-1}\Pi}$ forment un $\mathcal{O}$-module libre de rang un. Posant $\eta_i = M_i^{V^{-1}\Pi}$, on établit assez facilement au §5 une bijection naturelle entre $\overline{G}(\overline{k})$ et $\overline{H}(\overline{k})$.

Le tour de force de Drinfeld réside dans l'extension de cette bijection à toute algèbre B de $\overline{Nilp}$. Une construction ingénieuse expliquée au §3 permet de définir (η, T, u) sur toute base B. On explicite le lien entre cette construction de η et les $M_i^{V^{-1}\Pi}$ au §4. Après avoir défini des filtrations convenables, on montre au §6 que η est un faisceau constructible au sens π-adique. L'introduction d'une rigidification, la quasiisogénie $\rho : \Phi \to X$, permet au §7 de récupérer l'isomorphisme $r : \underline{K}^2 \xrightarrow{\sim} \eta \otimes_{\mathcal{O}} K$ et de montrer que η est constructible au sens strict. Le morphisme de foncteurs $\overline{\xi} : \overline{G} \to \overline{H}$ est alors bien défini.

Il ne reste plus qu'à comparer les théories de déformation (§10) et à montrer que $\overline{\xi}$ induit des bijections sur les espaces tangents (§11) en les points géométriques de $\overline{G}$ et $\overline{H}$. Un dernier argument de représentabilité relative (§12) permet enfin de conclure que $\overline{\xi}$ est un isomorphisme! En complément, on décrit au §9 les actions naturelles des groupes $GL(2, K)$ et D^* sur toute la situation.

Pour clore ce chapitre on construit au §13, à l'aide des points de torsion du $\mathcal{O}_D$-module formel spécial de hauteur 4 universel sur $\widehat{\Omega} \widehat{\otimes}_{\mathcal{O}} \widehat{\mathcal{O}}^{nr}$, un système projectif de revêtements étales Σ_n de l'espace analytique rigide $\Omega \otimes_K \widehat{K}^{nr}$ dont le groupe de Galois est le complété profini $\widehat{\mathcal{O}}_D^*$ de $\mathcal{O}_D^*$.

1. Théorie de Cartier des $\mathcal{O}$-modules formels.

Rappelons brièvement les résultats de la théorie de Cartier des $\mathcal{O}$-modules formels. Pour le cas plus familier des groupes formels ($\mathcal{O} = \mathbb{Z}_p$), le lecteur pourra consulter M. Lazard [La] ou Th. Zink [Zi 3]; c'est ce cas qui servira dans la démonstration du théorème de Čerednik. Le cas général est traité dans M. Hazewinkel [Ha].

(1.1) Il existe un unique foncteur $W_{\mathcal{O}}$ de la catégorie des $\mathcal{O}$-algèbres (commutatives) dans elle-même tel que, pour toute $\mathcal{O}$-algèbre B, on ait ensemblistement $W_{\mathcal{O}}(B) = B^{\mathbb{N}}$ et que, pour tout $n \geq 0$, l'application $w_n : W_{\mathcal{O}}(B) \to B$ définie par

$$w_n(a_0, a_1, a_2, \ldots) = a_0^{q^n} + \pi a_1^{q^{n-1}} + \cdots + \pi^n a_n$$

soit un homomorphisme de $\mathcal{O}$-algèbres.

Ce foncteur possède un endomorphisme $\mathcal{O}$-linéaire τ défini par

$$\tau(a_0, a_1, \ldots) = (0, a_0, a_1, \ldots)$$

et un endomorphisme de $\mathcal{O}$-algèbres σ tel que

$$w_n \sigma = w_{n+1} \ , \text{ pour } n \geq 0.$$

Ces endomorphismes vérifient les relations :

$$\sigma\tau = \pi$$
$$^{\tau}x.y = {}^{\tau}(x.{}^{\sigma}y) \ , \qquad x, y \in W_{\mathcal{O}}(B).$$

Pour $a \in B$, on note $[a] = (a, 0, 0, \ldots)$. On a :

$$[ab] = [a] \cdot [b]$$
$${}^{\sigma}[a] = [a^q].$$

Si B est une k-algèbre, on a :

$${}^{\sigma}(a_0, a_1, a_2, \ldots) = (a_0^q, a_1^q, a_2^q, \ldots)$$
$$\tau\sigma = \sigma\tau = \pi.$$

Lorsque $\mathcal{O} = \mathbb{Z}_p$, $W_{\mathcal{O}}$ est le foncteur W des vecteurs de Witt.

(1.2) Pour toute $\mathcal{O}$-algèbre B, on considère la $\mathcal{O}$-algèbre non commutative $W_{\mathcal{O}}(B)[F, V]$ où F et V vérifient les relations :

$$Fx = {}^{\sigma}xF$$
$$xV = V{}^{\sigma}x$$
$$VxF = {}^{\tau}x$$
$$FV = \pi.$$

L'*anneau de Cartier* $E_{\mathcal{O}}(B)$ est le complété de cette algèbre pour la topologie définie par les idéaux à droite engendrés par les V^n, dite topologie V-adique.

Tout élément de $E_{\mathcal{O}}(B)$ s'écrit de manière unique

$$\sum_{m,n\geq 0} V^m[a_{m,n}]F^n \quad , \quad a_{m,n} \in B,$$

soumis à la condition : pour tout m, $a_{m,n} = 0$ pour n assez grand. L'application :

$$(a_0, a_1, \ldots) \mapsto \sum_{n\geq 0} V^n[a_n]F^n$$

est un homomorphisme de $\mathcal{O}$-algèbres qui identifie $W_{\mathcal{O}}(B)$ à son image dans $E_{\mathcal{O}}(B)$. Par suite, tout élément de $E_{\mathcal{O}}(B)$ s'écrit aussi de manière unique

$$\sum_{m>0} V^m x_m + x_0 + \sum_{n>0} y_n F^n \quad , \quad x_m, y_n \in W_{\mathcal{O}}(B),$$

soumis à la condition : $y_n \to 0$ dans la topologie τ-adique lorsque $n \to \infty$.

(1.3) Pour $a \in \mathcal{O}$, on prendra soin de distinguer l'élément $a = a.1$ provenant de la structure de $\mathcal{O}$-algèbre de $W_{\mathcal{O}}(B)$ et $E_{\mathcal{O}}(B)$ de l'élément $[a]$ représentant multiplicatif de l'élément $a.1$ de B. Pour tout $n \geq 0$, on a $w_n(a) = a$ et $w_n([a]) = a^{q^n}$.

En particulier

$$w_n(\pi - [\pi]) = \pi(1 - \pi^{q^n - 1}).$$

Il existe une unité ε de $W_{\mathcal{O}}(B)$, provenant de $W_{\mathcal{O}}(\mathcal{O})$, dont les composantes fantômes sont

$$w_n(\varepsilon) = 1 - \pi^{q^{n+1}-1},$$

telle que

$$\pi - [\pi] = {}^{\tau}\varepsilon = V\varepsilon F.$$

(1.4) Un *$\mathcal{O}$-module formel* sur une $\mathcal{O}$-algèbre B est un groupe formel lisse X sur B muni d'une action de $\mathcal{O}$, c'est-à-dire d'un homomorphisme d'anneaux $i : \mathcal{O} \to \mathrm{End}(X)$, telle que l'action induite sur l'espace tangent $\mathrm{Lie}(X)$ coïncide avec celle provenant de la structure de B-module de $\mathrm{Lie}(X)$.

Un *$\mathcal{O}$-module de Cartier* sur B est par définition un $E_{\mathcal{O}}(B)$-module à gauche M tel que

(i) M/VM est un B-module libre de rang fini,

(ii) V est injectif sur M,

(iii) M est séparé et complet pour la filtration V-adique.

Un tel module est souvent qualifié de réduit dans la littérature. Le résultat fondamental de la théorie de Dieudonné-Cartier est le suivant ([Zi 3] 4.23; [Ha] 26.3) :

THÉORÈME. — *La catégorie des $\mathcal{O}$-modules formels sur B est équivalente à celle des $\mathcal{O}$-modules de Cartier sur B.*

De plus, si M est le $\mathcal{O}$-module de Cartier associé au $\mathcal{O}$-module formel X, on a $M/VM = \mathrm{Lie}(X)$.

Si B' est une B-algèbre, le module de Cartier du $\mathcal{O}$-module formel $X_{B'}$ déduit de X par changement de base est $M' = E_{\mathcal{O}}(B')\widehat{\otimes}_{E_{\mathcal{O}}(B)}M$ complété de $E_{\mathcal{O}}(B') \otimes_{E_{\mathcal{O}}(B)} M$ pour la topologie V-adique.

(1.5) Soit M un $\mathcal{O}$-module de Cartier sur B. Nous dirons que des éléments $\gamma_1, \ldots, \gamma_d$ de M forment une *V-base* de M si leurs images $\overline{\gamma}_1, \ldots, \overline{\gamma}_d$ mod VM forment une base du B-module libre M/VM. Tout

élément de M s'écrit alors de manière unique $\sum_{m\geq 0}\sum_{i=1}^{d} V^m[c_{m,i}]\gamma_i$ avec $c_{m,i}\in B$.

En particulier le choix des γ_i détermine une famille $c_{m,i,j}$ ($m\in\mathbb{N}$; $i,j\in\{1,\dots,d\}$) d'éléments de B tels que

$$F(\gamma_j)=\sum_{m\geq 0}\sum_{i=1}^{d} V^m[c_{m,i,j}]\gamma_i\ ,\qquad j=1,\dots,d.$$

Réciproquement, étant donnée une famille $c_{m,i,j}$ ($m\in\mathbb{N}$; $i,j\in\{1,\dots,d\}$) d'éléments de $W_{\mathcal{O}}(B)$, il existe un $\mathcal{O}$-module de Cartier M, unique à isomorphisme près, et une V-base $\gamma_1,\dots,\gamma_d$ de M vérifiant les relations

$$(*)\qquad F(\gamma_j)=\sum_{m\geq 0}\sum_{i=1}^{d} V^m c_{m,i,j}\gamma_i\ ,\qquad j=1,\dots,d.$$

Ce module possède la présentation

$$0\longrightarrow E_{\mathcal{O}}(B)^d\xrightarrow{\psi}E_{\mathcal{O}}(B)^d\xrightarrow{\varphi}M\longrightarrow 0$$

où, notant (ε_i) la base canonique de $E_{\mathcal{O}}(B)^d$, φ et ψ sont les applications $E_{\mathcal{O}}(B)$-linéaires définies par

$$\varphi(\varepsilon_i)=\gamma_i$$
$$\psi(\varepsilon_j)=F(\varepsilon_j)-\sum_{m\geq 0}\sum_{i=1}^{d} V^m c_{m,i,j}\varepsilon_i.$$

(1.6) Il sera plus commode pour la suite d'utiliser une formulation un peu modifiée des relations $(*)$. Le choix d'une V-base γ_i de M détermine une famille $d_{m,i,j}$ ($m\in\mathbb{N}^*$; $i,j\in\{1,\dots,d\}$) d'éléments de B tels que

$$\pi\gamma_j=[\pi]\gamma_j+\sum_{m\geq 1}\sum_{i=1}^{d} V^m[d_{m,i,j}]\gamma_i\ ,\qquad j=1,\dots,d.$$

Réciproquement, étant donnée une famille $d_{m,i,j}$ ($m\in\mathbb{N}^*$; $i,j\in\{1,\dots,d\}$) d'éléments de $W_{\mathcal{O}}(B)$, il existe un $\mathcal{O}$-module de Cartier M, unique à isomorphisme près, et une V-base $\gamma_1,\dots,\gamma_d$ de M vérifiant les relations

$$(**)\qquad \pi\gamma_j=[\pi]\gamma_j+\sum_{m\geq 1}\sum_{i=1}^{d} V^m d_{m,i,j}\gamma_i\ ,\qquad j=1,\dots,d.$$

Sachant que $\pi - [\pi] = V\varepsilon F$, où ε est une unité de $W_{\mathcal{O}}(B)$, et que V est injectif sur M, on a alors

$$F\gamma_j = \varepsilon^{-1}V^{-1}\left(\sum_{m\geq 1}\sum_{i=1}^{d} V^m d_{m,i,j}\gamma_i\right)$$
$$= \sum_{m\geq 1}\sum_{i=1}^{d} V^{m-1}\,{}^{\sigma^{m-1}}\varepsilon^{-1} d_{m,i,j}\gamma_i$$

d'où les relations $(*)$ avec $c_{m,i,j} = {}^{\sigma^m}\varepsilon^{-1} d_{m+1,i,j}$.

2. Théorie de Cartier des $\mathcal{O}_D$-modules formels.

(2.1) Soient D un corps de quaternions sur K et $\mathcal{O}_D$ son anneau des entiers. Soient K' une extension quadratique non ramifiée de K contenue dans D, $\mathcal{O}'$ l'anneau des entiers de K' et σ l'automorphisme de conjugaison de K' sur K. Soit enfin Π un élément de $\mathcal{O}_D$ tel que $\Pi^2 = \pi$ et $\Pi a = {}^{\sigma}a\Pi$ pour tout $a \in K'$.

Un *$\mathcal{O}_D$-module formel* sur une $\mathcal{O}$-algèbre B est un $\mathcal{O}$-module formel X sur B muni d'une action $i : \mathcal{O}_D \to \mathrm{End}(X)$ prolongeant l'action de $\mathcal{O}$. Un $\mathcal{O}_D$-module formel est dit *spécial* si l'action de $\mathcal{O}'$ fait de $\mathrm{Lie}(X)$ un $B \otimes_{\mathcal{O}} \mathcal{O}'$-module libre de rang un.

Si B est une $\mathcal{O}'$-algèbre et X un $\mathcal{O}_D$-module formel sur B, le B-module $\mathrm{Lie}(X)$ est $\mathbb{Z}/2\mathbb{Z}$-gradué par l'action de $\mathcal{O}'$:

$$(\mathrm{Lie}(X))_0 = \{m \in \mathrm{Lie}(X); i(a)m = am\,,\ a \in \mathcal{O}'\},$$
$$(\mathrm{Lie}(X))_1 = \{m \in \mathrm{Lie}(X); i(a)m = {}^{\sigma}am\,,\ a \in \mathcal{O}'\}.$$

Alors X est spécial si chaque composante de $\mathrm{Lie}(X)$ est un B-module libre de rang un.

(2.2) Munissons l'anneau de Cartier $E_{\mathcal{O}}(B)$ de la $\mathbb{Z}/2\mathbb{Z}$-graduation définie par

$$\deg V = \deg F = 1,$$
$$\deg[b] = 0 \text{ pour } b \in B.$$

Remarquons que le sous-anneau $W_{\mathcal{O}}(B)$ de $E_{\mathcal{O}}(B)$ est contenu dans la composante homogène de degré 0, en effet tout élément de $W_{\mathcal{O}}(B)$ s'écrit $\sum_{n\geq 0} V^n[a_n]F^n$, $a_n \in B$.

On appellera *$\mathcal{O}[\Pi]$-module de Cartier gradué* sur B un $\mathcal{O}$-module de Cartier $\mathbb{Z}/2\mathbb{Z}$-gradué $M = M_0 \oplus M_1$ muni d'un endomorphisme $E_{\mathcal{O}}(B)$-linéaire Π de degré 1 tel que $\Pi^2 = \pi$. D'après ce qui précède, M_0 et M_1 sont automatiquement des sous-$W_{\mathcal{O}}(B)$-modules de M.

On dira que M est *spécial*, si M_0/VM_1 et M_1/VM_0 sont des B-modules libres de rang un.

THÉORÈME. — *Si B est une $\mathcal{O}'$-algèbre, la catégorie des $\mathcal{O}_D$-modules formels sur B est équivalente à celle des $\mathcal{O}[\Pi]$-modules de Cartier gradués sur B.*

De plus, un $\mathcal{O}_D$-module formel est spécial si et seulement si le $\mathcal{O}[\Pi]$-module de Cartier correspondant est spécial.

Démonstration. — (*cf.* T. Zink [Zi 2], Satz 2.2). Remarquons tout d'abord que, lorsque B est une $\mathcal{O}'$-algèbre, les structures de $\mathcal{O}$-algèbres de $W_{\mathcal{O}}(B)$ et $E_{\mathcal{O}}(B)$ se prolongent en structures de $\mathcal{O}'$-algèbres. En effet $\mathcal{O}'$ est engendré sur $\mathcal{O}$ par les racines (q^2-1)-ièmes de l'unité ; pour $\zeta \in \mathcal{O}'$ tel que $\zeta^{q^2-1} = 1$ on dispose du représentant multiplicatif $[\zeta]$ dans $W_{\mathcal{O}}(B)$ de l'image de ζ dans B et l'application $\zeta \mapsto [\zeta]$ est un isomorphisme des groupes des racines (q^2-1)-ièmes de l'unité dans $\mathcal{O}'$ et dans $W_{\mathcal{O}}(B)$; il existe donc un unique homomorphisme de $\mathcal{O}$-algèbres $j : \mathcal{O}' \to W_{\mathcal{O}}(B)$ tel que $j(\zeta) = [\zeta]$.

On a noté σ aussi bien l'homomorphisme de conjugaison de $\mathcal{O}'$ sur $\mathcal{O}$ que l'endomorphisme de Frobenius de $W_{\mathcal{O}}(B)$. L'homomorphisme j est compatible à σ, en effet ${}^{\sigma}\zeta = \zeta^q$ dans $\mathcal{O}'$et ${}^{\sigma}[\zeta] = [\zeta^q]$ dans $W_{\mathcal{O}}(B)$, par suite $j({}^{\sigma}a) = {}^{\sigma}j(a)$ pour tout $a \in \mathcal{O}'$.

Ainsi tout $E_{\mathcal{O}}(B)$-module, en particulier tout $\mathcal{O}$-module de Cartier M sur B, est muni de deux structures naturelles de $\mathcal{O}'$-module via j et $j\sigma$. On notera simplement am et ${}^{\sigma}am$, $a \in \mathcal{O}'$, $m \in M$, ces structures.

D'après (1.4) la catégorie des $\mathcal{O}_D$-modules formels sur B est équivalente à celle des $\mathcal{O}$-modules de Cartier M sur B munis d'une action $i : \mathcal{O}_D \to \mathrm{End}(M)$ prolongeant l'action de $\mathcal{O}$. En particulier ils sont munis d'une action de $\mathcal{O}'$ via i, de sorte qu'on a une décomposition du $\mathcal{O}$-module M en $M = M_0 \oplus M_1$ où

$$M_0 = \{m \in M \mid i(a)m = am\,,\ a \in \mathcal{O}'\},$$
$$M_1 = \{m \in M \mid i(a)m = {}^{\sigma}am\,,\ a \in \mathcal{O}'\}.$$

Les opérateurs $V, F, [b]$ sont des homomorphismes de $\mathcal{O}$-module de degrés respectifs $1, 1, 0$ car

$$aV = V{}^{\sigma}a$$
$$Fa = {}^{\sigma}aF \qquad\qquad a \in \mathcal{O}'\,,\ b \in B.$$
$$a[b] = [b]a$$

Réciproquement la donnée d'une $\mathbf{Z}/2\mathbf{Z}$-graduation du $\mathcal{O}$-module M, telle que $\deg V = \deg F = 1$ et $\deg[b] = 0$ pour $b \in B$, équivaut à la donnée d'une action de $\mathcal{O}'$ compatible à l'action de $\mathcal{O}$.

Donner une action de $\mathcal{O}_D$ revient à donner de plus l'action de Π; on notera simplement Π l'endomorphisme de $E_{\mathcal{O}}(B)$-module de M défini par $i(\Pi)$. Puisque $\Pi^2 = \pi$ dans $\mathcal{O}_D$, l'endomorphisme Π de M vérifie également $\Pi^2 = \pi$ (où π est défini par la structure de $\mathcal{O}$-algèbre de $E_{\mathcal{O}}(B)$). C'est un opérateur de degré 1 car $\Pi(a) = {}^{\sigma}a\Pi$ pour $a \in \mathcal{O}'$.

Enfin les graduations sur l'algèbre de Lie d'un $\mathcal{O}_D$-module formel X et sur son module de Cartier M sont définies toutes deux par l'action de $\mathcal{O}'$, elles sont donc compatibles :

$$(\mathrm{Lie}(X))_0 = M_0/VM_1,$$
$$(\mathrm{Lie}(X))_1 = M_1/VM_0.$$

Par suite M est spécial si et seulement si X est spécial.

(2.3) Soit M un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur B. Soit (γ_0, γ_1) une V-base homogène ($\gamma_0 \in M_0, \gamma_1 \in M_1$) de M. Tout élément de M s'écrit de manière unique

$$x = \sum_{m \geq 0} (V^m[c_{m,0}]\gamma_0 + V^m[c_{m,1}]\gamma_1), \quad c_{m,i} \in B.$$

Puisque V est de degré 1 et $[c_{m,i}]$ de degré 0, la décomposition de x en composantes homogènes $x \in M_0$ et $x_1 \in M_1$ est donnée par

$$x_0 = [c_{0,0}]\gamma_0 + \sum_{m>0} V^m[c_{m,\overline{m}}]\gamma_{\overline{m}}$$
$$x_1 = [c_{0,1}]\gamma_1 + \sum_{m>0} V^m[c_{m,\overline{m+1}}]\gamma_{\overline{m+1}}$$

où $\overline{m}$ est la classe de m dans $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

En particulier le choix de la V-base homogène (γ_0, γ_1) de M détermine des éléments $a_{m,i}$ ($m \in \mathbb{N}; i = 0, 1$) de B tels que

$$\Pi\gamma_0 = [a_{0,0}]\gamma_1 + \sum_{m>0} V^m[a_{m,0}]\gamma_{\overline{m+1}},$$
$$\Pi\gamma_1 = [a_{0,1}]\gamma_0 + \sum_{m>0} V^m[a_{m,1}]\gamma_{\overline{m}}.$$

On en déduit

$$\Pi^2 = [a_{0,0}.a_{0,1}] \bmod VM.$$

Or on a $\Pi^2 = \pi$ et $\pi \equiv [\pi] \bmod VM$, d'où

$$a_{0,0}.a_{0,1} = \pi.$$

Réciproquement ;

PROPOSITION. — *Soit B une $\mathcal{O}'$-algèbre. Etant donnés des éléments $a_{m,i} (m \in \mathbf{N} ; i = 0,1)$ de B tels que $a_{0,0}.a_{0,1} = \pi$, il existe un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial M sur B, unique à isomorphisme près, et une V-base homogène (γ_0, γ_1) de M vérifiant les relations*

$$\Pi\gamma_0 = [a_{0,0}]\gamma_1 + \sum_{m>0} V^m [a_{m,0}]\gamma_{\overline{m+1}},$$
$$\Pi\gamma_1 = [a_{0,1}]\gamma_0 + \sum_{m>0} V^m [a_{m,1}]\gamma_{\overline{m}}.$$

Démonstration. — La connaissance des formules donnant l'action de Π permet de déterminer celles donnant l'action de $\Pi^2 = \pi$ (sachant que Π est un endomorphisme de $E_{\mathcal{O}}(B)$-module, donc commute à V et aux $[a_{m,i}]$). Puisque $a_{0,0}.a_{0,1} = \pi$, on trouve des éléments $d_{m,i} (m \in \mathbf{N}^* ; i = 0,1)$ de B tels que

$$\pi\gamma_i = [\pi]\gamma_i + \sum_{m>0} V^m [d_{m,i}]\gamma_{\overline{m+i}}, \quad i = 0,1.$$

D'après (1.6), il existe un $\mathcal{O}$-module de Cartier M sur B, unique à isomorphisme près, et une V-base (γ_0, γ_1) de M telle que ces relations soient vérifiées. Posons

$$M_i = \left\{ \sum_{m \geq 0} V^m x_m \gamma_{\overline{m+i}} \ ; \ x_m \in W_{\mathcal{O}}(B) \right\}, \ i = 0,1.$$

Alors M_0 et M_1 sont des sous-$W_{\mathcal{O}}(B)$-modules de M tels que $M = M_0 \oplus M_1$. Par construction les opérateurs Π, V et $[b]$ $(b \in B)$ sont de degrés respectifs 1,1 et 0. Par suite $\pi - [\pi] : M \to VM$ est de degré 0 et, puisque V est injectif sur M et $F = \varepsilon^{-1}V^{-1}(\pi - [\pi])$ où ε est une unité dans $W_{\mathcal{O}}(B)$ (1.3), F est de degré 1. Ainsi M est un $\mathcal{O}[\Pi]$-module de Cartier gradué. Il est spécial puisque M_0/VM_1 est libre de base γ_0 et M_1/VM_0 libre de base γ_1.

(2.4) Soient B' une B-algèbre et $M' = E_{\mathcal{O}}(B')\widehat{\otimes}_{E_{\mathcal{O}}(B)}M$ le module de Cartier sur B' déduit de M par changement de base. Alors M' est

un $\mathcal{O}[\Pi]$-module de Cartier gradué sur B' ; l'image (γ'_0, γ'_1) dans M' de (γ_0, γ_1) est une V-base homogène de M' vérifiant les relations

$$\Pi\gamma'_i = [a'_{0,i}]\gamma'_{i+1} + \sum_{m>0} V^m[a'_{m,i}]\gamma'_{\overline{m+1+i}}\,, \quad i = 0, 1,$$

où les $a'_{m,i}$ sont les images dans B' des éléments $a_{m,i}$ de B.

3. Construction de (η_M, T_M, u_M).

(3.1) Pour toute $\mathcal{O}'$-algèbre B, on considère la $\mathcal{O}'$-algèbre non commutative $W_{\mathcal{O}}(B)[V, \Pi]$ où Π et V vérifient les relations :

$$\begin{aligned} \Pi V &= V\Pi \\ \Pi x &= x\Pi \\ xV &= V^\sigma x \qquad , x \in W_{\mathcal{O}}(B) \\ \Pi^2 &= \pi. \end{aligned}$$

On notera $E'_{\mathcal{O}}(B)$ le complété de cette algèbre pour la topologie définie par les idéaux à droite engendrés par les V^n. Un élément de $E'_{\mathcal{O}}(B)$ s'écrit de manière unique

$$\sum_{m\geq 0} V^m x_m + \sum_{m\geq 0} V^m x'_m \Pi, \qquad\qquad x_m, x'_m \in W_{\mathcal{O}}(B).$$

On munit $E'_{\mathcal{O}}(B)$ de la $\mathbb{Z}/2\mathbb{Z}$-graduation définie par

$$\begin{aligned} \deg x &= 0\ ,\ x \in W_{\mathcal{O}}(B), \\ \deg V &= \deg\Pi = 1. \end{aligned}$$

Tout $\mathcal{O}[\Pi]$-module de Cartier gradué sur B est en particulier un $E'_{\mathcal{O}}(B)$-module gradué (par oubli de l'action de F).

(3.2) Si M est un $W_{\mathcal{O}}(B)$-module, on notera M^σ le $W_{\mathcal{O}}(B)$-module obtenu par restriction des scalaires via $\sigma : W_{\mathcal{O}}(B) \to W_{\mathcal{O}}(B)$. Si M est un $E'_{\mathcal{O}}(B)$-module, M^σ est encore un $E'_{\mathcal{O}}(B)$-module et V définit un homomorphisme $E'_{\mathcal{O}}(B)$-linéaire de M^σ dans M. Si $M = M_0 \oplus M_1$ est gradué, $M^\sigma = M_0^\sigma \oplus M_1^\sigma$ l'est également et $V : M^\sigma \to M$ est de degré 1.

Pour tout $E'_{\mathcal{O}}(B)$-module M, on définit un $E'_{\mathcal{O}}(B)$-module $N(M)$ par la suite exacte

$$\begin{aligned} M^\sigma \xrightarrow{\alpha_M} M \oplus M^\sigma \xrightarrow{\beta_M} N(M) \longrightarrow 0 \\ m \longmapsto (Vm, -\Pi m). \end{aligned}$$

Si M est gradué, $N(M)$ l'est également avec

$$N(M)_i = \beta_M(M_i \oplus M_i^\sigma) \qquad i = 0, 1.$$

Remarquons que, lorsque V est injectif sur M, l'application α_M est injective.

Ainsi N est un foncteur covariant exact à droite de la catégorie des $E'_{\mathcal{O}}(B)$-modules dans elle-même. De plus, si la suite de $E'_{\mathcal{O}}(B)$-modules

$$0 \to M' \to M \to M'' \to 0$$

est exacte et si V est injectif sur M'', la suite

$$0 \to N(M') \to N(M) \to N(M'') \to 0$$

est exacte.

(3.3) On notera $\beta_M(m, m') = ((m, m'))$.

L'application $E'_{\mathcal{O}}(B)$-linéaire canonique $M^\sigma \to N(M)$ définie par $m \mapsto ((0, m))$ est injective lorsque V est injectif sur M.

L'application

$$\begin{aligned} M \oplus M^\sigma &\longrightarrow M/VM \\ (m, m') &\longmapsto \overline{m} \pmod{VM} \end{aligned}$$

définit une surjection canonique $N(M) \to M/VM$.

Enfin l'application

$$\begin{aligned} M \oplus M^\sigma &\longrightarrow M \\ (m, m') &\longmapsto \Pi m + V m' \end{aligned}$$

définit une application $E'_{\mathcal{O}}(B)$-linéaire (de degré 1) canonique $\lambda_M : N(M) \to M$.

LEMME (3.4). — *Si B est une K-algèbre, λ_M est bijective.*

Démonstration. — Si B est une K-algèbre, la famille des applications w_n définit un isomorphisme de $\mathcal{O}$-algèbres $W_{\mathcal{O}}(B) \xrightarrow{\sim} B^{\mathbf{N}}$; en particulier π est inversible dans $W_{\mathcal{O}}(B)$. Puisque $\Pi^2 = \pi$, il en résulte que Π est inversible dans $E'_{\mathcal{O}}(B)$.

Alors l'application $M \to N(M)$ définie par $m \mapsto ((m, 0))$ est bijective et, puisque $\lambda_M((m, 0)) = \Pi m$, λ_M est également bijective.

LEMME (3.5). — *Soient B une $\mathcal{O}'$-algèbre sans torsion et M un $\mathcal{O}'$-module de Cartier sur B. Soient $B_K = B \otimes_{\mathcal{O}} K$ et $M_K =$*

$M\widehat{\otimes}_{E_{\mathcal{O}}(B)}E_{\mathcal{O}}(B_K)$. *Alors l'application canonique* $M \to M_K$ *est injective et* V *est injectif sur* M_K/M.

Démonstration. — Soit γ_i une V-base de M. Si

$$x = \sum_{i,m} V^m[a_{m,i}]\gamma_i \quad , \quad a_{m,i} \in B,$$

est un élément de M, son image x_K dans M_K s'écrit

$$x_K = \sum V^m[a_{m,i;K}]\gamma_{i,K}$$

où $\gamma_{i,K}$ est la V-base de M_K image de γ_i et $a_{m,i;K}$ l'image de $a_{m,i}$ dans B_K. Si $x_K = 0$, on a $a_{m,i;K} = 0$ pour tout m, i; d'où, puisque B est sans torsion, $a_{m,i} = 0$ et $x = 0$.

De plus si

$$x' = \sum_{i,m} V^m[a'_{m,i}]\gamma_{i,K} \quad , \quad a'_{m,i} \in B_K,$$

est un élément de M_K, on a

$$Vx' = \sum_{i,m} V^{m+1}[a'_{m,i}]\gamma_{i,K}.$$

Si $Vx' \in M$, on a $a'_{m,i} \in B$ pour tout m, i; donc $x' \in M$.

LEMME (3.6). — *Soient* B *une* $\mathcal{O}'$*-algèbre sans torsion et* M *un* $\mathcal{O}[\Pi]$*-module de Cartier sur* B. *Alors l'application* $\lambda_M : N(M) \to M$ *est injective.*

Démonstration. — D'après (3.5) on a une suite exacte de $E'_{\mathcal{O}}(B)$-modules

$$0 \to M \to M_K \to M_K/M \to 0$$

et V est injectif sur M_K/M. Par suite (3.2), l'application canonique $N(M) \to N(M_K)$ est injective. Le diagramme commutatif

$$\begin{array}{ccc} N(M) & \xrightarrow{\lambda_M} & M \\ \downarrow & & \downarrow \\ N(M_K) & \xrightarrow{\lambda_{M_K}} & M_K \end{array}$$

et l'injectivité de λ_{M_K} (3.4) montrent que λ_M est injective.

LEMME (3.7). — *Soit $B \to B'$ une surjection de $\mathcal{O}'$-algèbres de noyau I. Soient M un $\mathcal{O}$-module de Cartier sur B et $M' = M\widehat{\otimes}_{E_{\mathcal{O}}(B)}E_{\mathcal{O}}(B')$. Soient $\{\gamma_i\}$ une V-base de M et*

$$M_I = \left\{ \sum_{m,i} V^m[a_{m,i}]\gamma_i \ ; \ a_{m,i} \in I \right\}.$$

Alors on a des suites exactes de $E_{\mathcal{O}}(B)$-modules

$$0 \to M_I \to M \to M' \to 0$$

et de $E'_{\mathcal{O}}(B)$-modules

$$0 \to N(M_I) \to N(M) \to N(M') \to 0.$$

Démonstration. — Un élément $\sum_{m,i} V^m[a_{m,i}]\gamma_i$ de M a une image nulle dans M'si et seulement si les $a_{m,i}$ ont une image nulle dans B', d'où la première suite exacte. La deuxième résulte alors de (3.2).

PROPOSITION (3.8). — *Il existe une et une seule façon de définir, pour toute $\mathcal{O}'$-algèbre B et tout $\mathcal{O}[\Pi]$-module de Cartier gradué spécial M sur B, une application $L_M = M \to N(M)$ telle que*

(i) *si $B \to B'$ est un homomorphisme de $\mathcal{O}'$-algèbres et si $M' = M\widehat{\otimes}_{E_{\mathcal{O}}(B)}E_{\mathcal{O}}(B')$, le diagramme*

$$\begin{array}{ccc} M & \xrightarrow{L_M} & N(M) \\ \downarrow & & \downarrow \\ M' & \xrightarrow{L_{M'}} & N(M') \end{array}$$

est commutatif.

(ii) *on a $F = \lambda_M \circ L_M$.*

Démonstration. — a) Supposons tout d'abord que B est une $\mathcal{O}'$-algèbre sans torsion. Alors λ_M est injectif (3.6), il s'agit donc de vérifier que

$F(M) \subset \lambda_M(N(M))$, où $\lambda_M(N(M)) = \Pi M + VM$ est un sous-$E'_{\mathcal{O}}(B)$-module de M.

Soit (γ_0, γ_1) une V-base homogène de M. Tout élément de M s'écrit $[a_0]\gamma_0 + [a_1]\gamma_1 \bmod VM, a_i \in B$. Or $FVM = \pi M = \Pi^2 M$ et $F[a_i]\gamma_i = [a_i^q]F\gamma_i$, il suffit donc de vérifier que $F\gamma_i \in \Pi M + VM$, $i = 0, 1$. On a $V\varepsilon F = \pi - [\pi]$, où ε est une unité de $W_{\mathcal{O}}(B)$ (1.3) et V est injectif sur M ; il revient donc au même de montrer que

$$(\pi - [\pi])\gamma_i \in V\varepsilon(\Pi M + VM) = V(\Pi M + VM).$$

On a

$$\Pi\gamma_0 = [a_{0,0}]\gamma_1 + Vx_0$$
$$\Pi\gamma_1 = [a_{0,1}]\gamma_0 + Vx_1$$

où $a_{0,0}$ et $a_{0,1}$ sont des éléments de B tels que $a_{0,0}.a_{0,1} = \pi$ et $x_0 \in M_0$, $x_1 \in M_1$. Par suite

$$(\pi - [\pi])\gamma_0 = (\Pi^2 - [\pi])\gamma_0 = [a_{0,0}]Vx_1 + \Pi Vx_0.$$

Or

$$\Pi Vx_0 = V\Pi x_0$$
$$[a_{0,0}]Vx_1 = V[a_{0,0}][a_{0,0}^{q-1}]x_1 \ \in V[a_{0,0}]M_1,$$

mais $[a_{0,0}]\gamma_1 = \Pi\gamma_0 - Vx_0$, donc $[a_{0,0}]M_1 \subset \Pi M + VM$. On a ainsi montré que $(\pi - [\pi])\gamma_0 \in V(\Pi M + VM)$.

De même on a

$$(\pi - [\pi])\gamma_1 = [a_{0,1}]Vx_0 + \Pi Vx_1$$

et on conclut sachant que $[a_{0,1}]M_0 \subset \Pi M + VM$.

Remarquons que L_M est additif et vérifie :

$$L_M(ax) = {}^{\sigma}aL_M(x) \quad , \quad a \in W_{\mathcal{O}}(B), x \in M,$$
$$L_M(Vx) = ((\Pi x, 0)).$$

En effet

$$\lambda_M L_M(ax) = F(ax) = {}^{\sigma}aFx = {}^{\sigma}a\lambda_M L_M(x) = \lambda_M({}^{\sigma}aL_M(x))$$
$$\lambda_M L_M(Vx) = FVx = \Pi^2 x = \lambda_M((\Pi x, 0)).$$

b) Soient I un idéal de B, $B' = B/I$ et $M' = M\widehat{\otimes}_{E_{\mathcal{O}}(B)}E_{\mathcal{O}}(B')$. Pour montrer l'existence de $L_{M'}$ rendant commutatif le diagramme (i), il faut

et il suffit, d'après (3.7), que $L_M(M_I) \subset N(M_I)$. Un élément de M_I peut s'écrire

$$x = [c_0]\gamma_0 + [c_1]\gamma_1 + Vy$$

avec c_0 et $c_1 \in I$ et $y \in M_I$. Alors on a

$$L_M(x) = [c_0^q]L_M(\gamma_0) + [c_1^q]L_M(\gamma_1) + ((\Pi y, 0)).$$

Il est clair que chacun des termes du second membre a une image nulle dans $N(M')$, d'où $L_M(x) \in N(M_I)$.

c) Soient maintenant B une $\mathcal{O}'$-algèbre quelconque et M un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur B. Soient (γ_0, γ_1) une base homogène de M et $a_{m,i}$ les éléments de B tels que

$$\Pi\gamma_0 = [a_{0,0}]\gamma_1 + \sum_{m>0} V^m[a_{m,0}]\gamma_{m+1}$$
$$\Pi\gamma_1 = [a_{0,1}]\gamma_0 + \sum_{m>0} V^m[a_{m,1}]\gamma_m.$$

Soit $\widetilde{B} = \mathcal{O}'[X_b; b \in B]/X_{a_{0,0}}.X_{a_{0,1}} - \pi$, où les X_b sont des variables indépendantes indexées par $b \in B$. Soit $\widetilde{M}$ le $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur $\widetilde{B}$ de base homogène $(\tilde{\gamma}_0, \tilde{\gamma}_1)$ vérifiant

$$\Pi\tilde{\gamma}_i = [X_{a_{0,i}}]\tilde{\gamma}_{i+1} + \sum_{m>0} V^m[X_{a_{m,i}}]\tilde{\gamma}_{m+i+1}.$$

Alors $\widetilde{B}$ est une $\mathcal{O}'$-algèbre sans torsion dont B est un quotient via $X_b \mapsto b$ et M est déduit de $\widetilde{M}$ par changement de base. D'après a) et b), il existe d'uniques applications $L_{\widetilde{M}} : \widetilde{M} \to N(\widetilde{M})$ et $L_M : M \to N(M)$ rendant commutatif le diagramme

$$\begin{array}{ccc} \widetilde{M} & \xrightarrow{L_{\widetilde{M}}} & N(\widetilde{M}) \\ \downarrow & & \downarrow \\ M & \xrightarrow{L_M} & N(M) \end{array}$$

telles que $\lambda_{\widetilde{M}} L_{\widetilde{M}} = F$ et $\lambda_M L_M = F$.

d) Si $B \to B'$ est un homomorphisme de $\mathcal{O}'$-algèbres et si $M' = M\widehat{\otimes}_{E_{\mathcal{O}}(B)}E_{\mathcal{O}}(B')$, la construction précédente fournit un diagramme commutatif de $\mathcal{O}'$-algèbres

$$\begin{array}{ccc} \widetilde{B} & \longrightarrow & B \\ \downarrow & & \downarrow \\ \widetilde{B}' & \longrightarrow & B' \end{array}$$

où $\widetilde{B}$ et $\widetilde{B}'$ sont sans torsion. La commutativité du diagramme

$$\begin{array}{ccc} M & \xrightarrow{L_M} & N(M) \\ \downarrow & & \downarrow \\ M' & \xrightarrow{L_{M'}} & N(M') \end{array}$$

se déduit par passage au quotient de la commutativité du diagramme analogue relatif à $\widetilde{M}$ et $\widetilde{M}'$. Celle-ci résulte de l'injectivité de $\lambda_{\widetilde{M}'}$ et de la commutativité des diagrammes :

$$\begin{array}{ccc} N(\widetilde{M}) & \xrightarrow{\lambda_{\widetilde{M}}} & \widetilde{M} \\ \downarrow & & \downarrow \\ N(\widetilde{M}') & \xrightarrow[\lambda_{\widetilde{M}'}]{} & \widetilde{M}' \end{array} \qquad \begin{array}{ccc} \widetilde{M} & \xrightarrow{F} & \widetilde{M} \\ \downarrow & & \downarrow \\ \widetilde{M}' & \xrightarrow[F]{} & \widetilde{M}' \end{array}$$

La preuve de la proposition (3.8) est donc achevée.

Remarque (3.9). L'application $L_M : M \to N(M)$ ainsi définie est additive et vérifie

$$\begin{aligned} L_M(ax) &= {}^{\sigma}aL_M(x) \\ L_M(Vx) &= ((\Pi x, 0)) \end{aligned} \qquad a \in W_{\mathcal{O}}(B),\ x \in M.$$

En effet ceci est vrai dans le cas où B est sans torsion comme on l'a remarqué en a) ; c'est donc vrai dans le cas général par passage au quotient.

Une application $L : M \to N(M)$ additive et vérifiant

$$\begin{aligned} L([a]x) &= [a^q]L(x) \\ L(Vx) &= ((\Pi x, 0)) \end{aligned} \qquad a \in B,\ x \in M,$$

est complètement déterminée par la donnée de $L(\gamma_0)$ et $L(\gamma_1)$. En effet un élément quelconque de M s'écrit de manière unique

$$x = [a_0]\gamma_0 + [a_1]\gamma_1 + Vy$$

avec $a_0, a_1 \in B$ et $y \in M$. On définit L en posant

$$L(x) = [a_0^q]L(\gamma_0) + [a_1^q]L(\gamma_1) + ((\Pi y, 0)).$$

De plus pour que $\lambda_M L = F$, il suffit que $\lambda_M L(\gamma_i) = F\gamma_i$ pour $i = 0, 1$. En effet on a alors

$$\begin{aligned} \lambda_M L(x) &= [a_0^q]F\gamma_0 + [a_1^q]F\gamma_1 + \Pi^2 y \\ &= F([a_0]\gamma_0 + [a_1]\gamma_1 + Vy) = F(x). \end{aligned}$$

L'essentiel est donc de montrer qu'il existe des éléments y_i de $N(M)$ tels que $\lambda_M(y_i) = F\gamma_i$. Ceci peut se vérifier dans le cas "universel" où B est sans torsion et λ_M injectif, ce qu'on a fait en a).

Remarque (3.10). Notons également que L_M commute avec Π. En effet il suffit encore une fois de le vérifier dans le cas où B est sans torsion et après composition avec λ_M ; or on a $\lambda_M L_M = F$ et aussi bien F que λ_M commutent avec Π.

De plus L_M est de degré 0, car F et λ_M sont tous deux de degré 1.

DÉFINITION (3.11). — L'application $M \oplus M^{\sigma} \to N(M)$ donnée par $(x, x') \mapsto L_M(x) + ((x', 0))$ définit une application $\varphi_M : N(M) \to N(M)$. En effet $(Vx, -\Pi x) \mapsto 0$ puisque $L_M(Vx) = ((\Pi x, 0))$.

L'application φ_M est additive de degré 0, commute avec Π et vérifie

$$\varphi_M(ay) = {}^{\sigma}a\varphi_M(y) \qquad , a \in W_{\mathcal{O}}(B),\ y \in N(M).$$

En particulier φ_M est $\mathcal{O}[\Pi]$-linéaire.

PROPOSITION (3.12). — *Soit $B \to B'$ une surjection de $\mathcal{O}'$-algèbres de noyau I tel que $I^2 = 0$ et $\pi I = 0$. Soient M un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur B et $M' = M \widehat{\otimes}_{E_{\mathcal{O}}(B)} E_{\mathcal{O}}(B')$. Alors le noyau de l'application canonique $N(M) \to N(M')$ est annulé par φ_M^3.*

Démonstration. — Soit (γ_0, γ_1) une V-base homogène de M. Tout élément de $M_I = \mathrm{Ker}(M \to M')$ s'écrit (3.7) :

$$x = [a_0]\gamma_0 + [a_1]\gamma_1 + Vx' \ , \ a_i \in I \, , \, x' \in M_I.$$

De plus on a $N(M_I) = \mathrm{Ker}(N(M) \to N(M'))$. Or

$$\begin{aligned} \varphi_M((x,0)) &= L_M(x) \\ &= [a_0^q]L_M(\gamma_0) + [a_1^q]L_M(\gamma_1) + ((\Pi x', 0)) \\ &= ((\Pi x', 0)) \end{aligned}$$

car $a_0^q = a_1^q = 0$. De même en écrivant :

$$x' = [a_0']\gamma_0 + [a_1']\gamma_1 + Vx'' \ , a_i' \in I \ , \ x'' \in M_I,$$

il vient :

$$\varphi_M^2((x,0)) = ((\Pi^2 x'', 0)) = ((\pi x'', 0)) = 0,$$

car $\pi M_I = 0$. En effet si $x \in M_I$, on a :

$$\begin{aligned} x &= \sum_{m,i} V^m [a_{m,i}]\gamma_i \ , \ a_{m,i} \in I, \\ \pi x &= \sum_{m,i} V^m \pi [a_{m,i}]\gamma_i. \end{aligned}$$

Mais $\pi[a] = 0$ si $a \in I$, puisque :

$$\begin{aligned} \pi[a] &= ([\pi] + V\varepsilon F)[a] \\ &= [\pi a] + V\varepsilon[a^q]F. \end{aligned}$$

On conclut sachant que $\varphi_M((0,x)) = ((x,0))$.

DÉFINITION (3.13). — A tout $\mathcal{O}[\Pi]$-module de Cartier gradué spécial M sur B, on associe un $\mathcal{O}[\Pi]$-module gradué η_M défini par

$$\eta_M = N(M)^{\varphi_M} = \{z \in N(M) / \varphi_M(z) = z\}$$

et une application $\mathcal{O}[\Pi]$-linéaire de degré zéro $u_M : \eta_M \to M/VM$, en composant l'injection $\eta_M \hookrightarrow N(M)$ avec l'application canonique $N(M) \to M/VM$ (3.3).

De plus, si B' est une B-algèbre et $M' = M\widehat{\otimes}_{E_{\mathcal{O}}(B)}E_{\mathcal{O}}(B')$, l'application canonique $M \to M'$ induit une application $\mathcal{O}[\Pi]$-linéaire de degré zéro $\eta_M \to \eta_{M'}$, telle que le diagramme

$$\begin{array}{ccc} \eta_M & \xrightarrow{u_M} & M/VM \\ \downarrow & & \downarrow \\ \eta_{M'} & \xrightarrow{u_{M'}} & M'/VM' \quad = (M/VM)\otimes_B B' \end{array}$$

soit commutatif.

PROPOSITION (3.14). — *Si B' est le quotient de B par un idéal nilpotent annulé par une puissance de π, l'application canonique $\eta_M \to \eta_{M'}$ est bijective.*

Démonstration. — La proposition est vraie si $I^2 = 0$ et $\pi I = 0$, en effet $N(M) \to N(M')$ est surjectif (3.7) et $1 - \varphi_M$ est inversible sur le noyau (3.12). Le cas général s'en déduit par récurrence.

4. Calcul des composantes homogènes de η_M.

(4.1) Dans ce paragraphe B est une $\mathcal{O}'$-algèbre telle que $\pi B = 0$ et $M = M_0 \oplus M_1$ un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur B. Un indice $i \in \mathbb{Z}/2\mathbb{Z}$ est dit *critique* si l'application $\Pi : M_i/VM_{i-1} \to M_{i+1}/VM_i$ est nulle, autrement dit si $\Pi M_i \subset VM_i$.

Si B est intègre, l'un au moins des deux indices 0 ou 1 est critique. En effet M_i/VM_{i-1} est un B-module libre de rang 1 ($i = 0, 1$) et le composé $\Pi \circ \Pi = \pi$ est nul.

LEMME (4.2). — *Si i est un indice critique et $x \in M_i$, on a $L_M x = ((V^{-1}\Pi x, 0))$.*

[$V^{-1}\Pi x$ est bien défini puisque $\Pi M_i \subset VM_i$ et V injectif].

Démonstration. — On sait déjà que si $x = Vx'$, on a $L_M x = ((\Pi x', 0))$ et $\Pi x' = V^{-1}\Pi x$, puisque $\Pi V = V\Pi$. De plus, pour $a \in B$, on a $L_M[a]x = [a^q]L_M x$ et $V^{-1}\Pi[a]x = [a^q]V^{-1}\Pi x$. Puisque tout élément de

M_i est de la forme $[a]\gamma_i + Vx'$, il suffit de démontrer le lemme lorsque $x = \gamma_i$.

Soit, comme en (3.8), $\widetilde{B}$ une $\mathcal{O}'$-algèbre sans torsion dont B est un quotient et $\widetilde{M}$ un relèvement de M en un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur $\widetilde{B}$. Soient $\tilde{\gamma}_i$ relevant γ_i, on a

$$\Pi\tilde{\gamma}_i = [\tilde{a}_i]\tilde{\gamma}_{i+1} + V\tilde{x}_i$$

avec $\tilde{a}_i \in \widetilde{B}$ et $\tilde{x}_i \in \widetilde{M}_i$. Puisque i est critique, l'image a_i de $\tilde{a}_i$ dans B est nulle et

$$\Pi\gamma_i = Vx_i$$

où x_i est l'image de $\tilde{x}_i$ dans M_i.

Il s'agit de montrer que $L_M\gamma_i = ((x_i, 0))$. Par définition $L_M\gamma_i$ est l'image de $L_{\widetilde{M}}\tilde{\gamma}_i$. Reprenons le calcul de $L_{\widetilde{M}}\tilde{\gamma}_i$ effectué en (3.8) en supposant pour simplifier les notations $i = 0$:

$$\begin{aligned} V\varepsilon F\tilde{\gamma}_0 &= (\Pi^2 - [\pi])\tilde{\gamma}_0 \\ &= [\tilde{a}_0]V\tilde{x}_1 + \Pi V\tilde{x}_0, \qquad \tilde{x}_i \in \widetilde{M}_i. \end{aligned}$$

De plus

$$[\tilde{a}_0]V\tilde{x}_1 = V[\tilde{a}_0^q]\tilde{x}_1$$

et

$$[\tilde{a}_0]\tilde{x}_1 \in \Pi\widetilde{M}_0 + V\widetilde{M}_0$$

donc il existe $\tilde{u}_0, \tilde{v}_0 \in \widetilde{M}_0$ tels que

$$[\tilde{a}_0]V\tilde{x}_1 = V\Pi[\tilde{a}_0]\tilde{u}_0 + V^2[\tilde{a}_0]\tilde{v}_0.$$

Comme $F = \lambda_{\widetilde{M}} L_{\widetilde{M}}$, il vient :

$$\lambda_{\widetilde{M}} L_{\widetilde{M}}\tilde{\gamma}_0 = \Pi\left(\varepsilon^{-1}\tilde{x}_0 + \varepsilon^{-1}[\tilde{a}_0]\tilde{u}_0\right) + V\left({}^{\sigma}\varepsilon^{-1}[\tilde{a}_0]\tilde{v}_0\right)$$

d'où étant donné l'injectivité de $\lambda_{\widetilde{M}}$:

$$L_{\widetilde{M}}\tilde{\gamma}_0 = \left(\left(\varepsilon^{-1}\tilde{x}_0 + \varepsilon^{-1}[\tilde{a}_0]\tilde{u}_0, {}^{\sigma}\varepsilon^{-1}[\tilde{a}_0]\tilde{v}_0\right)\right).$$

L'image de ε dans $W_{\mathcal{O}}(B)$ est 1 car $\pi B = 0$; en effet ${}^{\tau}\varepsilon = \pi - [\pi] = \pi = {}^{\tau\sigma}1$, donc $\varepsilon = {}^{\sigma}1 = 1$. L'image de $\tilde{a}_0$ dans B est nulle. D'où :

$$L_M\gamma_0 = ((x_0, 0)).$$

LEMME (4.3). — *Si i est un indice critique, l'application*

$$\rho : N(M)_i \longrightarrow M_i/VM_{i-1} \oplus M_i^\sigma$$
$$((m, m')) \longmapsto (\overline{m}, V^{-1}\Pi m + m')$$

est un isomorphisme $W_{\mathcal{O}}(B)$-linéaire.

[*On note $\overline{m}$ la classe de m modulo V. On remarquera que $V^{-1}\Pi m + m' = V^{-1}\lambda_M((m, m'))$*].

Démonstration. — On définit l'application inverse

$$\rho^{-1} : M_i/VM_{i-1} \oplus M_i^\sigma \longrightarrow N(M)_i$$
$$(\overline{m}, m'') \longmapsto ((m, -V^{-1}\Pi m + m'')).$$

L'application ρ^{-1} est bien définie : en effet, pour $m \in M_i$, $V^{-1}\Pi m$ est défini et l'application $m \mapsto ((m, -V^{-1}\Pi m))$ de M_i dans $N(M)_i$ est nulle sur VM_{i-1} car $Vm_1 \mapsto ((Vm_1, -\Pi m_1)) = 0$. Ces applications sont clairement $W_{\mathcal{O}}(B)$-linéaires et inverses l'une de l'autre, d'où le lemme.

LEMME (4.4). — *Si i est un indice critique, l'endomorphisme $\rho\varphi_M\rho^{-1}$ de $M_i/VM_{i-1} \oplus M_i^\sigma$ induit par φ_M via l'isomorphisme ρ est donné par*

$$\rho\varphi_M\rho^{-1}(\overline{m}, m'') = (\overline{m}'', V^{-1}\Pi m'').$$

Démonstration. — Cela résulte immédiatement des définitions de φ_M et ρ et du lemme (4.2) :

$$(0, m'') \xmapsto{\rho^{-1}} ((0, m'')) \xmapsto{\varphi_M} ((m'', 0)) \xmapsto{\rho} (\overline{m}'', V^{-1}\Pi m'')$$
$$(\overline{m}, 0) \xmapsto{\rho^{-1}} ((m, -V^{-1}\Pi m)) \xmapsto{\varphi_M} L_M m + ((-V^{-1}\Pi m, 0)) = 0$$

On en déduit :

PROPOSITION (4.5). — *Si i est un indice critique pour M, l'application $V^{-1}\lambda_M$ induit un isomorphisme $\mathcal{O}$-linéaire*

$$\eta_{M,i} = N(M)_i^{\varphi_M} \xrightarrow{\sim} M_i^{V^{-1}\Pi}.$$

Plus précisément $\eta_{M,i} = \left\{((m, 0))/m \in M_i^{V^{-1}\Pi}\right\}$ et la restriction de $V^{-1}\lambda_M$ à $\eta_{M,i}$ est l'application $((m, 0)) \mapsto m$.

Lorsqu'il existe un indice non critique, on utilisera les résultats suivants :

LEMME (4.6). — *Si l'application* $\Pi : M_j/VM_{j-1} \to M_{j+1}/VM_j$ *est un isomorphisme, l'application*

$$\begin{aligned} \lambda_M : N(M)_j &\to M_{j+1} \\ ((m, m')) &\longmapsto \Pi m + Vm' \end{aligned}$$

est un isomorphisme $W_{\mathcal{O}}(B)$*-linéaire.*

Démonstration. — D'après l'hypothèse sur Π, tout élément de M_{j+1} peut s'écrire $\Pi m + Vm'$, donc λ_M est surjectif.

Montrons que λ_M est injectif. Soient $m, m' \in M_j$ tels que $\Pi m + Vm' = 0$. Alors $\Pi m \in VM_j$, il existe donc $m'' \in M_{j-1}$ tel que $m = Vm''$. De plus $\Pi m + Vm' = V(\Pi m'' + m') = 0$, donc $m' = -\Pi m''$. Ainsi $((m, m')) = (Vm'', -\Pi m'')) = 0$.

LEMME (4.7). — *Sous l'hypothèse de (4.6), l'endomorphisme* $\lambda_M \varphi_M \lambda_M^{-1}$ *de* M_{j+1} *induit par* φ_M *via l'isomorphisme ci-dessus est égal à* $V^{-1}\Pi$.

Démonstration. — On notera que $j+1$ est nécessairement critique, puisque $\Pi^2 = 0$ sur M/VM. Pour $m, m' \in M_j$, on a :

$$\begin{aligned} \varphi_M((m, m')) &= L_M m + ((m', 0)) \\ \lambda_M \varphi_M((m, m')) &= Fm + \Pi m' \\ \lambda_M((m, m')) &= \Pi m + Vm' \\ (V^{-1}\Pi)\lambda_M((m, m')) &= V^{-1}\pi m + \Pi m' = Fm + \Pi m' \end{aligned}$$

d'où l'assertion.

PROPOSITION (4.8). — *Sous l'hypothèse de (4.6), l'application* λ_M *induit un isomorphisme* $\mathcal{O}$*-linéaire*

$$\eta_{M,j} = N(M)_j^{\varphi_M} \xrightarrow{\sim} M_{j+1}^{V^{-1}\Pi}.$$

De plus le diagramme :

$$\begin{array}{ccc} M_{j+1}^{V^{-1}\Pi} & \xlongequal{\text{id}} & M_{j+1}^{V^{-1}\Pi} \\ {\scriptstyle \lambda_M}\uparrow\iota & & \uparrow\iota\, {\scriptstyle V^{-1}\lambda_M} \\ \eta_{M,j} & \xrightarrow[\Pi]{} & \eta_{M,j+1} \end{array}$$

est commutatif.

Démonstration. — L'isomorphisme résulte des deux lemmes précédents. La commutativité du diagramme de celle du diagramme :

$$\begin{array}{ccc} M_{j+1} & \xrightarrow{V^{-1}\Pi} & M_{j+1} \\ {\scriptstyle \lambda_M}\uparrow & & \uparrow{\scriptstyle V^{-1}\lambda_M} \\ N(M)_j & \xrightarrow[\Pi]{} & N(M)_{j+1} \end{array}$$

puisque $V^{-1}\Pi \Big|_{M_{j+1}^{V^{-1}\Pi}} = \mathrm{id}$.

5. $\mathcal{O}_D$-modules formels spéciaux sur un corps algébriquement clos.

Dans ce paragraphe, on suppose que $B = L$ est un corps algébriquement clos de caractéristique p. On note $\mathcal{W} = W_{\mathcal{O}}(L)$ et $\mathcal{K}$ le corps des fractions de $\mathcal{W}$. L'anneau $\mathcal{W}$ est de valuation discrète complet d'uniformisante π et de corps résiduel L, il est muni d'un automorphisme σ tel que $\mathcal{W}^{\sigma} = \mathcal{O}$.

Si X est un $\mathcal{O}$-module formel (lisse) sur L, son module de Cartier M est un $\mathcal{W}$-module libre de rang fini. On appelle hauteur de X le rang de M sur $\mathcal{W}$.

PROPOSITION (5.1). — *Si X est un $\mathcal{O}_D$-module formel spécial, sa hauteur est multiple de 4.*

Démonstration. — Pour $M' \subset M''$ deux $\mathcal{W}$-modules libres, on notera $[M'' : M']$ la longueur du $\mathcal{W}$-module M''/M'. Par hypothèse on a $[M_0 : VM_1] = [M_1 : VM_0] = 1$ et V est injectif, donc M_0 et M_1 ont le même rang r sur $\mathcal{W}$ et $M = M_0 \oplus M_1$ est de rang $2r$. On a $\Pi^2 = \pi$, donc Π est injectif et

$$\begin{aligned} r = [M_0 : \pi M_0] &= [M_0 : \Pi M_1] + [\Pi M_1 : \Pi^2 M_0] \\ &= [M_0 : \Pi M_1] + [M_1 : \Pi M_0]. \end{aligned}$$

Des inclusions

$$\begin{array}{ccccc} \Pi V M_0 & \subset & VM_1 & \subset & \\ & \subset & \Pi M_1 & \subset & M_0, \end{array}$$

on déduit l'égalité

$$[M_0 : VM_1] + [VM_1 : \Pi VM_0] = [M_0 : \Pi M_1] + [\Pi M_1 : \Pi VM_0].$$

Or

$$[\Pi M_1 : \Pi VM_0] = [M_1 : VM_0] = [M_0 : VM_1] = 1$$

et

$$[VM_1 : \Pi VM_0] = [M_1 : \Pi M_0],$$

d'où

$$[M_1 : \Pi M_0] = [M_0 : \Pi M_1],$$

en particulier r est pair, d'où la proposition.

PROPOSITION (5.2). — *Il existe une seule classe d'isogénie de $\mathcal{O}_D$-modules formels spéciaux de hauteur 4.*

Démonstration. — On sait que la classe d'isogénie du $\mathcal{O}$-module formel X est déterminée par l'isocristal $(M \otimes_{\mathcal{W}} \mathcal{K}, V)$. Celui-ci est bien déterminé par l'isocristal $(M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})$, puisque $M_1 \otimes_{\mathcal{W}} \mathcal{K}$ s'identifie via Π à $M_0 \otimes_{\mathcal{W}} \mathcal{K}$.

Or $(M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})$ est un isocristal unité : si i est critique, M_i est un réseau stable par $V\Pi^{-1}$ dans $M_i \otimes_{\mathcal{W}} \mathcal{K}$ et $V\Pi^{-1}|_{M_i}$ est bijectif. Puisque L est algébriquement clos, un tel isocristal est unique à isomorphisme près ; il existe une base e_1, e_2 de M_i sur $\mathcal{W}$ telle que $V\Pi^{-1}e_1 = e_1$ et $V\Pi^{-1}e_2 = e_2$.

Remarque (5.2'). Le $\mathcal{O}$-module formel X est isogène à la somme de deux $\mathcal{O}$-modules formels de dimension 1 et de hauteur 2. Autrement dit l'isocristal $(M \otimes_{\mathcal{W}} \mathcal{K}, V)$ est de dimension 2 et de pente 1/2.

PROPOSITION (5.3). — *On a* $\mathrm{End}_D^0 X \simeq M_2(K)$. [*On note* $\mathrm{End}_D^0 X = \mathrm{End}_{\mathcal{O}_D} X \otimes \mathbb{Q}$].

Démonstration. — Les correspondances $X \mapsto (M \otimes_{\mathcal{W}} \mathcal{K}, V) \mapsto (M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})$ induisent des isomorphismes

$$\mathrm{End}_D^0 X = \mathrm{End}_D(M \otimes_{\mathcal{W}} \mathcal{K}, V) = \mathrm{End}_K(M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1}).$$

Enfin $\mathrm{End}_K(M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1}) \simeq M_2(K)$, puisque $(M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})$ est un isocristal unité de rang 2 : un endomorphisme $\mathcal{K}$-linéaire de $M_0 \otimes_{\mathcal{W}} \mathcal{K}$ commute à l'application σ^{-1}-linéaire $V\Pi^{-1}$ si et seulement si sa matrice dans la base e_1, e_2 est à coefficients dans $\mathcal{K}^\sigma = K$.

On suppose dorénavant que X est un $\mathcal{O}_D$-module formel spécial de *hauteur* 4. Alors

$$[M_1 : \Pi M_0] = [M_0 : \Pi M_1] = 1.$$

En particulier, si i est critique, on a $\Pi M_i = VM_i$.

(5.4) Rappelons que, pour toute $\mathcal{O}$-algèbre B, on note $B[\Pi]$ l'algèbre commutative $\mathbf{Z}/2\mathbf{Z}$-graduée engendrée par B en degré 0 et un élément Π de degré 1 tel que $\Pi^2 = \pi$ (I.5).

On associe à X un triplet (η, T, u) où

(i) η est un $\mathcal{O}[\Pi]$-module gradué,

(ii) T est un $L[\Pi]$-module gradué dont les composantes homogènes T_0 et T_1 sont de dimension 1,

(iii) $u : \eta \to T$ est une application $\mathcal{O}[\Pi]$-linéaire de degré 0,

en posant $\eta = \eta_M$, $T = M/VM$ et en définissant u par composition de l'inclusion $\eta_M \subset N(M)$ et de l'application $((m, m')) \mapsto \overline{m}$ de $N(M)$ dans M/VM.

PROPOSITION (5.5). — *Les composantes homogènes η_0 et η_1 de η sont des $\mathcal{O}$-modules libres de rang 2 et l'application $\eta \otimes_{\mathcal{O}} L \to T$ est surjective.*

Démonstration. — Si i est critique, on a vu en (4.5) que η_i s'identife à $M_i^{V^{-1}\Pi}$ et $u_i : \eta_i \to T_i$ à l'application composée $M_i^{V^{-1}\Pi} \hookrightarrow M_i \twoheadrightarrow M_i/VM_{i-1}$. L'endomorphisme σ-linéaire $V^{-1}\Pi : M_i \to M_i$ est bijectif, autrement dit $(M_i, V^{-1}\Pi)$ est un cristal unité sur L et L est algébriquement clos. Par suite $M_i^{V^{-1}\Pi}$ est un $\mathcal{O}$-module libre de rang 2 et l'application $M_i^{V^{-1}\Pi} \otimes_{\mathcal{O}} \mathcal{W} \to M_i$ est bijective, en particulier l'application $M_i^{V^{-1}\Pi} \otimes_{\mathcal{O}} L \to M_i/VM_{i-1}$ est surjective.

Si j n'est pas critique, on a d'après (4.8) un diagramme commutatif

$$\begin{array}{ccc} \eta_j & \xrightarrow[\sim]{\Pi} & \eta_{j+1} \\ {\scriptstyle u_j}\downarrow & & \downarrow{\scriptstyle u_{j+1}} \\ T_j & \xrightarrow[\Pi]{\sim} & T_{j+1} \end{array}$$

où les flèches horizontales induites par Π sont des isomorphismes, et $j+1$ est critique, d'où la proposition.

PROPOSITION (5.6). — *L'application $\eta/\Pi\eta \to T/\Pi T$, induite par u, est injective.*

Démonstration. — Pour vérifier que $\eta_i/\Pi\eta_{i-1} \to T_i/\Pi T_{i-1}$ est injectif, on distinguera trois cas.

1^{er} *cas : i critique et* $i-1$ *non critique* – On a alors $\Pi\eta_{i-1} = \eta_i$ et l'assertion est évidente.

2^{e} *cas : i et* $i-1$ *critiques* – On a un diagramme commutatif

$$\begin{array}{ccc}
\eta_{i-1} & \xrightarrow{\Pi} & \eta_i \\
\downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\
M_{i-1}^{V^{-1}\Pi} & \xrightarrow{\Pi} & M_i^{V^{-1}\Pi} \\
\downarrow & & \downarrow \\
T_{i-1} & \xrightarrow{\Pi=0} & T_i.
\end{array}$$

Si $x \in M_i^{V^{-1}\Pi}$ a une image nulle dans T_i, il existe $y \in M_{i-1}$ tel que $x = Vy$. Mais, de $\Pi x = Vx$, on déduit $\Pi y = Vy$, autrement dit $y \in M_{i-1}^{V^{-1}\Pi}$ et $x = \Pi y$.

3^{e} *cas : i non critique et* $i-1$ *critique* – Le diagramme commutatif

$$\begin{array}{ccccc}
\eta_{i-1} & \xrightarrow{\Pi} & \eta_i & \underset{\sim}{\xrightarrow{\Pi}} & \eta_{i-1} \\
\downarrow{\scriptstyle u_{i-1}} & & \downarrow{\scriptstyle u_i} & & \downarrow{\scriptstyle u_{i-1}} \\
T_{i-1} & \underset{\Pi=0}{\xrightarrow{\quad}} & T_i & \underset{\Pi}{\xrightarrow{\sim}} & T_{i-1}
\end{array}$$

montre qu'il s'agit alors de vérifier que l'application $\eta_{i-1}/\pi\eta_{i-1} \to T_{i-1}$ induite par u_{i-1} est injective. De plus $u_{i-1} : \eta_{i-1} \to T_{i-1}$ s'identifie à $M_{i-1}^{V^{-1}\Pi} \to M_{i-1}/VM_i$.

Si $x \in M_{i-1}^{V^{-1}\Pi}$ a une image nulle dans M_{i-1}/VM_i, il existe $y \in M_i$ tel que $x = Vy$. De $\Pi x = Vx$, on déduit $\Pi y = Vy$; en particulier l'image $\overline{y}$ de y dans M_i/VM_{i-1} est nulle, car $\Pi\overline{y} = \overline{x} = 0$ et $\Pi : M_i/VM_{i-1} \to M_{i-1}/VM_i$ est un isomorphisme. Donc il existe $z \in M_{i-1}$ tel que $y = Vz$.

Mais encore une fois de $\Pi y = Vy$, on déduit $\Pi z = Vz$; d'où $z \in M_{i-1}^{V^{-1}\Pi}$ et $x = \pi z$.

PROPOSITION (5.7). — *Le triplet (η, T, u) détermine X à isomorphisme unique près.*

Démonstration. — Il suffit de montrer que M_0, M_1, Π et V sont déterminés par (η, T, u).

Si i est un indice critique et σ l'automorphisme $\mathrm{id} \otimes \sigma$ de $\eta_i \otimes_{\mathcal{O}} \mathcal{W}$, l'inclusion $\eta_i \subset M_i$ induit un isomorphisme $(\eta_i \otimes_{\mathcal{O}} \mathcal{W}, \sigma) \simeq (M_i, \Pi V^{-1})$. De plus, si

$$\mathcal{H} = \mathrm{Ker}\,\{\eta_i \otimes_{\mathcal{O}} \mathcal{W} \xrightarrow{u_i \otimes \mathrm{id}} T_i\},$$

l'isomorphisme ci-dessus identifie $\mathcal{H}$ à VM_{i-1} et $\sigma(\mathcal{H})$ à ΠM_{i-1}. Ainsi le diagramme

$$M_{i-1} \underset{V}{\overset{\Pi}{\rightrightarrows}} M_i \underset{V}{\overset{\Pi}{\rightrightarrows}} M_{i-1}$$

s'identifie au diagramme

$$\sigma(\mathcal{H}) \underset{\mathrm{incl}\circ\sigma^{-1}}{\overset{\mathrm{incl}}{\rightrightarrows}} \eta_i \otimes_{\mathcal{O}} \mathcal{W} \underset{\pi\circ\sigma^{-1}}{\overset{\pi}{\rightrightarrows}} \sigma(\mathcal{H}).$$

DÉFINITION (5.8). — Un triplet (η, T, u) est dit *admissible* s'il vérifie les conditions (5.5) et (5.6). Un indice $i \in \{0, 1\}$ est dit *critique* pour (η, T, u) si $\Pi : T_i \to T_{i+1}$ est nul.

LEMME (5.9). — *Un triplet admissible (η, T, u) est déterminé à isomorphisme unique près par (η_i, T_i, u_i) pour i critique.*

Démonstration. — Notons $H = \mathrm{Ker}\, u_i$. On a $\pi\eta_i \subset H \subset \eta_i$ et $H \neq \eta_i$ d'après (5.5).

Si $i - 1$ n'est pas critique, on a $\Pi T_{i-1} = T_i$, donc $\Pi\eta_{i-1} = \eta_i$, d'après (5.6). Par suite le diagramme

$$\begin{array}{ccccc}
\eta_i & \xrightarrow{\Pi} & \eta_{i-1} & \xrightarrow{\Pi} & \eta_i \\
\downarrow{\scriptstyle u_i} & & \downarrow{\scriptstyle u_{i-1}} & & \downarrow{\scriptstyle u_i} \\
T_i & \xrightarrow{0} & T_{i-1} & \xrightarrow{\Pi} & T_i
\end{array}$$

s'identifie au diagramme

$$\begin{array}{ccccc} \eta_i & \xrightarrow{\pi} & \eta_i & \xrightarrow{\mathrm{id}} & \eta_i \\ \downarrow{\scriptstyle u_i} & & \downarrow{\scriptstyle u_i} & & \downarrow{\scriptstyle u_i} \\ T_i & \xrightarrow{0} & T_i & \xrightarrow{\mathrm{id}} & T_i. \end{array}$$

De plus la condition (5.6) implique dans ce cas $H = \pi\eta_i$.

Si $i-1$ est critique, on a $\Pi\eta_{i-1} \neq \eta_i$; sinon on aurait $u_i = 0$ ce qui contredirait (5.5). De même, puisque i est critique, on a $\Pi\eta_i \neq \eta_{i-1}$, donc $\pi\eta_i \neq \Pi\eta_{i-1}$. Alors, d'après (5.6), u_i et $u_{i-1}\Pi^{-1}$ induisent des isomorphismes

$$\eta_i/\Pi\eta_{i-1} \otimes_k L \xrightarrow{\sim} T_i \text{ et } \Pi\eta_{i-1}/\pi\eta_i \otimes_k L \xrightarrow{\sim} T_{i-1}.$$

On a dans ce cas $H = \Pi\eta_{i-1} \neq \pi\eta_i$ et le diagramme

$$\begin{array}{ccccc} \eta_i & \xrightarrow{\Pi} & \eta_{i-1} & \xrightarrow{\Pi} & \eta_i \\ \downarrow{\scriptstyle u_i} & & \downarrow{\scriptstyle u_{i-1}} & & \downarrow{\scriptstyle u_i} \\ T_i & \xrightarrow{0} & T_{i-1} & \xrightarrow{0} & T_i \end{array}$$

s'identifie au diagramme

$$\begin{array}{ccccc} \eta_i & \xrightarrow{\pi} & H & \xrightarrow{\mathrm{incl}} & \eta_i \\ \downarrow & & \downarrow & & \downarrow \\ \eta_i/H \otimes_k L & \xrightarrow{0} & H/\pi\eta_i \otimes_k L & \xrightarrow{0} & \eta_i/H \otimes_k L \end{array}$$

où les flèches verticales sont les applications canoniques.

Remarquons qu'on reconnait si $i-1$ est ou n'est pas critique selon que $H \neq \pi\eta_i$ ou $H = \pi\eta_i$; la démonstration du lemme est donc complète.

PROPOSITION (5.10). — *Tout triplet admissible (η, T, u) est isomorphe au triplet associé à un $\mathcal{O}_D$-module formel spécial de hauteur 4.*

Démonstration. — Soient i un indice critique, σ l'automorphisme $\mathrm{id}\otimes\sigma$ de $\eta_i \otimes_{\mathcal{O}} \mathcal{W}$ et $\mathcal{H} = \mathrm{Ker}\{u_i \otimes \mathrm{id} : \eta_i \otimes_{\mathcal{O}} \mathcal{W} \to T_i\}$. Comme $\eta_i \otimes_{\mathcal{O}} L \to T_i$ est surjectif, on a $\pi(\eta_i \otimes_{\mathcal{O}} \mathcal{W}) \subsetneqq \mathcal{H} \subsetneqq \eta_i \otimes_{\mathcal{O}} \mathcal{W}$; de même pour $\sigma(\mathcal{H})$.

Définissons le diagramme

$$M_{i-1} \underset{V}{\overset{\Pi}{\rightleftarrows}} M_i \underset{V}{\overset{\Pi}{\rightleftarrows}} M_{i-1}$$

comme égal au diagramme

$$\sigma(\mathcal{H}) \underset{\mathrm{incl}\circ\sigma^{-1}}{\overset{\mathrm{incl}}{\rightleftarrows}} \eta_i \otimes_{\mathcal{O}} \mathcal{W} \underset{\pi\circ\sigma^{-1}}{\overset{\pi}{\rightleftarrows}} \sigma(\mathcal{H}).$$

Ainsi V est σ^{-1} linéaire, Π est linéaire, $\Pi^2 = \pi$ et

$$[M_i : VM_{i-1}] = [M_{i-1} : VM_i] = [M_i : \Pi M_{i-1}] = [M_{i-1} : \Pi M_i] = 1,$$

donc (M, Π, V) est le module de Cartier d'un $\mathcal{O}_D$-module formel spécial de hauteur 4.

L'indice i est critique pour M, la composante homogène d'indice i du triplet admissible associé à M est

$$(M_i^{V\Pi^{-1}}, M_i/VM_{i-1}, \mathrm{can.}) \simeq (\eta_i, \eta_i \otimes_{\mathcal{O}} \mathcal{W}/\mathcal{H}, \mathrm{can}) \simeq)(\eta_i, T_i, u_i),$$

par suite ce triplet est isomorphe à (η, T, u).

On peut résumer les propositions précédentes en un seul énoncé :

THÉORÈME (5.11). — *Sur un corps algébriquement clos de caractéristique p, la correspondance $X \mapsto (\eta, T, u)$ réalise une équivalence de catégories entre d'une part le groupoïde des $\mathcal{O}_D$-modules formels spéciaux de hauteur 4 et de leurs isomorphismes, d'autre part le groupoïde des triplets admissibles et de leurs isomorphismes.*

LEMME (5.12). — *Soit (η, T, u) le triplet admissible associé à un $\mathcal{O}_D$-module formel spécial de hauteur 4 de module de Cartier M. Alors, quel que soit $i \in \{0, 1\}$, l'isocristal $(M_i \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})$ est canoniquement isomorphe à $(\eta_i \otimes_{\mathcal{O}} \mathcal{K}, \sigma^{-1})$.*

Démonstration. — Pour i critique, $(M_i, V\Pi^{-1})$ est un cristal unité, autrement dit $V\Pi^{-1}$ est une application σ^{-1}-linéaire bijective de M_i dans

M_i, de plus η_i s'identifie à $M_i^{V\Pi^{-1}}$ (4.5). Il résulte alors du théorème de structure des cristaux unités ([Zi 3], Satz 6.26) que $(M_i, V\Pi^{-1})$ s'identifie à $(\eta_i \otimes_{\mathcal{O}} \mathcal{W}, \sigma^{-1})$, a fortiori l'isocristal $(M_i \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})$ s'identifie à $(\eta_i \otimes_{\mathcal{O}} \mathcal{K}, \sigma^{-1})$.

Par ailleurs Π induit des isomorphismes d'isocristaux :

$$(M_i \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1}) \xrightarrow{\sim} (M_{i+1} \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1}),$$
$$(\eta_i \otimes_{\mathcal{O}} \mathcal{K}, \sigma^{-1}) \xrightarrow{\sim} (\eta_{i+1} \otimes_{\mathcal{O}} \mathcal{K}, \sigma^{-1});$$

lesquels sont compatibles aux isomorphismes précédents lorsque 0 et 1 sont tous deux critiques.

DÉFINITION (5.13). — Soient X et X' deux $\mathcal{O}_D$-modules formels spéciaux de hauteur 4 sur L. On appelle *quasiisogénie* entre X et X' un élément de $\mathrm{Hom}_{\mathcal{O}_D}(X, X') \otimes_{\mathcal{O}} K$ inversible dans $\mathrm{Hom}_{\mathcal{O}_D}(X', X) \otimes_{\mathcal{O}} K$. Autrement dit, si α est une quasiisogénie de X dans X', il existe $n \geq 0$ tel que $\pi^n \alpha$ soit une $\mathcal{O}_D$-isogénie de X dans X'. On dira que α est de *hauteur* 0 si $h(\pi^n \alpha) = h(\pi^n)$.

PROPOSITION (5.14). — *Soient (η, T, u) et (η', T', u') les triplets admissibles associés à X et X'. On a alors un isomorphisme canonique :*

$$\mathrm{Quasiisog}(X, X') \simeq \mathrm{Isom}_K(\eta_0 \otimes_{\mathcal{O}} K, \eta_0' \otimes_{\mathcal{O}} K).$$

Démonstration. — Soient M et M' les modules de Cartier de X et X'. On a, d'après (2.2), un isomorphisme canonique :

$$\mathrm{Quasiisog}(X, X') = \mathrm{Isom}((M \otimes_{\mathcal{W}} \mathcal{K}, V), (M' \otimes_{\mathcal{W}} \mathcal{K}, V)),$$

où les isomorphismes d'isocristaux du membre de droite doivent être compatibles à la graduation et à l'action de Π ; ils sont donc déterminés par leur action sur la composante homogène de degré 0, plus précisément, on a :

$$\mathrm{Isom}((M \otimes_{\mathcal{W}} \mathcal{K}, V), (M' \otimes_{\mathcal{W}} \mathcal{K}, V)) = \mathrm{Isom}((M_0 \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1}), (M_0' \otimes_{\mathcal{W}} \mathcal{K}, V\Pi^{-1})).$$

On conclut grâce au lemme (5.12).

PROPOSITION (5.15). — *Supposons 0 critique pour X. Alors, dans l'isomorphisme précédent, les quasiisogénies de hauteur 0 correspondent aux isomorphismes $r : \eta_0 \otimes_{\mathcal{O}} K \xrightarrow{\sim} \eta_0' \otimes_{\mathcal{O}} K$ tels que :*

$$[\eta_0' : r(\eta_0)] = 0 \text{ si } 0 \text{ est critique pour } X',$$
$$[\eta_1' : \Pi r(\eta_0)] = 1 \text{ si } 1 \text{ est critique pour } X';$$

autrement dit, tels que $\bigwedge^2 \eta_i' = \pi^{-i} \bigwedge^2 \Pi^i r(\eta_0)$ *si* $i \in \{0,1\}$ *est critique pour* X'.

Démonstration. — Une quasiisogénie est de hauteur 0 si et seulement si l'isomorphisme $\alpha : M \otimes_{\mathcal{W}} \mathcal{K} \xrightarrow{\sim} M' \otimes_{\mathcal{W}} \mathcal{K}$ correspondant est tel que $[M' : \alpha(\pi^n M)] = [M : \pi^n M]$ pour n tel que $\alpha(\pi^n M) \subset M'$, autrement dit si $[M' : \alpha(M)] = 0$. Puisque $[M_1 : \Pi M_0] = [M_0 : \Pi M_1] = 1$, et de même pour M', il revient au même de demander $[M_0' : \alpha(M_0)] = 0$ ou $[M_1' : \Pi\alpha(M_0)] = 1$.

Puisque 0 est critique pour X, M_0 s'identifie à $\eta_0 \otimes_{\mathcal{O}} \mathcal{W}$. Si 0 est également critique pour X', M_0' s'identifie à $\eta_0' \otimes_{\mathcal{O}} \mathcal{W}$ et $[M_0' : \alpha(M_0)] = [\eta_0' : r(\eta_0)]$. Si 1 est critique pour X', c'est M_1' qui s'identifie à $\eta_1' \otimes_{\mathcal{O}} \mathcal{W}$ et $[M_1' : \Pi\alpha(M_0)] = [\eta_1' : \Pi r(\eta_0)]$.

(5.16) Soit $\overline{k}$ une clôture algébrique de $k = \mathcal{O}/\pi\mathcal{O}$. Choisissons un $\mathcal{O}_D$-module formel spécial Φ de hauteur 4 sur $\overline{k}$ tel que 0 soit critique pour Φ (un tel module est unique à isogénie près d'après (5.2)) et fixons un isomorphisme $\mathcal{O}^2 \simeq \eta_{0,\Phi}$.

Un $\mathcal{O}_D$-module formel spécial X de hauteur 4 sur un corps L extension de $\overline{k}$ est dit *rigidifié* s'il est muni d'une quasiisogénie de hauteur zéro $\rho : \Phi_L \to X$.

Un triplet admissible (η, T, u) sur L est dit *rigidifié* s'il est muni d'un isomorphisme $r : K^2 \xrightarrow{\sim} \eta_0 \otimes_{\mathcal{O}} K$ tel que $[\eta_i : \Pi^i r(\mathcal{O}^2)] = i$ si $i \in \{0,1\}$ est critique pour η, autrement dit $\bigwedge^2 \eta_i = \pi^{-i} \bigwedge^2 \Pi^i r(\mathcal{O}^2)$ si i est critique.

D'après ce qui précède, si (η, T, u) est associé à X, une rigidification ρ de X correspond à une rigidification r de (η, T, u), et on a :

THÉORÈME (5.17). — *Soit L un corps algébriquement clos extension de $\overline{k}$. La correspondance $(X, \rho) \mapsto (\eta, T, u, r)$ réalise une bijection entre l'ensemble des classes d'isomorphie de $\mathcal{O}_D$-modules formels spéciaux de hauteur 4 rigidifiés sur L et celui des classes d'isomorphie de triplets admissibles rigidifiés sur L.*

Rappelons (I.5.2) que ce dernier ensemble s'identife à $\widehat{\Omega}(L)$.

6. Filtration de $N(M)$ et η_M.

(6.1) Dans ce paragraphe, B est une $\mathcal{O}'$-algèbre telle que $\pi B = 0$ et M un $\mathcal{O}[\Pi]$-module de Cartier gradué spécial sur B. De plus on suppose que $i \in \{0,1\}$ est un indice critique, autrement dit $\Pi M_i \subset VM_i$. Nous noterons pour simplifier $N = N(M)$, $\varphi = \varphi_M$ et $\eta = \eta_M$.

Considérons les filtrations de N_i et N_{i-1} par les sous-$\mathcal{O}$-modules

$$V^{2n}M_i = ((0, V^{2n}M_i)) \subset N_i$$
$$V^{2n-1}M_i = ((0, V^{2n-1}M_i)) \subset N_{i-1}$$

pour $n > 0$. Soient $N_{i,n} = N_i/V^{2n}M_i$ et $N_{i-1,n} = N_{i-1}/V^{2n-1}M_i$. Pour $j \in \{0,1\}$, on posera $\varepsilon = 0$ si $j = i$ et $\varepsilon = 1$ si $j \equiv i-1$, de sorte que $N_{j,n} = N_j/V^{2n-\varepsilon}M_i$.

LEMME (6.2). — *Pour tout $r > 0$, on a $\varphi(V^rM_i) \subset V^rM_i$.*

Démonstration. — Pour $m \in M_i$, on a

$$\varphi((0, V^rm)) = ((V^rm, 0)) = ((0, \Pi V^{r-1}m)),$$

mais $\Pi m \in \Pi M_i \subset VM_i$, donc $\Pi V^{r-1}m = V^{r-1}\Pi m \in V^rM_i$.

Ainsi φ induit un endomorphisme $\mathcal{O}$-linéaire de $N_{j,n}$. Dans la suite, on notera $\eta_{j,n} = \{z \in N_{j,n}/\varphi(z) = z\}$.

LEMME (6.3). — *On a $N_j = \varprojlim N_{j,n}$ et $\eta_j = \varprojlim \eta_{j,n}$.*

Démonstration. — Considérons la suite exacte de $\mathcal{O}$-modules définissant N_j :

$$0 \longrightarrow M_{j-1} \xrightarrow{\alpha} M_j \oplus M_j \longrightarrow N_j \longrightarrow 0. \tag{6.3.1}$$
$$\alpha(m) = (Vm, -\Pi m).$$

Puisque V est injectif, on a $\alpha(M_{j-1}) \cap (0, V^{2n-\varepsilon}M_i) = \{0\}$; d'où un système projectif de suites exactes :

$$0 \to M_{j-1} \to M_j \oplus M_j/V^{2n-\varepsilon}M_i \to N_{j,n} \to 0,$$

et, en passant à la limite projective, une suite exacte :

$$0 \to M_{j-1} \to M_j \oplus \varprojlim M_j/V^{2n-\varepsilon}M_i \to \varprojlim N_{j,n} \to 0.$$

Mais M est complet pour la topologie V-adique, d'où $M_j = \varprojlim M_j/V^{2n-\varepsilon}M_i$ et $N_j = \varprojlim N_{j,n}$.

L'assertion correspondante pour η_j s'en déduit en prenant le noyau de $1 - \varphi$.

(6.4) Nous considèrerons dans la suite de ce pararaphe $M_j, N_j, \eta_j, N_{j,n}, \eta_{j,n}$ comme des foncteurs sur la catégorie des B-algèbres : pour une telle algèbre B', $M(B') = M\widehat{\otimes}_{E'_{\mathcal{O}}(B)}E'_{\mathcal{O}}(B')$ est un $\mathcal{O}[\Pi]$-module de Cartier gradué

spécial sur B' et $N_j(B')$, $\eta_j(B')$, $N_{j,n}(B')$, $\eta_{j,n}(B')$ sont obtenus à partir de $M(B')$ par les constructions précédentes; les flèches de transition sont définies de manière évidente, compte-tenu du fait que φ a été construit de manière compatible au changement de base.

LEMME (6.5). — *Le foncteur $N_{j,n}$ est représentable par un schéma en $\mathcal{O}$-modules affine sur B dont le schéma sous-jacent est l'espace affine de dimension $2n+1-\varepsilon$ sur B.*

Démonstration. — Soit (γ_0, γ_1) une V-base homogène de M et soit $M_{j,(0)}$ le sous-foncteur en ensembles de M_j défini par

$$M_{j,(0)}(B') = \{[a]\gamma_j \quad ; a \in B'\}.$$

La suite exacte (6.3.1) définit une application naturelle :

$$M_{j,(0)} \times M_j/V^{2n-\varepsilon}M_i \to N_{j,n}.$$

Cette application est bijective.

En effet, soient $m, m' \in M_j$; on a $m = m_0 + Vm_1$ avec $m_0 \in M_{j,(0)}$ et $m_1 \in M_{j-1}$, d'où $((m, m')) = ((m_0, m' + \Pi m_1))$ dans N_j.

De plus, soient m_0 et $\ell_0 \in M_{j,(0)}$, m' et $\ell' \in M_j$, tels que $((m_0, m'))$ et $((\ell_0, \ell'))$ aient même image dans $N_{j,n}$; d'après (6.3.1), il existe $m_1 \in M_{j-1}$ tel que

$$\begin{aligned} m_0 + Vm_1 &= \ell_0 \\ m' - \Pi m_1 &\equiv \ell' \pmod{V^{2n-\varepsilon}M_i}. \end{aligned}$$

De la première égalité résulte nécessairement $m_1 = 0$, d'où l'assertion.

Par ailleurs les applications

$$\begin{aligned} B' &\longrightarrow M_{j,(0)}(B') \\ a &\longmapsto [a]\gamma_j \end{aligned}$$

et

$$\begin{aligned} B'^{2n-\varepsilon} &\longrightarrow M_j/V^{2n-\varepsilon}M_i(B') \\ (a_k) &\longmapsto \sum_{0 \le k < 2n-\varepsilon} V^k[a_k]\gamma_{j-k} \end{aligned}$$

sont fonctorielles et bijectives. On obtient ainsi une bijection fonctorielle entre $\mathbf{A}^{2n+1-\varepsilon}$ et $N_{j,n}$.

LEMME (6.6). — *Le foncteur $\eta_{j,n}$ est représentable par un schéma en $\mathcal{O}$-modules affine de présentation finie et étale sur B.*

Démonstration. — En effet $\eta_{j,n} = \mathrm{Ker}\{1-\varphi : N_{j,n} \to N_{j,n}\}$ est l'image réciproque de la section nulle de $N_{j,n}$ par $1-\varphi$ et cette section, qui coïncide

via l'isomorphisme précédent avec la section nulle de $\mathbf{A}^{2n+1-\varepsilon}$, est une immersion fermée de présentation finie. Ainsi $\eta_{j,n} \hookrightarrow N_{j,n}$ est également une immersion fermée de présentation finie.

Pour montrer que $\eta_{j,n}$ est étale sur B reste à vérifier que, si $B' \to B''$ est une surjection de B-algèbres définie par un idéal de carré nul, l'application $\eta_{j,n}(B') \to \eta_{j,n}(B'')$ est bijective. Or, dans le diagramme à lignes exactes :

$$\begin{array}{ccccccccc} 0 & \to & V^{2n-\varepsilon}M_i(B') & \longrightarrow & N_j(B') & \longrightarrow & N_{j,n}(B') & \to & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \to & V^{2n-\varepsilon}M_i(B'') & \longrightarrow & N_j(B'') & \longrightarrow & N_{j,n}(B'') & \to & 0, \end{array}$$

α et β sont surjectifs (3.7), donc γ est surjectif et φ est nilpotent sur $\operatorname{Ker}\gamma$ puisqu'il l'est sur $\operatorname{Ker}\beta$ (3.12) dont $\operatorname{Ker}\gamma$ est un quotient.

En d'autres termes, $\eta_{j,n}$ est un faisceau constructible pour la topologie étale sur Spec(B) et sa formation est compatible au changement de base. Notons $S = \operatorname{Spec}(B)$ et soit S_{i-1} le fermé de S où $i-1$ est critique. On a plus précisément :

PROPOSITION (6.7).

(1) *$\eta_{i,n}$ est un faisceau lisse* [1] *sur S en $\mathcal{O}/\pi^n$-modules libres de rang 2.*

(2) *$\eta_{i-1,n}$ est constructible sur S et $\Pi : \eta_{i-1,n} \to \eta_{i,n}$ est injectif, de plus :*

(2a) *$\eta_{i-1,n}\big|_{S-S_{i-1}}$ est lisse et $\Pi\big|_{S-S_{i-1}}$ est un isomorphisme.*

(2b) *$\eta_{i-1,n}\big|_{S_{i-1}}$ est lisse et $(\eta_{i,n}/\Pi\eta_{i-1,n})\big|_{S_{i-1}}$ est lisse en $\mathcal{O}/\pi$-vectoriels de rang 1.*

Démonstration. — Compte-tenu de ce qui précède, pour vérifier la lissité des faisceaux ci-dessus, il suffit de s'assurer que le cardinal de leurs fibres en les points géométriques de S est constant. On peut donc, pour démontrer la proposition, supposer que $B = L$ est un corps algébriquement clos de caractéristique p.

(1) D'après (4.3), on a un isomorphisme

$$N_{i,n} \simeq M_i/VM_{i-1} \oplus M_i/V^{2n}M_i$$

[1] lisse = localement constant pour la topologie étale.

tel que l'endomorphisme φ de $N_{i,n}$ corresponde à

$$(\overline{m}, \overline{m}'') \longmapsto (\overline{m}'', V^{-1}\Pi\overline{m}'').$$

D'où un isomorphisme :

$$\eta_{i,n} \simeq (M_i/V^{2n}M_i)^{V^{-1}\Pi}.$$

Identifions $(M_i, V^{-1}\Pi)$ à $(\eta_i \otimes_{\mathcal{O}} W, \sigma)$; alors V^2 s'identifie à $\pi.\sigma^{-2}$ et $V^{2n}M_i$ à $\pi^n\eta_i \otimes_{\mathcal{O}} W$; d'où

$$\eta_{i,n} \simeq \eta_i/\pi^n\eta_i \simeq (\mathcal{O}/\pi^n)^2.$$

(2) L'application $\Pi : N_{i-1} \to N_i$ est injective et $\Pi N_{i-1} \cap V^{2n}M_i = V^{2n}M_i = \Pi V^{2n-1}M_i$, donc $\Pi : N_{i-1,n} \to N_{i,n}$ est injective. A fortiori l'application $\Pi : \eta_{i-1,n} \to \eta_{i,n}$ induite sur les invariants sous φ est injective.

(2a) Si $i-1$ n'est pas critique, on a d'après (4.6) un isomorphisme :

$$N_{i-1,n} \simeq M_i/V^{2n}M_i$$

tel que φ corresponde à $V^{-1}\Pi$, d'où un isomorphisme

$$\eta_{i-1,n} \simeq (M_i/V^{2n}M_i)^{V^{-1}\Pi} \simeq \eta_{i,n}.$$

(2b) Si $i-1$ est critique, on a comme en (1) un isomorphisme

$$\eta_{i-1,n} \simeq (M_{i-1}/V^{2n-1}M_i)^{V^{-1}\Pi}.$$

De plus le diagramme

$$M_{i-1} \underset{V}{\overset{\Pi}{\rightleftarrows}} M_i \underset{V}{\overset{\Pi}{\rightleftarrows}} M_{i-1}$$

s'identifie à

$$\eta_{i-1} \otimes_{\mathcal{O}} \mathcal{W} \underset{\Pi\circ\sigma^{-1}}{\overset{\Pi}{\rightleftarrows}} \eta_i \otimes_{\mathcal{O}} \mathcal{W} \underset{\Pi\circ\sigma^{-1}}{\overset{\Pi}{\rightleftarrows}} \eta_{i-1} \otimes_{\mathcal{O}} \mathcal{W}.$$

Les inclusions $\Pi V^{2n-1}M_i = V^{2n}M_i \subset \Pi M_{i-1} \subset M_i$ sont σ-invariantes et se déduisent en tensorisant par $\mathcal{W}$ des inclusions $\pi^n\eta_i \subset \Pi\eta_{i-1} \subset \eta_i$. D'où

$$\eta_{i-1,n} \simeq \Pi\eta_{i-1}/\pi^n\eta_i;$$

de plus on a dans ce cas $[\eta_i : \Pi\eta_{i-1}] = 1$, donc

$$\eta_{i,n}/\Pi\eta_{i-1,n} \simeq \mathcal{O}/\pi.$$

Remarque (6.8). Les calculs précédents montrent de plus que, pour $j \in \{0,1\}$ et $m \geq n$, les applications canoniques $\eta_{j,m} \otimes_{\mathcal{O}} \mathcal{O}/\pi^n \to \eta_{j,n}$ sont des isomorphismes. Ainsi le système projectif $\eta_{j,n}$ définit un *faisceau π-adique* η_j. La proposition (6.7) se réécrit :

PROPOSITION (6.9).

(1) *η_i est un faisceau π-adique lisse en $\mathcal{O}$-modules libres de rang 2.*

(2) *η_{i-1} est un faisceau π-adique constructible en $\mathcal{O}$-modules libres de rang 2 et $\Pi : \eta_{i-1} \to \eta_i$ est injectif, de plus :*

(2a) *$\eta_{i-1}\,|_{S-S_{i-1}}$ est lisse et $\Pi\,|_{S-S_{i-1}}$ est un isomorphisme.*

(2b) *$\eta_{i-1}\,|_{S_{i-1}}$ est lisse et $(\eta_i/\Pi\eta_{i-1})\,|_{S_{i-1}}$ est lisse en $\mathcal{O}/\pi$-vectoriels de rang 1.*

7. Rigidification.

(7.1) Soient B une $\overline{k}$-algèbre et X un $\mathcal{O}_D$-module formel spécial de hauteur 4 sur B. On appelle *rigidification* de X la donnée d'une quasiisogénie de hauteur zéro $\rho : \Phi_B \to X$, où Φ_B est déduit par changement de base du $\mathcal{O}_D$-module formel Φ choisi sur $\overline{k}$ en (5.16).

Par définition, une *isogénie* $\alpha : \Phi_B \to X$ est un homomorphisme de $\mathcal{O}_D$-modules formels dont le noyau est représentable par un schéma en groupes fini localement libre sur B. On dit que α est de hauteur h si $\operatorname{Ker}\alpha$ est de degré q^h sur B.

Sur $\overline{k}$, la multiplication par π est une isogénie de hauteur 4 de Φ dans lui-même; par changement de base, il en est de même sur B de la multiplication par π de Φ_B dans lui-même. En particulier, Φ_B est π-divisible et le $\mathcal{O}$-module $\operatorname{Hom}_{\mathcal{O}_D}(\Phi_B, X)$ est sans torsion ([Zi 3], 5.31).

Par définition, une *quasiisogénie* $\rho : \Phi_B \to X$ est un élément de $\operatorname{Hom}_{\mathcal{O}_D}(\Phi_B, X) \otimes_{\mathcal{O}} K$ tel que $\pi^n\rho$ soit une isogénie pour n entier suffisamment grand. Noter, d'après ce qui précède, que $\pi^n\rho$ détermine ρ sans ambiguïté. On dit que ρ est de hauteur zéro si $\pi^n\rho$ est de hauteur $4n$.

On montre qu'un homomorphisme $\alpha : \Phi_B \to X$ est une isogénie si et seulement si il existe un entier m et un homomorphisme $\beta : X \to \Phi_B$ tel que $\beta \circ \alpha = \pi^m$ ([Zi 3], Satz 5.25). Par suite, un élément ρ de $\operatorname{Hom}_{\mathcal{O}_D}(\Phi_B, X) \otimes_{\mathcal{O}} K$ est une quasiisogénie si et seulement si il admet un inverse dans $\operatorname{Hom}_{\mathcal{O}_D}(X, \Phi_B) \otimes_{\mathcal{O}} K$.

Signalons également un résultat de T. Zink ([Zi 3], Satz 5.15 ou [Zi 1]) : Lorsque B est noethérien, un homomorphisme $\alpha : \Phi_B \to X$ est une isogénie de hauteur h si et seulement si pour tout idéal premier $\mathfrak{p}$ de B l'homomorphisme $\alpha_{\overline{k}(\mathfrak{p})} : \Phi_{\overline{k}(\mathfrak{p})} \to X_{\overline{k}(\mathfrak{p})}$ déduit de α par restriction à une clôture algébrique $\overline{k}(\mathfrak{p})$ du corps résiduel $k(\mathfrak{p}) = B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ est une isogénie de hauteur h.

Notons $S = \mathrm{Spec}(B)$ et, pour $j \in \{0,1\}$, S_j le fermé de S au-dessus duquel j est critique pour X.

Supposons tout d'abord qu'il existe un indice $i \in \{0,1\}$ tel que $S = S_i$ (schématiquement), autrement dit i est critique pour X, et considérons les faisceaux π-adiques η_j associés à X au paragraphe 6.

PROPOSITION (7.2). — *Supposons $S = S_i$ et X rigidifié. Alors :*

(1) *Le faisceau π-adique η_i est constant sur S.*

(2) *Les restrictions à $S - S_{i-1}$ et à S_{i-1} du faisceau π-adique constructible η_{i-1} sont constantes.*

(3) *A une rigidification ρ de X est associée un isomorphisme de faisceaux $r : \underline{K}^2 \xrightarrow{\sim} \eta_0 \otimes_{\mathcal{O}} K$ tel que $[\eta_j \,|_{S_j} : \Pi^j r\mathcal{O}^2] = j$ pour $j \in \{0,1\}$.*

Démonstration. — Rappelons que 0 est un indice critique pour Φ et qu'on a choisi une identification de $\eta_{\Phi,0}$ avec $\mathcal{O}^2$. D'après le lemme suivant, l'isogénie $\pi^n\rho : \Phi_B \to X$ induit un homomorphisme de faisceaux π-adiques $\pi^n r : \underline{\mathcal{O}}^2 \to \eta_0$, d'où un homomorphisme $r = \underline{K}^2 \to \eta_0 \otimes_{\mathcal{O}} K$.

LEMME (7.3). — *Soit $\alpha : X \to X'$ un homomorphisme de $\mathcal{O}_D$-modules formels spéciaux de hauteur 4 sur S. Supposons que $i \in \{0,1\}$ [resp. j] est critique pour X [resp. X'] sur S. Soit η [resp. η'] le faisceau π-adique $\mathbb{Z}/2\mathbb{Z}$-gradué associé à X [resp. X'] à l'aide de la filtration $V^r M_i$ [resp. $V^r M'_j$]. Alors α induit un homomorphisme naturel de faisceaux π-adiques de η_i dans η'_i.*

Démonstration. — Le problème est que la construction de φ, donc de η, n'est pas fonctorielle en X ; cependant ce lemme établit une fonctorialité partielle et en tout cas la fonctorialité de $\eta \otimes_{\mathcal{O}} K$.

Pour tout $n > 0$, on a d'après (4.3) des isomorphismes

$$N_{i,n} \simeq M_i/VM_{i-1} \oplus M_i/V^{2n}M_i$$
$$N'_{j,n} \simeq M'_j/VM'_{j-1} \oplus M'_j/V^{2n}M'_j$$

tels que l'endomorphisme φ des premiers membres corresponde à l'application

$$(\overline{m}, \overline{m}'') \mapsto (\overline{m}'', V^{-1}\Pi\overline{m}'')$$

sur les seconds membres.

Notons $\varepsilon = |j - i|$. L'application naturelle de M_i dans M'_j induite par $\Pi^\varepsilon \alpha$ commute à V et Π; elle définit donc une application de $N_{i,n}$ dans $N'_{j,n}$ qui commute à φ et par conséquent une application de $\eta_{i,n}$ dans $\eta'_{j,n}$. Lorsque n varie, ces applications sont compatibles entre elles et définissent un homomorphisme de η_i dans η'_j.

Lorsque $j \neq i$, montrons que cet homomorphisme se factorise à travers l'injection naturelle $\Pi : \eta'_i \to \eta'_j$. Cette assertion se vérifie sur les fibres, on peut donc supposer que S est le spectre d'un corps algébriquement clos. Il y a alors deux cas :

a) i n'est pas critique pour X'. Alors Π induit un isomorphisme de η'_i dans η'_j, il n'y a rien à vérifier.

b) i est critique pour X'. On a alors des isomorphismes

$$N'_{i,n} \simeq M'_i/VM'_{i-1} \oplus M'_i/V^{2n-1}M'_j$$

tels que l'endomorphisme φ des premiers membres corresponde à l'application définie comme précédemment sur les seconds membres. Par suite l'application de $N_{i,n}$ dans $N'_{j,n}$ induite par $\Pi\alpha$ se factorise en l'application induite par α de $N_{i,n}$ dans $N'_{i,n}$ [remarquez que $\alpha(V^{2n}M_i) \subset V^{2n}M'_i \subset V^{2n-1}M'_j$] suivie de l'application induite par Π de $N'_{i,n}$ dans $N'_{j,n}$. Ces applications commutent à φ et définissent donc des applications $\eta_{i,n} \to \eta'_{i,n}$ et $\eta'_{i,n} \to \eta'_{j,n}$ dont le composé est l'application $\eta_{i,n} \to \eta'_{j,n}$ induite par $\Pi\alpha$. En faisant varier n, on obtient la factorisation cherchée.

Reprenons la démonstration de la proposition (7.2). En tout point géométrique $\overline{s}$ de S, l'homomorphisme $r_{\overline{s}}$ induit sur les fibres en $\overline{s}$ est un isomorphisme, comme on l'a vu lors de l'étude de la situation sur un corps algébriquement clos (5.14); par suite $r : \underline{K}^2 \to \eta_0 \otimes_{\mathcal{O}} K$ est un isomorphisme. En particulier le faisceau $\eta_0 \otimes_{\mathcal{O}} K$ est constant; il en est de même de $\eta_1 \otimes_{\mathcal{O}} K$, puisque $\Pi : \eta_0 \to \eta_1$ induit un isomorphisme $\eta_0 \otimes_{\mathcal{O}} K \xrightarrow{\sim} \eta_1 \otimes_{\mathcal{O}} K$, ce qui se vérifie également sur les fibres.

Le faisceau π-adique η_i est lisse sur S et $\eta_i \otimes_{\mathcal{O}} K$ est constant, donc η_i est constant. En effet, on peut pour le vérifier supposer S connexe; alors η_i correspond à une représentation du groupe fondamental $\Pi_1(S, \overline{s})$ dans $\eta_{i,\overline{s}} \simeq \mathcal{O}^2$ et $\eta_i \otimes_{\mathcal{O}} K$ à la représentation dans K^2 qui s'en déduit; cette dernière étant triviale, la représentation dans $\mathcal{O}^2$ l'est également.

De même, puisque les restrictions à $S - S_{i-1}$ et à S_{i-1} du faisceau π-adique η_{i-1} sont lisses et que $\eta_{i-1} \otimes_{\mathcal{O}} K$ est constant, ces restrictions sont elles aussi constantes.

Enfin les propriétés de l'isomorphisme $r : \underline{K}^2 \to \eta_0 \otimes_{\mathcal{O}} K$ relativement aux faisceaux constants $\eta_j \,|_{S_j}$ se vérifient sur les fibres en un point géométrique, on les a établies en (5.15).

Remarque (7.4). On notera que la construction des faisceaux η_j et de l'isomorphisme r associés à (X, ρ) commutent à tout changement de base de B à une B-algèbre B'. On l'a vu en (6.6) pour ce qui concerne η_j et cela résulte de la démonstration du lemme pour r.

On a d'ailleurs utilisé implicitement cette propriété au cours de la démonstration lorsqu'on s'est ramené au cas où la base est un corps algébriquement clos pour calculer les fibres.

Considérons maintenant le cas général (sans supposer $S = S_i$) et regardons η comme un foncteur sur les B-algèbres (et non plus comme un faisceau π-adique).

PROPOSITION (7.5). — *Supposons X rigidifié. Alors pour $j \in \{0,1\}$:*

(1) *η_j est un faisceau constructible pour la topologie de Zariski sur S, en $\mathcal{O}$-modules libres de rang 2.*

(2) *La restriction de η_j à S_j est un faisceau constant.*

(3) *A une rigidification ρ de X est associée un isomorphisme de faisceaux $r : \underline{K}^2 \xrightarrow{\sim} \eta_0 \otimes_{\mathcal{O}} K$ tel que $[\eta_j \,|_{S_j} : \Pi^j r \mathcal{O}^2] = j$.*

De plus la formation de (η, r) à partir de (X, ρ) commute à tout changement de base de B à une B-algèbre B'.

Démonstration. — Lorsque l'un des indices $i \in \{0,1\}$ est critique sur S tout entier, ces assertions résultent des assertions analogues (7.2) pour les faisceaux π-adiques η_j, compte-tenu du fait que $\eta_j(B') = \varprojlim \eta_{j,n}(B')$ quelle que soit la B-algèbre B' (6.3). En particulier (7.5.2) résulte de (7.2.1).

La constructibilité de η dans le cas général s'en déduit par réduction au cas où B est réduit ce qui ne modifie pas η (3.14), puis au cas où B est intègre, donc l'un des indices critique sur S tout entier, par recollement des composantes irréductibles grâce au lemme suivant.

LEMME (7.6). — *Soient I_1 et I_2 deux idéaux de B tels que $I_1 \cap I_2 = 0$. Soient i_1, i_2 et i_{12} les immersions fermées dans S des sous-schémas définis respectivement par I_1, I_2 et $I_1 + I_2$. On a alors une suite exacte*

$$0 \to \eta \to i_{1*}i_1^*\eta \oplus i_{2*}i_2^*\eta \to i_{12*}i_{12}^*\eta$$

de préfaisceaux sur S.

Démonstration. — Pour toute B-algèbre B', soient $B'_1 = B'/I_1B'$, $B'_2 = B'/I_2B'$ et $B'_{12} = B'/(I_1 + I_2)B'$. De la suite exacte :

$$\begin{aligned} 0 \to B' \to B'_1 \times B'_2 &\to B'_{12} \to 0 \\ (a,b) &\mapsto a - b \end{aligned}$$

on déduit une suite exacte de modules de Cartier :

$$0 \to M_{B'} \to M_{B'_1} \times M_{B'_2} \to M_{B'_{12}} \to 0$$

et de modules de Cartier modifiés :

$$0 \to N(M_{B'}) \to N(M_{B'_1}) \times N(M_{B'_2}) \to N(M_{B'_{12}}) \to 0.$$

En prenant le noyau de $1 - \varphi$, on en déduit la suite exacte :

$$0 \to \eta(B') \to \eta(B'_1) \times \eta(B'_2) \to \eta(B'_{12})$$

d'où le lemme.

Enfin on notera que l'isomorphisme $r : \underline{K}^2 \to \eta_0 \otimes_{\mathcal{O}} K$ associé à la rigidification ρ grâce au lemme (7.3) lorsque 0 et 1 sont tous deux critiques sur S ne dépend pas du choix de l'indice critique $i \in \{0, 1\}$; par suite les isomorphismes $r|_{S_0}$ et $r|_{S_1}$ se recollent en un isomorphisme r défini sur S tout entier.

8. Le théorème de Drinfeld.

Rappelons que l'on a choisi une clôture algébrique $\overline{k}$ de k, un $\mathcal{O}_D$-module formel spécial Φ de hauteur 4 sur $\overline{k}$ tel que 0 soit critique pour Φ et un isomorphisme $\mathcal{O}^2 \simeq \eta_{\Phi,0}$. On note $\mathcal{O}^{nr}$ l'hensélisé strict (= extension non ramifiée maximale) de $\mathcal{O}$ de corps résiduel $\overline{k}$.

DÉFINITION (8.1). Soit $\overline{Nilp}$ la catégorie des $\mathcal{O}^{nr}$-algèbres où l'image de π est nilpotente. On définit un foncteur $\overline{G}$ sur $\overline{Nilp}$ en associant à $B \in \mathrm{Ob}\,\overline{Nilp}$ l'ensemble $\overline{G}(B)$ des classes d'isomorphie de couples (X, ρ) consistant en :

1) un $\mathcal{O}_D$-module formel spécial X de hauteur 4 sur B.

2) une quasi-isogénie de hauteur zéro $\rho : \Phi_{B/\pi B} \to X_{B/\pi B}$.

Toutefois dans cette définition, il convient de prendre $\mathcal{O}_D$-module formel dans un sens un peu plus général que précédemment : on demande seulement que $\mathrm{Lie}(X)$ soit un B-module projectif. Localement pour la topologie de Zariski sur B, on retrouve les $\mathcal{O}_D$-modules formels définis au paragraphe 2.

Le résultat fondamental de Drinfeld est le :

THÉORÈME (8.2). — *Le foncteur $\overline{G}$ est représentable par le $\widehat{\mathcal{O}}^{nr}$-schéma formel $\widehat{\Omega} \widehat{\otimes}_{\mathcal{O}} \widehat{\mathcal{O}}^{nr}$.*

DÉFINITION (8.3). Soit $Nilp$ la catégorie des $\mathcal{O}$-algèbres où l'image de π est nilpotente. On définit un foncteur G sur $Nilp$ en associant à $B \in \mathrm{Ob}\, Nilp$ l'ensemble $G(B)$ des couples formés

1) d'un k-homomorphisme $\psi : \overline{k} \to B/\pi B$

2) d'une classe d'isomorphie de couples (X, ρ) consistant en :

(2.1) un $\mathcal{O}_D$-module formel spécial X de hauteur 4 sur B.

(2.2) une quasi-isogénie de hauteur zéro $\rho : \psi_* \Phi \to X_{B/\pi B}$.

Si $B \to B'$ est un morphisme de $Nilp$, on définit de manière évidente une application $G(B) \to G(B')$ en associant à ψ son composé avec $B/\pi B \to B'/\pi B'$ et au couple (X, ρ) le couple $(X_{B'}, \rho_{B'/\pi B'})$ qui s'en déduit par extension des scalaires de B à B'.

Le foncteur G n'est autre que le foncteur déduit de $\overline{G}$ par restriction des scalaires de $\mathcal{O}^{nr}$ à $\mathcal{O}$. En effet, il revient au même de se donner un k-homomorphisme $\psi : \overline{k} \to B/\pi B$ ou un $\mathcal{O}$-homomorphisme $\widetilde{\psi} : \mathcal{O}^{nr} \to B$ faisant de B une $\mathcal{O}^{nr}$- algèbre $B_\psi \in \mathrm{Ob}\, \overline{Nilp}$, et un élément de $G(B)$ correspond à un couple formé de $\widetilde{\psi}$ et d'un élément de $\overline{G}(B_\psi)$.

Du théorème (8.2), on déduit par restriction des scalaires la variante :

THÉORÈME (8.4). — *Le foncteur G est représentable par le $\mathcal{O}$-schéma formel $\widehat{\Omega} \widehat{\otimes}_{\mathcal{O}} \widehat{\mathcal{O}}^{nr}$.*

Notons $\overline{H}$ la restriction à la catégorie $\overline{Nilp}$ du foncteur F sur $Nilp$ défini en (I.5.1). On a montré en (I.5.2) que F est représentable par le $\mathcal{O}$-schéma formel $\widehat{\Omega}$; par suite $\overline{H}$ est représentable par le $\widehat{\mathcal{O}}^{nr}$-schéma formel $\widehat{\Omega} \widehat{\otimes}_{\mathcal{O}} \widehat{\mathcal{O}}^{nr}$.

Pour $B \in \mathrm{Ob}\, \overline{Nilp}$, on définit une application $\overline{\xi}_B : \overline{G}(B) \to \overline{H}(B)$ en associant au couple (X, ρ) le quadruplet $(\eta_X, T_X, u_X, r_{(X,\rho)})$ où, si M est le module de Cartier de X sur B, on a :

1) $\eta_X = \eta_M$ vu comme faisceau sur $\mathrm{Spec}(B)$: si B' est une B-algèbre et si $M' = M_{B'}$, on a $\eta_X(B') = \eta_{M'}$;

2) $T_X = \mathrm{Lie}(X) = M/VM$;

3) $u_X : \eta_X \to T_X$ est l'homomorphisme de faisceaux tel que $u_X(B') = u_{M'} : \eta_{M'} \hookrightarrow N(M') \to M'/VM' = (M/VM) \otimes_B B'$ (*cf.* (3.13)) ;

4) $r_{(X,\rho)} : \underline{K}^2 \xrightarrow{\sim} \eta_{X,0}$ est l'isomorphisme associé à la rigidification ρ de X.

Les propositions (7.5), (5.5) et (5.6) montrent que le quadruplet $(\eta_X, T_X, u_X, r_{(X,\rho)})$ vérifie les conditions de la définition (I.5.1) et définit donc bien un élément de $\overline{H}(B) = F(B)$.

De plus, si $B \to B'$ est un morphisme de $\overline{Nilp}$, le diagramme :

$$\begin{array}{ccc} \overline{G}(B) & \xrightarrow{\overline{\xi}_B} & \overline{H}(B) \\ \downarrow & & \downarrow \\ \overline{G}(B') & \xrightarrow[\overline{\xi}_{B'}]{} & \overline{H}(B') \end{array}$$

est commutatif. Cela résulte du fait que la construction de η_X et $r_{(X,\rho)}$ à partir de (X, ρ) commute au changement de base (*cf.* (6.6) et (7.4)). Ainsi les $\overline{\xi}_B$ définissent une transformation naturelle $\overline{\xi} : \overline{G} \to \overline{H}$.

Le théorème (8.2) est conséquence de l'énoncé plus précis :

THÉORÈME (8.5). — *La transformation naturelle $\overline{\xi} : \overline{G} \to \overline{H}$ est un isomorphisme de foncteurs.*

Nous poursuivrons la démonstration de ce théorème dans les paragraphes 10 à 12.

Notons H le foncteur sur $Nilp$ déduit de $\overline{H}$ par restriction des scalaires de $\mathcal{O}^{nr}$ à $\mathcal{O}$. Pour $B \in \mathrm{Ob}\, Nilp$, un élément de $H(B)$ consiste en la donnée d'un k-homomorphisme $\psi : \overline{k} \to B/\pi B$ et d'un élément de $\overline{H}(B_\psi) = F(B)$. Il est clair que H est représentable par le $\mathcal{O}$-schéma formel $\widehat{\Omega} \widehat{\otimes}_{\mathcal{O}} \widehat{\mathcal{O}}^{nr}$.

On définit par restriction des scalaires une transformation naturelle $\xi : G \to H$ en associant au couple (ψ, a), où $a \in \overline{G}(B_\psi)$, le couple $(\psi, \overline{\xi}_{B_\psi}(a))$. Le théorème (8.5) implique alors :

THÉORÈME (8.6). — *La transformation naturelle $\xi : G \to H$ est un isomorphisme de foncteurs.*

On prendra soin de noter que l'application $\overline{\xi}_{B_\psi} : \overline{G}(B_\psi) \to \overline{H}(B_\psi) = F(B)$ dépend de la structure de $\mathcal{O}^{nr}$-algèbre de B_ψ, en particulier la $\mathbb{Z}/2\mathbb{Z}$-graduation de η_X et T_X associés à X dépend de sa structure de $\mathcal{O}'$-algèbre.

9. Action des groupes $GL(2, K)$ et D^*.

(9.1) *Le morphisme de Frobenius.*

On note $Fr : \overline{k} \to \overline{k}$ l'homomorphisme de Frobenius $Fr(x) = x^q$ et Frob : $Fr_*^{-1}\Phi \to \Phi$ le morphisme de Frobenius. C'est un $\overline{k}$-homomorphisme de $\mathcal{O}_D$-modules formels du $\mathcal{O}_D$-module formel $Fr_*^{-1}\Phi$ déduit de Φ par extension des scalaires via Fr^{-1} (souvent noté $\Phi^{(q^{-1})}$)

dans Φ. Plus précisément, c'est une isogénie de hauteur 2 (égale à la dimension de Φ).

Si M_Φ est le $\mathcal{O}[\Pi]$-module de Cartier gradué de Φ sur $\overline{k}$, celui de $Fr_*^{-1}\Phi$ s'identifie à $M_\Phi^\sigma[1]$, déduit de M_Φ par restriction des scalaires via $\sigma : \mathcal{W}_\mathcal{O}(\overline{k}) \to \mathcal{W}_\mathcal{O}(\overline{k})$ et décalage de la graduation (car l'action de $\mathcal{O}'$ via $\mathcal{O}_D$ est inchangée). Le morphisme de Frobenius correspond à l'homomorphisme $\mathcal{W}_\mathcal{O}(\overline{k})$- linéaire de degré zéro $V : M_\Phi^\sigma[1] \to M_\Phi$.

Puisque 0 est critique pour Φ, 1 est critique pour $Fr_*^{-1}\Phi$ et l'identification $M_{Fr_*^{-1}\Phi} = M_\Phi^\sigma[1]$ induit une identification :

$$\eta_{Fr_*^{-1}\Phi,1} = M_{Fr_*^{-1}\Phi,1}^{V^{-1}\Pi} = M_{\Phi,0}^{V^{-1}\Pi} = \eta_{\Phi,0}$$

d'où une identification $\eta_{Fr_*^{-1}\Phi} \otimes_\mathcal{O} K = (\eta_\Phi \otimes_\mathcal{O} K)[1]$. Le morphisme de Frobenius correspond donc à l'isomorphisme K-linéaire de degré zéro $\Pi : (\eta_\Phi \otimes_\mathcal{O} K)[1] \to \eta_\Phi \otimes_\mathcal{O} K$.

(9.2) *Action de $GL(2,K)$ sur le foncteur G.*

Soit v la valuation de K normalisée par $v(\pi) = 1$. Via l'identification (5.14) : $GL(2,K) = GL(\eta_{\Phi,0} \otimes_\mathcal{O} K) = (\mathrm{End}^0_{\mathcal{O}_D}\Phi)^*$, un élément g de $GL(2,K)$ définit une quasiisogénie de Φ de hauteur $2n$ si $v(\det g) = n$. Ainsi $g^{-1} \circ \mathrm{Frob}^n : Fr_*^{-n}\Phi \to \Phi$ est une quasiisogénie de hauteur zéro. On définit une action de $GL(2,K)$ sur le foncteur G en posant, pour $B \in \mathrm{Ob}\, Nilp$ et $(\psi; X, \rho)$ représentant un élément de $G(B)$:

$$g \cdot (\psi; X, \rho) = (\psi \circ Fr^{-n}; X, \rho \circ \psi_*(g^{-1} \circ \mathrm{Frob}^n)).$$

On note $\widetilde{Fr} : \mathcal{O}^{nr} \to \mathcal{O}^{nr}$ le relèvement du k-homomorphisme $Fr : \overline{k} \to \overline{k}$ en un $\mathcal{O}$-homomorphisme.

THÉORÈME (9.3). — *L'action de $GL(2,K)$ sur le foncteur G correspond à l'action sur le schéma formel $\widehat{\Omega}\widehat{\otimes}_\mathcal{O}\widehat{\mathcal{O}}^{nr}$ définie par l'action naturelle de $PGL(2,K)$ sur $\widehat{\Omega}$ et l'action $g \mapsto \widetilde{Fr}^{-v(\det g)}$ sur $\mathcal{O}^{nr}$.*

Démonstration. — D'après (I.6.2), cette dernière action est décrite sur les éléments de $H(B)$ par :

$$g \cdot (\psi; \eta, T, u, r) = (\psi \circ Fr^{-n}; \eta[n], T[n], u[n], \Pi^n r g^{-1}).$$

Il s'agit donc de vérifier, si $\overline{\xi}_{B_\psi}(X, \rho) = (\eta, T, u, r)$, qu'on a :

$$\overline{\xi}_{B_{\psi \circ Fr^{-n}}}(X, \rho \circ \psi_*(g^{-1} \circ \mathrm{Frob}^n)) = (\eta[n], T[n], u[n], \Pi^n r g^{-1}).$$

Le décalage de la graduation de (η, T, u) associé à X selon qu'on utilise la structure de $\overline{k}$-algèbre B_ψ ou $B_{\psi \circ Fr^{-n}}$ provient du changement par σ^n

de l'action de $\mathcal{O}'$ sur M_X via $W_{\mathcal{O}}(\overline{k})$ alors que l'action de $\mathcal{O}'$ via $\mathcal{O}_D$ est inchangée.

Pour calculer la rigidification, convenons de noter

$$g^{-1} : \eta_\Phi \otimes_{\mathcal{O}} K \xrightarrow{\sim} \eta_\Phi \otimes_{\mathcal{O}} K \text{ et } r : \psi_*(\eta_\Phi \otimes_{\mathcal{O}} K) \xrightarrow{\sim} \eta \otimes_{\mathcal{O}} K$$

les isomorphismes définis, compte-tenu de l'identification $K^2 = \eta_{\Phi,0} \otimes_{\mathcal{O}} K$, par g^{-1} et r sur les composantes de degré zéro et étendus par conjugaison par Π aux composantes de degré 1, de telle sorte qu'on ait $g^{-1} \circ \Pi = \Pi \circ g^{-1}[1]$ et $r \circ \Pi = \Pi \circ r[1]$.

Puisque la quasi-isogénie

$$g^{-1} \circ \mathrm{Frob}^n : Fr_*^{-n}\Phi \to \Phi$$

correspond via $\overline{\xi}_{\overline{k}}$ à :

$$(\eta_\Phi \otimes_{\mathcal{O}} K)[n] \xrightarrow{\Pi^n} \eta_\Phi \otimes_{\mathcal{O}} K \xrightarrow{g^{-1}} \eta_\Phi \otimes_{\mathcal{O}} K,$$

la quasi-isogénie

$$\rho \circ \psi_*(g^{-1} \circ \mathrm{Frob}^n) : \psi_* \circ Fr_*^{-n}\Phi \to X$$

correspond via $\overline{\xi}_{B_\psi}$ à :

$$\psi_*(\eta_\Phi \otimes_{\mathcal{O}} K)[n] \xrightarrow{\Pi^n} \psi_*(\eta_\Phi \otimes_{\mathcal{O}} K) \xrightarrow{g^{-1}} \psi_*(\eta_\Phi \otimes_{\mathcal{O}} K) \xrightarrow{r} \eta \otimes_{\mathcal{O}} K,$$

ou encore, en faisant commuter Π^n à g^{-1} et r et en décalant la graduation de n, via $\overline{\xi}_{B_{\psi \circ Fr^{-n}}}$ à :

$$\psi_*(\eta_\Phi \otimes_{\mathcal{O}} K) \xrightarrow{g^{-1}} \psi_*(\eta_\Phi \otimes_{\mathcal{O}} K) \xrightarrow{r} \eta \otimes_{\mathcal{O}} K \xrightarrow{\Pi^n} (\eta \otimes_{\mathcal{O}} K)[n].$$

Le résultat cherché s'obtient en prenant la composante de degré zéro et en composant avec l'identification fixée $K^2 = \eta_{\Phi,0} \otimes_{\mathcal{O}} K$.

(9.4) *Action de D^* sur le foncteur G.*

Soit $N_{D/K} : D^* \to K^*$ la norme réduite : tout élément de D^* s'écrit $g = \Pi^n \cdot g_0$ avec $g_0 \in \mathcal{O}_D^*$ et $n = v(N_{D/K}g)$.

Pour $g \in D^*$, notons ${}^gX$ le $\mathcal{O}_D$-module formel qui coïncide avec X en tant que $\mathcal{O}$-module, mais où l'action de $a \in \mathcal{O}_D$ sur ${}^gX$ est identique à l'action de $g^{-1}ag$ sur X.

L'action de $\mathcal{O}_D$ sur Φ associe à g^{-1} une quasi-isogénie $\mathcal{O}_D$-équivariante $g^{-1} : \Phi \to {}^g\Phi$ de hauteur $-2n$ si $v(N_{D/K}g) = n$. Ainsi $g^{-1} \circ \mathrm{Frob}^n : Fr_*^{-n}\Phi \to {}^g\Phi$ est une quasi-isogénie $\mathcal{O}_D$-équivariante de hauteur zéro. On définit une action de D^* sur le foncteur G en posant, pour $B \in \mathrm{Ob}Nilp$ et $(\psi; X, \rho)$ représentant un élément de $G(B)$:

$$g \cdot (\psi; X, \rho) = (\psi \circ Fr^{-n}; {}^gX, \rho \circ \psi_*(g^{-1} \circ \mathrm{Frob}^n)).$$

THÉORÈME (9.5). — *L'action de D^* sur le foncteur G correspond à l'action sur le schéma formel $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$ définie par l'action $g \mapsto \widetilde{Fr}^{-v(N_{D/K}g)}$ sur $\mathcal{O}^{nr}$.*

Démonstration. — Notons tout d'abord que $\mathcal{O}_D^*$ agit trivialement car, si $g \in \mathcal{O}_D^*$, l'application $g^{-1} : X \to {}^gX$ est un isomorphisme de (X, ρ) sur $({}^gX, \rho \circ \psi_*(g^{-1}))$.

Reste à vérifier que l'action de Π sur G correspond à celle de $\widetilde{Fr}^{-1}$ sur $\mathcal{O}^{nr}$; autrement dit que, si $\overline{\xi}_{B_\psi}(X, \rho) = (\eta, T, u, r)$, on a :

$$\overline{\xi}_{B_{\psi \circ Fr^{-1}}}({}^{\Pi}X, \rho \circ \psi_*(\Pi^{-1} \circ \mathrm{Frob})) = (\eta, T, u, r).$$

Soient M_X et $M_{{}^{\Pi}X}$ les $\mathcal{O}[\Pi]$-modules de Cartier gradués sur B_ψ associés à X et ${}^{\Pi}X$. Alors $M_{{}^{\Pi}X}$ coïncide avec M_X en tant que $W_{\mathcal{O}}(\overline{k})[V, \Pi]$-module, mais l'action de $a \in \mathcal{O}'$ via $\mathcal{O}_D$ sur $M_{{}^{\Pi}X}$ doit être identique à celle de $\Pi^{-1}a\Pi = \sigma(a)$ sur M_X, donc $M_{{}^{\Pi}X} = M_X[1]$. Par suite le triplet sur B associé à ${}^{\Pi}X$ est $(\eta, T, u)[1]$ si B est munie de la structure de $\overline{k}$-algèbre B_ψ, et (η, T, u) si B est munie de la structure de $\overline{k}$-algèbre $B_{\psi \circ Fr^{-1}}$.

La quasi-isogénie

$$\Pi^{-1} \circ \mathrm{Frob} : Fr_*^{-1}\Phi \to {}^{\Pi}\Phi$$

correspond via $\overline{\xi}_{\overline{k}}$ à :

$$(\eta_\Phi \otimes_{\mathcal{O}} K)[1] \xrightarrow{\Pi} \eta_\Phi \otimes_{\mathcal{O}} K \xrightarrow{\Pi^{-1}} \eta_\Phi \otimes_{\mathcal{O}} K[1],$$

c'est-à-dire à $\mathrm{id}_{\eta_\Phi \otimes_{\mathcal{O}} K[1]}$. Par suite la quasi-isogénie

$$\rho \circ \psi_*(\Pi^{-1} \circ \mathrm{Frob}) : \psi_* Fr_*^{-1}\Phi \to {}^{\Pi}X$$

correspond via $\overline{\xi}_{B_\psi}$ à

$$r[1] : \psi_*(\eta_\Phi \otimes_{\mathcal{O}} K)[1] \to \eta[1]$$

et via $\overline{\xi}_{B_{\psi \circ Fr^{-1}}}$ à r.

10. Théorie de déformation.

On travaille dans la catégorie $\overline{Nilp}$ des $\mathcal{O}^{nr}$-algèbres où l'image de π est nilpotente. On appelle extension infinitésimale un homomorphisme surjectif $B' \to B$ dont le noyau est nilpotent.

PROPOSITION (10.1). — *Soit $B' \to B$ une extension infinitésimale. Soient $B'_0 = B'/\pi B'$ et $B_0 = B/\pi B$. Soient X' un $\mathcal{O}_D$-module formel spécial de hauteur 4 sur B' et $X = X'_B$. Supposons X muni d'une rigidification ρ, c'est-à-dire d'une quasi-isogénie de hauteur zéro $\rho : \Phi_{B_0} \to X_{B_0}$. Alors :*

(i) X' est π-divisible (i.e. $\pi : X' \to X'$ est une isogénie).

(ii) ρ se relève de manière unique en une rigidification de X', c'est-à-dire en une quasi-isogénie de hauteur zéro $\rho' : \Phi_{B'_0} \to X_{B'_0}$.

Démonstration. — (i) Soit n tel que $\alpha = \pi^n \rho$ soit une isogénie. Puisque Φ_{B_0} est π-divisible, $\alpha \circ \pi$ est une isogénie. Mais $\alpha \circ \pi = \pi \circ \alpha$, donc $\pi : X_{B_0} \to X_{B_0}$ est aussi une isogénie ([Zi 3], 5.10). Par déformation, il en est de même de $\pi : X' \to X'$ ([Zi 3], 5.12).

(ii) Par récurrence, on peut supposer que $I = \mathrm{Ker}(B' \to B)$ est de carré nul. L'isogénie $\alpha = \pi^n \rho : \Phi_{B_0} \to X_{B_0}$ ne se relève peut-être pas, mais $\beta = \pi\alpha = \pi^{n+1}\rho$ se relève toujours ([Zi 3], 4.47) en une isogénie $\beta' : \Phi_{B'_0} \to X'_{B'_0}$; donc ρ se relève en $\rho' = \beta/\pi^{n+1}$. De plus ce relèvement est unique d'après la rigidité des groupes p-divisibles ([Zi 3], 5.30).

Ainsi on peut oublier les rigidifications pour étudier la théorie de déformation. De plus il n'y a pas d'automorphismes infinitésimaux, par rigidité.

PROPOSITION (10.2). — *Soient $B' \to B$ et $B'' \to B$ deux extensions infinitésimales. Alors l'application canonique*

$$\overline{G}(B' \times_B B'') \to \overline{G}(B') \times_{\overline{G}(B)} \overline{G}(B'')$$

est bijective.

Démonstration. — On reprend mutatis mutandis la démonstration usuelle dans le cas des groupes p-divisibles ([Zi 3], 5.40). Soient X' et X'' des déformations sur B' et B'' respectivement de X donné sur B. Alors il existe une et une seule déformation $\widetilde{X}$ de X' et X'' simultanément sur $B' \times_B B''$; son $\mathcal{O}[\Pi]$-module de Cartier gradué est $M_{\widetilde{X}} = M_{X'} \times_{M_X} M_{X''}$.

Pour $x \in \overline{G}(B)$ et $C \to B$ une extension infinitésimale, notons $\overline{G}_x(C)$ l'image réciproque de x dans $\overline{G}(C)$ et $\overline{H}_x(C)$ l'image réciproque de $\overline{\xi}(x)$ dans $\overline{H}(C)$.

COROLLAIRE (10.3). — *Soit $B' \to B$ une extension infinitésimale dont le noyau I est de carré nul et soit $B[I]$ la B-algèbre $B \oplus I$ avec $I^2 = 0$. Alors :*

(i) $\overline{G}_x(B[I])$ est un groupe abélien,

(ii) si $\overline{G}_x(B')$ est non vide, c'est un $\overline{G}_x(B[I])$-ensemble homogène principal.

Ces structures sont canoniques.

Démonstration. — C'est une conséquence classique de la commutation de $\overline{G}$ au produit fibré, énoncé la plupart du temps pour des anneaux locaux artiniens, mais valable dans ce contexte (*cf.* Schlessinger [Sc], Artin [A]). La structure de groupe est définie par l'homomorphisme

$$\begin{aligned} B[I] \times_B B[I] &\longrightarrow B[I] \\ (b+i) \times_b (b+j) &\longmapsto b+i+j \end{aligned}$$

dont on déduit, compte-tenu de (10.2), une application :

$$\overline{G}_x(B[I]) \times \overline{G}_x(B[I]) \to \overline{G}_x(B[I]).$$

De même, on déduit de l'isomorphisme

$$\begin{aligned} B' \times_B B' &\xrightarrow{\sim} B' \times_B B[I] \\ a \times_b c &\longmapsto a \times_b b + (c-a) \end{aligned}$$

une bijection

$$\overline{G}_x(B') \times \overline{G}_x(B') \xrightarrow{\sim} \overline{G}_x(B') \times \overline{G}_x(B[I])$$

induisant l'identité sur le premier facteur; d'où la structure d'espace homogène principal lorsque $\overline{G}_x(B') \neq \emptyset$.

Le foncteur $\overline{H}$, étant représentable, commute également au produit fibré d'extensions infinitésimales; d'où, sous les hypothèses de (10.3), une structure de groupe sur $\overline{H}_x(B[I])$ et d'espace homogène principal sous ce groupe sur $\overline{H}_x(B')$ lorsque $\overline{H}_x(B')$ est non vide. La façon dont ces structures sont définies implique que les applications $\overline{\xi}_{B[I]} : \overline{G}_x(B[I]) \to \overline{H}_x(B[I])$ et $\overline{\xi}_{B'} : \overline{G}_x(B') \to \overline{H}_x(B')$ leur sont compatibles.

PROPOSITION (10.4). — *Si $\overline{H}_x(B') \neq \emptyset$, alors $\overline{G}_x(B') \neq \emptyset$.*

Démonstration. — Soient (X, ρ) représentant $x \in \overline{G}(B)$ et M le $\mathcal{O}[\Pi]$-module de Cartier gradué de X sur B. On se ramène aisément par

localisation au cas où M/VM est un B-module libre. Soient alors (γ_0, γ_1) une V-base homogène de M et

$$\Pi\gamma_i = [a_{0,i}]\gamma_{\overline{i+1}} + \sum_{m>0} V^m[a_{m,i}]\gamma_{\overline{m+i+1}} \qquad (i = 0, 1)$$

les équations de définition de M. Pour relever X en X' sur B', il suffit de relever les $a_{m,i} \in B$ en des $a'_{m,i} \in B'$ vérifiant toutefois $a'_{0,0} \cdot a'_{0,1} = \pi$ (2.3).

Le foncteur $\overline{\xi}$ associe à (X, ρ) entre autre la classe d'isomorphisme de $T = M/VM$ muni de Π. L'image $(\overline{\gamma_0}, \overline{\gamma_1})$ de (γ_0, γ_1) est une base homogène de T telle que $\Pi\overline{\gamma}_0 = a_{0,0}\overline{\gamma}_1$ et $\Pi\overline{\gamma}_1 = a_{0,1}\overline{\gamma}_0$. Si $\overline{H}_x(B')$ est non vide, il existe (T', Π) sur B' relevant (T, Π) ; donc il existe $a'_{0,0}$ et $a'_{0,1} \in B'$ relevant $a_{0,0}$ et $a_{0,1}$ tels que $a'_{0,0} \cdot a'_{0,1} = \pi$.

Nous sommes maintenant en mesure d'établir le résultat essentiel de ce paragraphe :

PROPOSITION (10.5). — *Pour que $\overline{\xi} : \overline{G} \to \overline{H}$ soit un isomorphisme, il suffit qu'il en soit ainsi en restriction à la catégorie des $\overline{k}$-algèbres.*

Démonstration. — Soit $\overline{Nilp}_n$ la sous-catégorie pleine de $\overline{Nilp}$ formée des $\mathcal{O}^{nr}$-algèbres telles que l'image de π^n soit nulle, en particulier $\overline{Nilp}_1$ est la catégorie des $\overline{k}$-algèbres. Supposons par récurrence que $\overline{\xi}\Big|_{\overline{Nilp}_n}$ est un isomorphisme. Soient $B' \in \mathrm{Ob}\,\overline{Nilp}_{n+1}$ et $B = B'/\pi^n B'$, $I = \pi^n B'$. Alors B et $B[I] \in \mathrm{Ob}\,\overline{Nilp}_n$, donc $\overline{\xi}_B$ et $\overline{\xi}_{B[I]}$ sont bijectifs. Il résulte de ce qui précède qu'alors $\overline{\xi}_{B'}$ est bijectif.

11. Espaces tangents.

Notons $\overline{k}[\varepsilon]$ avec $\varepsilon^2 = 0$ les nombres duaux. Pour $x \in \overline{G}(\overline{k})$, l'espace tangent à $\overline{G}$ en x est $t_{\overline{G}}(x) = \{x' \in \overline{G}(\overline{k}[\varepsilon])$ d'image x dans $\overline{G}(\overline{k})\}$. Il résulte de la proposition (10.2) que $t_{\overline{G}}(x)$ est canoniquement un $\overline{k}$-vectoriel et que l'application tangente $t_{\overline{\xi}}(x) : t_{\overline{G}}(x) \to t_{\overline{H}}(\overline{\xi}(x))$ induite par $\overline{\xi}$ est $\overline{k}$-linéaire. On se propose de montrer dans ce paragraphe :

PROPOSITION (11.1). — *Quel que soit $x \in \overline{G}(\overline{k})$, l'application tangente $t_{\overline{\xi}}(x) : t_{\overline{G}}(x) \to t_{\overline{H}}(\overline{\xi}(x))$ est bijective.*

Pour démontrer la proposition, il faudra non seulement calculer l'espace tangent $t_{\overline{G}}(x)$, mais également identifier l'application tangente $t_{\overline{\xi}}(x)$ pour en vérifier l'injectivité.

Soit (X, ρ) un représentant de x et soit M le $\mathcal{O}[\Pi]$-module de Cartier gradué de X sur $\overline{k}$. D'après (10.1), déformer (X, ρ) revient à déformer X, autrement dit à déformer M. Ainsi

$t_{\overline{G}}(x) = \{$déformations de M en un $\mathcal{O}[\Pi]$-module de Cartier gradué M' sur $\overline{k}[\varepsilon]\}$.

(11.2) Rappelons tout d'abord comment calculer les déformations des modules de Cartier des groupes p-divisibles (*cf.* [No], [Zi 3] 5.41). Si M' est une déformation de M au-dessus de $\overline{k}[\varepsilon]$, on a une suite exacte :

$$0 \to M_\varepsilon \to M' \to M \to 0,$$

où $M_\varepsilon = \bigoplus_{i=0}^{\infty} V^i[\varepsilon](M/VM)$ car $[\varepsilon]V = V[\varepsilon^q] = 0$.

Cette suite exacte se scinde en relevant M en :

$$\widetilde{M} = \{m \in M' | \text{ il existe } \ell \text{ avec } V^\ell m \in FM' \oplus \bigoplus_{i=0}^{\ell-1} V^i[\varepsilon](M/VM)\}.$$

Ce relèvement de M en $\widetilde{M}$ prolonge le relèvement évident de FM en FM' venant de $FM' \cap M_\varepsilon = \{0\}$; on l'obtient en remarquant que l'action de V sur M/FM est nilpotente.

Le scindage ainsi défini est $W_{\mathcal{O}}(\overline{k})[F]$-équivariant ; par contre, notant V' l'action de V sur M', on a $V'\widetilde{M} \subset \widetilde{M} \oplus [\varepsilon](M/VM)$. La structure de M' est déterminée par l'application $\overline{k}$-linéaire $\beta : VM/\pi M \to M/VM$ telle que $V'm = Vm + [\varepsilon]\beta(Vm)$ pour $m \in \widetilde{M}$. Réciproquement une telle application définit une unique déformation M' de M.

LEMME (11.3). — *L'espace tangent $t_{\overline{G}}(x)$ s'identifie canoniquement à l'espace des applications $\overline{k}$-linéaires de degré zéro $\beta : VM/\pi M \to M/VM$ telles que $\beta\Pi = \Pi\beta$.*

A une telle application correspond le module $M' = M \oplus M_\varepsilon$ où $V'(m,0) = (Vm, [\varepsilon]\beta(Vm))$.

Démonstration. — Dans ce cas M et M' sont munis de plus d'une action de $\mathcal{O}_D$, donnée équivalente à la graduation et à l'action de Π, et la suite exacte est compatible à cette action. Comme l'action de $\mathcal{O}_D$ commute à $W_{\mathcal{O}}(\overline{k}[\varepsilon])[F,V]$, on a $\mathcal{O}_D \cdot \widetilde{M} \subset \widetilde{M}$; en d'autres termes le scindage est compatible à la graduation et à l'action de Π. Par ailleurs celles-ci sont déterminées sur M_ε par leur valeur sur M/VM. Ainsi le scindage $M' = \widetilde{M} \oplus M_\varepsilon$ détermine graduation et action de Π sur M' en fonction de celles sur M. De plus M' est un $\mathcal{O}[\Pi]$-module de Cartier gradué sur $\overline{k}[\varepsilon]$ si et seulement si V' est de degré 1 et commute à Π, autrement dit si β est de degré 0 et commute à Π.

LEMME (11.4). — (*i*) *Si M possède un seul indice critique l'espace tangent $t_{\overline{G}}(x)$ est de dimension 1. Plus précisément, si i est critique et*

$i+1$ non critique, on a nécessairement $\beta_{i+1}=0$ et $t_{\overline{G}}(x)$ s'identifie à l'espace des applications $\overline{k}$-linéaire $\beta_i : VM_{i+1}/\pi M_i \to M_i/VM_{i+1}$.

(ii) Si M possède deux indices critiques, l'espace tangent $t_{\overline{G}}(x)$ est de dimension 2. Plus précisément, $t_{\overline{G}}(x)$ s'identifie à l'espace des couples d'applications $\overline{k}$-linéaires $\beta_i : VM_{i+1}/\pi M_i \to M_i/VM_{i+1} (i=0,1)$.

Démonstration. — (*cf.* [Zi 2], 3.10). Les conditions suivantes sont équivalentes :

a) l'indice i est critique pour M,

b) l'application $\Pi : M_i/VM_{i+1} \to M_{i+1}/VM_i$ est nulle,

c) l'application $\Pi : VM_i/\pi M_{i+1} \to VM_{i+1}/\pi M_i$ est nulle.

En effet il y a inclusion entre sous-modules de même indice dans M_i ou M_{i+1} si et seulement si il y a égalité; l'assertion résulte donc de l'équivalence entre les conditions $\Pi M_i = VM_i$ et $\pi M_i = \Pi V M_i$.

Ainsi dans le premier cas, les relations $\Pi\beta_j = \beta_{j+1}\Pi$ sont satisfaites si et seulement si $\beta_{i+1}=0$; alors que dans le second cas elles sont satisfaites quels que soient β_0 et β_1.

LEMME (11.5). — *Supposons i critique pour M. Alors i est critique pour M' si et seulement si $\beta_{i+1}=0$.*

Démonstration. — Supposons $\beta_{i+1}=0$ et montrons qu'alors i est critique pour M', autrement dit $\Pi M_i' \subset V'M_i'$. Vérifions le séparément pour chacun des facteurs de $M_i' = \widetilde{M}_i \oplus M_{\varepsilon,i}$.

On a $\Pi M_{\varepsilon,i} \subset V'M_{\varepsilon,i}$. En effet $M_{\varepsilon,i} = [\varepsilon](M_i/VM_{i+1}) \oplus V'M_{\varepsilon,i+1}$ et Π est nul sur M_i/VM_{i+1}.

D'autre part $\Pi\widetilde{M}_i \subset V'\widetilde{M}_i$. En effet pour $m \in M_i$, on a $\Pi(m,0) = (\Pi m, 0)$; or il existe $m_1 \in M_i$ tel que $\Pi m = Vm_1$ et, puisque $\beta_{i+1}=0$, on a $(Vm_1,0) = V'(m_1,0)$.

Réciproquement supposons i critique pour M'. Soient m et m_1 dans M_i tels que $\Pi m = Vm_1 \notin \pi M_{i+1}$. On a $\Pi(m,0) = (\Pi m, 0) = (Vm_1, 0)$; mais $(Vm_1,0)$ ne peut appartenir à $V'M'$ que si $\beta_{i+1}(Vm_1)=0$, d'où $\beta_{i+1}=0$.

LEMME (11.6). — *Supposons i critique pour M'. Alors on a ${M_i'}^{V'^{-1}\Pi} = \widetilde{M}_i^{V^{-1}\Pi}$.*

Démonstration. — Pour $m \in \widetilde{M}_i$ et $n \in M_{\varepsilon,i}$, on a $V'(m,n) = (Vm, Vn)$, car $\beta_{i+1}=0$. Par ailleurs $\Pi(m,n) = (\Pi m, \Pi n)$. Ainsi $(m,n) \in {M_i'}^{V'^{-1}\Pi}$ si et seulement si $m \in \widetilde{M}_i^{V^{-1}\Pi}$ et $n \in M_{\varepsilon,i}^{V^{-1}\Pi}$.

Mais $M_{\varepsilon,i}^{V^{-1}\Pi} = 0$. En effet $M_{\varepsilon,i} = \bigoplus_j V^j[\varepsilon](M_{i+j}/VM_{i+j+1})$ est $\mathbb{N}$-gradué, de même que $M_{\varepsilon,i+1}$; l'application $V : M_{\varepsilon,i} \to M_{\varepsilon,i+1}$ est de degré 1 pour ces graduations, alors que Π est de degré 0. Ainsi $n = \sum n_j$ est tel

que $Vn = \Pi n$ si et seulement si $\Pi n_0 = 0$ et $\Pi n_j = Vn_{j-1}$ pour $j \geq 1$. De plus $\Pi n_j = 0$ pour j pair, car i est critique pour M. On en déduit $Vn_{j-1} = 0$, donc $n_{j-1} = 0$ et $Vn_{j-2} = \Pi n_{j-1} = 0$, donc $n_{j-2} = 0$; d'où $n = 0$.

Soit (η, T, u, r) un triplet admissible rigidifié (5.8 et 5.16) représentant $\overline{\xi}(x)$. Soient $\overline{\eta} = \eta \otimes_{\mathcal{O}} \overline{k}$ et $\overline{u} : \overline{\eta} \to T$ l'application $\overline{k}$-linéaire déduite de u.

LEMME (11.7). — *(i) Si (η, T, u) possède un seul indice critique i, l'espace tangent $t_{\overline{H}}(\overline{\xi}(x))$ est de dimension 1 et s'identifie à l'espace des applications $\overline{k}$-linéaires $\delta_i : \operatorname{Ker} \overline{u}_i \to T_i$.*

(ii) Si (η, T, u) possède deux indices critiques, l'espace tangent $t_{\overline{H}}(\overline{\xi}(x))$ est de dimension 2 et s'identifie à l'espace des couples d'applications $\overline{k}$-linéaires $\delta_i : \operatorname{Ker} \overline{u}_i \to T_i \quad (i = 0, 1)$.

Démonstration. — Soient (η', T', u') une déformation de (η, T, u) au-dessus de $\overline{k}[\varepsilon]$, $\overline{\eta}' = \eta' \otimes_{\mathcal{O}} \overline{k}$ et $\overline{u}' : \overline{\eta}' \to T'$ l'application $\overline{k}$-linéaire déduite de u'. L'application $\eta' \to \eta$ est un isomorphisme et le diagramme :

$$\begin{array}{ccc} \overline{\eta}' & \xrightarrow{\sim} & \overline{\eta} \\ {\scriptstyle \overline{u}'}\downarrow & & \downarrow{\scriptstyle \overline{u}} \\ T' & \longrightarrow & T \end{array}$$

détermine une application $\overline{k}$-linéaire de degré zéro $\delta : \operatorname{Ker} \overline{u} \to \varepsilon T = \operatorname{Ker}(T' \to T)$ telle que $\Pi\delta = \delta\Pi$. Réciproquement une telle application détermine à isomorphisme près une déformation de (η, T, u) et la rigidification r de η définit une rigidification de η'.

Si i est un indice critique, les applications $\Pi : T_i \to T_{i+1}$ et $\Pi : \overline{\eta}_i \to \overline{\eta}_{i+1}$ sont nulles; par contre si i n'est pas critique ce sont des isomorphismes. Ainsi s'il y a un seul indice critique, Π identifie δ_i et δ_{i+1}; s'il y a deux indices critiques, δ_i et δ_{i+1} sont indépendants.

Remarque (11.8) a) La dimension des espaces tangents est évidente sur l'interprétation géométrique de $\overline{H}\,|_{\overline{k}}$ comme représenté par un arbre de droites projectives. Les points d'intersection de ces droites projectives sont précisément ceux où il y a deux indices critiques.

b) On notera que $\delta_i = 0$ si et seulement si l'isomorphisme $\overline{\eta}'_i \xrightarrow{\sim} \overline{\eta}_i$ induit un isomorphisme $\operatorname{Ker} \overline{u}'_i \xrightarrow{\sim} \operatorname{Ker} \overline{u}_i$.

Soient M' une déformation de M, correspondant à (β_0, β_1), et (η', T', u'), correspondant à (δ_0, δ_1), la déformation de (η, T, u) image de M' par $t_{\overline{\xi}(x)}$.

LEMME (11.9). — *Supposons i critique pour M'. Alors $\beta_i = 0$ si et seulement si $\delta_i = 0$.*

Démonstration. — Puisque i est critique pour M et M', le diagramme :

$$\begin{array}{ccc} \eta'_i & \longrightarrow & \eta_i \\ {\scriptstyle u'_i}\downarrow & & \downarrow{\scriptstyle u_i} \\ T'_i & \longrightarrow & T_i \end{array}$$

s'identifie d'après (4.5) au diagramme :

$$\begin{array}{ccc} (M'_i)^{V'^{-1}\Pi} & \longrightarrow & M_i^{V^{-1}\Pi} \\ \downarrow & & \downarrow \\ M'_i/V'M'_{i-1} & \longrightarrow & M_i/VM_{i-1}. \end{array}$$

De plus $(M'_i)^{V'^{-1}\Pi} = \widetilde{M}_i^{V^{-1}\Pi}$ d'après (11.6). Ainsi le diagramme :

$$\begin{array}{ccc} \overline{\eta}'_i & \longrightarrow & \overline{\eta}_i \\ {\scriptstyle \overline{u}'_i}\downarrow & & \downarrow{\scriptstyle \overline{u}_i} \\ T'_i & \longrightarrow & T_i \end{array}$$

s'identifie au diagramme :

$$\begin{array}{ccc} \widetilde{M}_i/\pi\widetilde{M}_i & \longrightarrow & M_i/\pi M_i \\ \downarrow & & \downarrow \\ M'_i/V'M'_{i-1} & \longrightarrow & M_i/VM_{i-1}. \end{array}$$

On a $\delta_i = 0$ si et seulement si l'isomorphisme $\overline{\eta}'_i \xrightarrow{\sim} \overline{\eta}_i$ induit une bijection $\mathrm{Ker}\,\overline{u}'_i \xrightarrow{\sim} \mathrm{Ker}\,\overline{u}_i$ (11.8). Vu les identifications ci-dessus, c'est le cas si et seulement si on a $V'M'_{i-1} \cap \widetilde{M}_i = (VM_{i-1})^{\sim}$. Etant donné la description de V' en fonction de β_i (11.3), ceci équivaut à $\beta_i = 0$.

(11.10) La proposition (11.1) résulte des lemmes précédents :

Si i est le seul indice critique pour x, les espaces tangents $t_{\overline{G}}(x)$ et $t_{\overline{H}}(\overline{\xi}(x))$ sont de dimension 1. On a $\beta_{i+1} = 0$ (11.4) et i est critique pour M' (11.5). Enfin $t_{\overline{\xi}(x)}$ est injective (11.9), donc bijective.

S'il y a deux indices critiques, les espaces tangents sont de dimension 2. Les deux sous-espaces de dimension 1 d'équation $\beta_{i+1} = 0$ de $t_{\overline{G}}(x)$ ($i = 0, 1$) sont caractérisés de manière équivalente par la condition : i critique pour M' (11.5). De plus $t_{\overline{\xi}}(x)$ est injective en restriction à ces sous-espaces (11.9) et ceux-ci sont d'images distinctes dans $t_{\overline{H}}(\overline{\xi}(x))$; donc $t_{\overline{\xi}}(x)$ est encore bijective.

12. Fin de la démonstration.

On achève dans ce paragraphe la démonstration du théorème de Drinfeld. D'après (10.5), il suffit de montrer que $\overline{\xi} : \overline{G} \to \overline{H}$ est un isomorphisme en restriction à la catégorie des $\overline{k}$-algèbres. Nous nous restreignons désormais à cette catégorie.

On a établi précédemment que l'application $\overline{\xi}(\overline{k}) : \overline{G}(\overline{k}) \to \overline{H}(\overline{k})$ induite sur les points géométriques est bijective (5.17), de même que les applications tangentes $t_{\overline{\xi}}$ en chacun de ces points (11.1). Il suffit pour conclure de montrer que $\overline{\xi}$ est représentable par un morphisme de type fini.

DÉFINITION (12.1). — Pour n et m entiers ≥ 0, on définit le sous-foncteur $G_{n,m}$ de $\overline{G}$ qui, à une $\overline{k}$-algèbre B, associe l'ensemble des classes d'isomorphie de couples (X, ρ), comme en (8.1), tels que :

1) $\pi^n\rho : \Phi_B \to X$ est une isogénie,

2) $\mathrm{Ker}(\pi^n\rho) \subset \Phi_B(\pi^{n+m})$.

On note ici $\Phi_B(\pi^{n+m})$ le noyau de π^{n+m} dans Φ_B. La condition 2) équivaut à :

2') il existe une isogénie $\beta : X \to \Phi_B$ telle que $\beta\pi^n\rho = \pi^{n+m}$.

PROPOSITION (12.2). — *Quels que soient n et m, le foncteur $G_{n,m}$ est représentable par un $\bar{k}$-schéma projectif.*

Démonstration. — Soit $\mathcal{A}$ l'algèbre de $\Phi(\pi^{n+m})$ sur $\bar{k}$. La donnée du couple (X, ρ) sur une $\bar{k}$-algèbre B est équivalente à celle du noyau Z de $\pi^n\rho$. L'algèbre $\mathcal{O}_Z$ est une B-algèbre localement libre de rang q^{4n} quotient de $\mathcal{A}_B$. Donc $G_{n,m}$ est un sous-foncteur du schéma de Hilbert $\mathrm{Hilb}(\mathcal{A}, q^{4n})$ paramétrant ces algèbres, lequel est un $\bar{k}$-schéma projectif.

De plus l'inclusion de $G_{n,m}$ dans $\mathrm{Hilb}(\mathcal{A}, q^{4n})$ est représentable par une immersion fermée. En effet la condition que Z soit un sous-schéma en $\mathcal{O}_D$-modules de $\Phi_B(\pi^{n+m})$ est fermée.

Dire par exemple que Z est stable par multiplication signifie que la flèche

$$\mu_Z : Z \times Z \to \Phi_B(\pi^{n+m}) \times \Phi_B(\pi^{n+m}) \to \Phi_B(\pi^{n+m})$$

se factorise à travers l'immersion $Z \hookrightarrow \Phi_B(\pi^{n+m})$. Autrement dit, sur les algèbres de fonctions, l'homomorphisme

$$\mu_Z^* : \mathcal{A}_B \to \mathcal{A}_B \otimes_B \mathcal{A}_B \to \mathcal{O}_Z \otimes_B \mathcal{O}_Z$$

annule le noyau J_Z de la surjection $\mathcal{A}_B \to \mathcal{O}_Z$. Les B-modules J_Z et $\mathcal{O}_Z \otimes_B \mathcal{O}_Z$ sont localement libres de rang fini et leur formation commute à tout changement de base $B \to B'$. La condition $\mu_Z^*(J_Z) = 0$ définit bien un fermé de $\mathrm{Spec}(B)$.

On vérifie de même que l'appartenance à Z de l'élément neutre et de l'inverse sont des conditions fermées, ainsi que la stabilité de Z par l'action de $\mathcal{O}_D$.

Il est clair que, pour $n \leq n'$ et $m \leq m'$, le foncteur $G_{n,m}$ est un sous-foncteur de $G_{n',m'}$. De plus :

LEMME (12.3). — *Pour toute $\bar{k}$-algèbre B, on a*

$$\overline{G}(B) = \bigcup_{n,m} G_{n,m}(B).$$

Démonstration. — Soit (X, ρ) représentant un élément de $\overline{G}(B)$. Par définition $\rho : \Phi_B \to X$ est une quasiisogénie, donc il existe un entier n tel

que $\pi^n\rho$ soit une isogénie. Pour cette isogénie, il existe un entier m et une isogénie $\beta : X \to \Phi_B$ tels que $\beta\pi^n\rho = \pi^{n+m}$ ([Zi 3], Satz 5.25).

LEMME (12.4). — *Pour $x \in G_{n,m}(\bar{k})$, l'application tangente $t_{G_{n',m'}}(x) \to t_{\overline{G}}(x)$ est bijective dès que $n' > n$ et $m' > m$.*

Démonstration. — L'application tangente en x est évidemment injective puisque $G_{n',m'}$ est un sous-foncteur de $\overline{G}$. Montrons qu'elle est surjective.

Soient (X, ρ) représentant x et (X', ρ') une déformation de (X, ρ) au-dessus de $\bar{k}[\varepsilon]$. Par hypothèse $\pi^n\rho$ est une isogénie de $\Phi_{\bar{k}}$ sur X. Alors $\pi^{n+1}\rho$ se relève en une isogénie de $\Phi_{\bar{k}[\varepsilon]}$ sur X' ([Zi 3], 4.47) et, d'après la rigidité des groupes π-divisibles, cette isogénie est nécessairement $\pi^{n+1}\rho'$.

De plus on suppose $\mathrm{Ker}(\pi^n\rho) \subset \Phi(\pi^{n+m})$, autrement dit il existe une isogénie β de X sur $\Phi_{\bar{k}}$ telle que $\beta\pi^n\rho = \pi^{n+m}$. Alors $\pi\beta$ se relève en une isogénie β' de X' sur $\Phi_{\bar{k}[\varepsilon]}$ telle que $\beta'\pi^{n+1}\rho' = \pi^{n+m+2}$, autrement dit $\ker(\pi^{n+1}\rho') \subset \Phi(\pi^{n+m+2})$.

Ainsi (X', ρ') représente un élément de $G_{n',m'}(\bar{k}[\varepsilon])$ pourvu que $n' \geq n+1$ et $m' \geq m+1$.

(12.5) Notons $\xi_{n,m}$ le morphisme de $G_{n,m}$ dans $\overline{H}$ obtenu en composant l'inclusion de $G_{n,m}$ dans $\overline{G}$ avec $\bar{\xi}$. C'est un morphisme de type fini car $G_{n,m}$ est un schéma de type fini sur $\bar{k}$.

Pour $y \in \overline{H}(\bar{k})$ il existe, d'après (5.17) et (12.3), un unique $x \in \overline{G}(\bar{k})$ tel que $y = \bar{\xi}(x)$ et des indices n_y et m_y tels que $x \in G_{n_y,m_y}(\bar{k})$. Pour $n = n_y + 1$ et $m = m_y + 1$, l'application tangente en x à $\xi_{n,m}$ est bijective, d'après (11.1) et (12.4). Ainsi $\xi_{n,m}$ est étale au voisinage de x; mieux, puisque l'application induite par $\xi_{n,m}$ sur les points géométriques est injective, c'est une immersion ouverte au voisinage de x. Autrement dit, il existe un voisinage ouvert $\mathcal{V}_y$ de y dans $\overline{H}$ au-dessus duquel $\xi_{n,m}$ est un isomorphisme.

Pour $n' > n$ et $m' > m$, le morphisme $\xi_{n',m'}$ restreint à $\mathcal{V}_y$ induit encore des bijections sur les points géométriques et les espaces tangents en ces points, c'est donc également un isomorphisme. Ainsi on a $G_{n',m'}|\mathcal{V}_y = G_{n,m}|\mathcal{V}_y$ et, d'après (12.3), $\overline{G}|\mathcal{V}_y = G_{n,m}|\mathcal{V}_y$; au-dessus de $\mathcal{V}_y$ le morphisme $\bar{\xi}$ coïncide avec $\xi_{n,m}$, c'est un isomorphisme.

Il en est de même au voisinage de chaque point de $\overline{H}$, donc $\bar{\xi}$ est un isomorphisme.

Remarque (12.6). On montrerait facilement par des raisonnements analogues que, pour tout n, il existe m tel que $G_{n,m'} = G_{n,m}$ pour $m' > m$. Le sous-foncteur G_n de $\overline{G}$ défini par la seule condition que $\pi^n\rho$ soit une isogénie est donc représentable par un $\bar{k}$-schéma projectif.

Géométriquement G_n est représenté par un sous-arbre fini de l'arbre infini de droites projectives représentant $\bar{G}$ au-dessus de $\bar{k}$.

13. Construction d'un système de revêtements de $\Omega \otimes_K \widehat{K}^{nr}$.

(13.1) Puisqu'il représente le foncteur G de (8.3), le schéma formel $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$ est muni d'un $\mathcal{O}_D$-module formel "universel", noté X. Pour tout entier $n \geq 1$, on note π^n l'endomorphisme de X au-dessus de $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$ qui traduit l'action de $\pi^n \in \mathcal{O}_D$. En chaque point géométrique s de $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$ (c'est-à-dire, de sa fibre spéciale), la restriction de π^n à la fibre X_s est une isogénie, dont la hauteur est *constante* et égale à $4n$. Utilisant alors des résultats de Th. Zink ([Zi 1]) ou (10.1), on en déduit que π^n est une *isogénie* : par suite son noyau, que nous notons X_n, est *représentable par un schéma formel en groupes, fini et localement libre sur* $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$, *de rang* q^{4n}. Il est clair d'autre part que X_n est muni d'une action de $(\mathcal{O}_D/\pi^n\mathcal{O}_D)$. Remarquons aussi que *le module des différentielles* $\Omega^1_{X_n/\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}}$ est *annulé par* π^n : il suffit en effet de le vérifier sur la section nulle, et cela résulte de la définition d'un $\mathcal{O}_D$-module formel ; en effet, π^n doit opérer sur Lie (X) via le morphisme structural, et il en résulte que, localement sur $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$, l'algèbre affine de X_n est engendrée par deux "coordonnées" x_1 et x_2 vérifiant des équations $F_i(x_1, x_2) = 0$ ($i = 1$ ou 2), avec :

$$F_i = \pi^n x_i + (\text{termes de degré} \geq 2).$$

On a donc bien, sur la section nulle : $\pi^n dx_i = 0$.

On peut exprimer essentiellement la même chose en disant que X_n est "formellement étale au-dessus de $\widehat{\Omega}\widehat{\otimes}_{\mathcal{O}}\widehat{\mathcal{O}}^{nr}$ en dehors de la fibre spéciale "([El]).

(13.2) Notons alors $\mathcal{X}_n$ *l'espace rigide* associé à X_n, c'est-à-dire sa fibre générique au sens de Raynaud ([Ra 1]). D'après ce que l'on vient de voir, $\mathcal{X}_n$ est un *revêtement fini étale* de $\Omega \otimes_K \widehat{K}^{nr}$ (l'espace rigide sur $\widehat{K}^{nr}$ déduit de Ω par extension des scalaires), fibré en $(\mathcal{O}_D/\pi^n\mathcal{O}_D)$-modules. On a des inclusions $\mathcal{X}_{n-1} \hookrightarrow \mathcal{X}_n$, où $\mathcal{X}_{n-1}$ apparaît comme le sous-espace des points de $\mathcal{X}_n$ tués par π^{n-1}. Nous noterons $\mathcal{X}_{n-1/2}$ l'espace intermédiaire constitué des points de $\mathcal{X}_n$ tués par Π^{2n-1}.

On sait d'autre part que le cardinal des fibres de $\mathcal{X}_n$ est égal à q^{4n}, c'est-à-dire au cardinal de $(\mathcal{O}_D/\pi^n\mathcal{O}_D)$. Il est immédiat d'en déduire que ces fibres sont des $(\mathcal{O}_D/\pi^n\mathcal{O}_D)$-modules *libres de rang* 1 (tout élément de $\mathcal{X}_n - \mathcal{X}_{n-1/2}$ en constitue une base).

Considérons alors le complémentaire : $\Sigma_n \underset{\text{déf}}{=} \mathcal{X}_n - \mathcal{X}_{n-1/2}$, constitué des points de $\mathcal{X}_n$ "exactement tués par π^n". Il résulte de tout ce qui précède

que Σ_n *constitue un revêtement étale galoisien de* $\Omega \otimes_K \widehat{K}^{nr}$, *de groupe de Galois* $(\mathcal{O}_D/\pi^n\mathcal{O}_D)^*$. Pour n variable, les Σ_n forment un *système projectif*, via l'isogénie π qui induit des morphismes : $X_{n+1} \to X_n$, $\mathcal{X}_{n+1} \to \mathcal{X}_n$, $\Sigma_{n+1} \to \Sigma_n$; le groupe de Galois de ce système est le complété profini $\widehat{\mathcal{O}}_D^*$ de $\mathcal{O}_D^*$.

Il est important enfin de noter que les revêtements qu'on vient de construire sont *équivariants* relativement à l'action de $GL(2, K)$ considérée en (9.3) : il est clair en effet que cette dernière se relève en une action sur le $\mathcal{O}_D$-module universel X, d'où une action sur X_n, $\mathcal{X}_n$, Σ_n.

(13.3) *Quelques remarques.*

(a) Utilisant par exemple des résultats de Elkik ([El]), on peut montrer que la catégorie des revêtements étales finis de $\Omega \otimes_K \widehat{K}^{nr}$ est équivalente à celle des revêtements étales finis de $\Omega \otimes_K K^{nr}$. La construction ci-dessus définit donc un système de revêtements étales, encore notés Σ_n, de $\Omega \otimes_K K^{nr}$.

(b) On remarquera que cette construction de Σ_n est de nature purement rigide-analytique : bien que l'on sache "abstraitement" que Σ_n doit provenir d'un certain schéma formel $\widehat{\Sigma}_n$, ce dernier n'est pas construit (il faudrait pour cela définir ce qu'est une "base de Drinfeld" dans la présente situation).

(c) L'article [Ca 2] indique une méthode qui permet de calculer par voie globale — c'est-à-dire en utilisant le théorème de Čerednik-Drinfeld — la cohomologie des revêtements Σ_n : cela fournit une réalisation géométrique à la fois de la correspondance de Jacquet-Langlands (entre représentations de $GL(2, K)$ et D^*) et de celle de Langlands (entre représentations de $GL(2, K)$ et du groupe de Weil W_K).

Chapitre III : Le théorème de Čerednik-Drinfeld

0. Introduction et notations.

0.1. — On suppose fixé dans toute la suite un corps de quaternions Δ, indéfini, de centre $\mathbb{Q}$. Cela définit un groupe réductif sur $\mathbb{Q}$, noté Δ^* ("le groupe multiplicatif de Δ") tel que l'on ait, pour toute $\mathbb{Q}$-algèbre R :

$$\Delta^*(R) = (\Delta \otimes R)^* \quad \text{(et donc } \Delta^*(\mathbb{Q}) = \Delta^*\text{)}.$$

Le groupe $\Delta^*(\mathbb{R})$, en particulier, est alors isomorphe à $GL(2,\mathbb{R})$. Un tel isomorphisme étant fixé, $\Delta^*(\mathbb{R})$ opère donc sur le "double" demi-plan de Poincaré :

$$\mathcal{H}^{\pm} = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R}).$$

Soit d'autre part $U \subset \Delta^*(\mathbb{A}_f)$ un sous-groupe compact ouvert du groupe des points de Δ^* à valeurs dans les adèles finies. On associe alors à ces données la *courbe de Shimura*, notée S_U, définie sur $\mathbb{Q}$, dont l'ensemble des points complexes est décrit par la formule suivante :

$$S_U(\mathbb{C}) = \Delta^*(\mathbb{Q})\backslash[\mathcal{H}^{\pm} \times \Delta^*(\mathbb{A}_f)/U].$$

Le quotient que l'on vient d'écrire n'est d'ailleurs rien d'autre, ainsi que l'on vérifie facilement, que la réunion d'un nombre fini de quotients $\Gamma_i\backslash\mathcal{H}$ du demi-plan de Poincaré $\mathcal{H}$ par des sous-groupes arithmétiques Γ_i (i.e. commensurables à $\Delta^*(\mathbb{Z})$ pour une structure entière arbitraire). C'est en particulier une surface de Riemann compacte, mais en général disconnexe. Sa $\mathbb{Q}$-structure a été définie par Shimura, dans le cadre d'une théorie beaucoup plus générale pour laquelle nous renvoyons à [De]. Nous nous bornons à décrire ici (au §1) un problème de modules, défini sur $\mathbb{Q}$, représentable par S_U. Des situations plus générales, où Δ est une algèbre de quaternions de centre un corps totalement réel, ont été décrites dans [Mi] et [Br-La] (cas totalement indéfini), ainsi que dans [Ca 1] (cas des courbes).

0.2. — Notons δ le produit des nombres premiers où Δ est ramifiée. Les méthodes développées tant dans [Mi] et [Br-La] que dans [Ca 1] avaient pour but de décrire la réduction de S_U en un nombre premier ne divisant pas δ. Ici au contraire notre but est d'étudier la courbe S_U en un nombre premier p (fixé une fois pour toutes) *divisant* δ.

Le groupe $\Delta^*(\mathbb{Q}_p) = \Delta_p^*$ est le groupe multiplicatif du *corps* $\Delta_p = \Delta \otimes \mathbb{Q}_p$. Il possède un unique sous-groupe compact maximal noté U_p^0 (constitué des unités de l'unique ordre maximal de Δ_p). Ce sous-groupe maximal est filtré par une famille décroissante $(U_p^n)_{n\geq 0}$ de sous-groupes distingués, où U_p^n désigne le sous-groupe des unités qui sont congrues à 1 modulo la puissance $n^{\text{ième}}$de l'idéal maximal. Nous supposerons toujours que notre sous-groupe $U \subset \Delta^*(\mathbb{A}_f)$ se décompose comme un produit $U = U_p^n \cdot U^p$, où $U^p \subset \Delta^*(\mathbb{A}_f^p)$ est un sous-groupe compact ouvert arbitraire.

0.3. — Sous sa forme originelle, le théorème de Čerednik décrit, dans le cas où $n = 0$ (c'est-à-dire dans le cas où U est "maximal en p"), une uniformisation p-adique de $S_U \otimes \mathbb{Q}_p$ en termes de quotients à la Mumford ([Mu 2]) du "demi-plan" non-archimédien $\Omega = \Omega_{\mathbb{Q}_p}$. La démonstration modulaire de Drinfeld que nous allons exposer ici permet de retrouver ce résultat, tout en comparant la famille universelle de variétés abéliennes portée par S_U à la famille universelle de groupes formels portée par $\widehat{\Omega}$. Il en résulte alors aisément, pour $n > 0$, une uniformisation de $S_U \otimes \mathbb{Q}_p$ en termes des mystérieux revêtements Σ_n de Ω que le théorème local fondamental permet de définir.

0.4. — Nous nous plaçons dans le cas où $n = 0$. Nous commençons par rappeler (§1) quel est le problème de modules sur $\mathbb{Q}$, et donc sur $\mathbb{Q}_p$. Puis nous définissons au §3 un problème de modules sur $\mathbb{Z}_p$ qui le "prolonge" naturellement. Ce prolongement est possible parce que la "structure de niveau" est concentrée en dehors de p (car $n = 0$), et qu'elle garde donc un sens en caractéristique p. La seule chose qu'on ajoute en passant de $\mathbb{Q}_p$ à $\mathbb{Z}_p$ est une condition, en caractéristique p, portant sur le groupe formel de la variété abélienne, condition identique à celle que nous avons déjà rencontrée pour le foncteur que représente $\widehat{\Omega}$.

Puis on montre que le foncteur prolongé est représentable par un $\mathbb{Z}_p$-schéma en courbes propre (mais non lisse) $\mathbf{S}_U$ de fibre générique $S_U \otimes \mathbb{Q}_p$; pour prouver ce résultat, on a besoin de montrer que les variétés abéliennes considérées sont canoniquement munies d'une polarisation principale compatible à une involution positive bien choisie (que nous allons bientôt définir) de Δ : c'est l'objet du §4. Auparavant, on a prouvé au §2 que tous

les $\overline{\mathbf{F}}_p$-points de $\mathbf{S}_U$ sont dans la même classe d'isogénie : c'est là une différence fondamentale avec le cas où p ne divise pas δ.

Alors on est en mesure d'énoncer (au §5) le théorème de Čerednik-Drinfeld et ses différentes variantes. On le prouve au §6 au moyen du théorème local fondamental du chapitre II.

0.5. — Fixons dans toute la suite un *ordre maximal* noté $\mathcal{O}_\Delta$ dans Δ (rappelons qu'ils sont tous conjugués, ainsi qu'il résulte du théorème d'approximation forte). On impose qu'il soit *stable par l'involution canonique* $x \longrightarrow \overline{x}$ de Δ (cela n'était pas imposé dans [Br – La] ni dans [Mi]) ; que cela soit possible se voit localement à chaque place (la donnée d'un ordre maximal global $\mathcal{O}_\Delta$ est équivalente à la donnée, pour toutes les places finies v, d'un ordre maximal local $\mathcal{O}_{\Delta_v} = \mathcal{O}_\Delta \otimes \mathbb{Z}_v$ dans $\Delta_v = \Delta \otimes \mathbb{Q}_v$, ces données locales étant astreintes à coïncider presque partout avec celles provenant d'un ordre global fixé arbitraire).

Une involution positive $x \to x^*$ de Δ s'obtient, ainsi qu'il est expliqué dans (loc. cit.), en conjuguant l'involution canonique par un élément $t \in \Delta^*$ dont le carré t^2 est un élément négatif de $\mathbb{Q}$:

$$x^* = t^{-1}\overline{x}t.$$

Dans le cas présent, il sera utile de faire un choix plus précis de t. Ce choix résultera du lemme facile suivant, que l'on laisse au lecteur :

LEMME. — *On peut choisir t tel que : $t \in \mathcal{O}_\Delta$; $t^2 = -\delta$.* [Il suffit de remarquer que $\mathbb{Q}(\sqrt{-\delta})$ est un corps neutralisant pour Δ].

Nous supposerons dans la suite que t est ainsi fixé, et donc aussi l'involution positive $x \to x^*$; noter que cette dernière stabilise l'ordre $\mathcal{O}_\Delta$.

Pour terminer cette liste de notations, nous noterons W l'ordre $\mathcal{O}_\Delta$, vu avec sa structure de $\mathcal{O}_\Delta$-module à gauche, et $V = W \otimes \mathbb{Q}$ (un Δ-module à gauche). Nous nous intéresserons surtout aux différentes complétions $W_\ell = W \otimes \mathbb{Z}_\ell$ (vues comme des $\mathcal{O}_{\Delta_\ell}$-modules à gauche), et aux $V_\ell = W \otimes \mathbb{Q}_\ell$ (des Δ_ℓ-modules). On notera que le groupe $\mathrm{Aut}_{\Delta_\ell}(V_\ell)$ s'identifie à $\Delta^*(\mathbb{Q}_\ell) = \Delta_\ell^*$, un élément g agissant par multiplication à droite par g^{-1}.

Enfin, nous utiliserons, pour A une variété abélienne, les notations standard : A_n pour désigner le groupe des points de n-torsion, $T_\ell(A)$ pour le module de Tate et $V_\ell(A)$ pour $T_\ell(A) \otimes \mathbb{Q}$. On dénotera enfin par $T_f(A)$ le produit des modules de Tate pour tous les nombres premiers ℓ, et $V_f(A)$ le produit restreint des $V_\ell(A)$.

1. Le problème de modules sur C ; polarisations.

1.1. — Un problème de modules représentable par S_U est décrit dans [Mi] et [Gi] dans le cas plus général où Δ est une algèbre de quaternions indéfinie sur un corps totalement réel. Dans le cas particulier qui nous intéresse ici, on obtient :

THÉORÈME (1.1). — *La courbe $S_U/\mathbf{C}$ représente, si U est assez petit (voir plus loin), le foncteur $\mathcal{M}_U : Sch/\mathbf{C} \to \mathcal{E}ns$ défini comme suit : Pour $S \in Sch/\mathbf{C}$, $\mathcal{M}_U(S)$ est l'ensemble des classes d'isomorphie de triplets $(A, \iota, \overline{\nu})$ tels que :*

(i) A est un schéma abélien sur S de dimension relative 2.

(ii) $\iota : \mathcal{O}_\Delta \to \mathrm{End}_S A$ est une action de $\mathcal{O}_\Delta$ sur A.

(iii) $\overline{\nu}$ est une structure de niveau U sur A. (voir ci-dessous).

Remarque : On appelle parfois le couple (A, ι) une "fausse courbe elliptique". Dans l'introduction de [De-Ra], on explique pourquoi la réduction de tels objets, en un nombre premier *ne divisant pas* δ, se comporte comme celle des courbes elliptiques usuelles.

1.2. — Commençons par rappeler, d'après [Bo], comment définir une "structure de niveau U" :

(a) Dans le cas particulier où $U = U(N)$ est le sous-groupe des unités de $(\mathcal{O}_\Delta \otimes \widehat{\mathbf{Z}})$ qui sont congrues à 1 modulo un entier N, une structure de niveau U (ou N) est la donnée d'un isomorphisme $\mathcal{O}_\Delta$-linéaire :

$$\nu : A_N \simeq W \otimes (\mathbf{Z}/N\mathbf{Z}).$$

(b) Dans le cas général, on choisit un quelconque entier N tel que $U(N) \subset U$. Une structure de niveau U est alors la donnée, localement pour la topologie étale, d'une classe $\overline{\nu}$ modulo U d'isomorphismes ν comme ci-dessus. [On vérifie sans mal que cette définition est indépendante du choix de N].

(c) Pour S le spectre d'un corps algébriquement clos, on peut encore voir une telle structure de niveau comme la donnée d'une classe $\overline{\nu}$ modulo U d'isomorphismes :

$$\nu : T_f(A) \simeq W \otimes \widehat{\mathbf{Z}}.$$

Il est même possible de se placer plutôt, comme expliqué dans [De], dans la catégorie des variétés abéliennes à isogénie près, et de voir les structures de niveau comme des classes modulo U d'isomorphismes $V_f(A) \simeq W \otimes \mathbf{A}_f$. C'est de cette dernière façon que l'on décrit le plus simplement l'action du

groupe $\Delta^*(\mathbb{A}_f)$ sur le système projectif des S_U – ou si l'on préfère, l'action des opérateurs de Hecke.

1.3. — *Remarque sur la condition "U assez petit" :* C'est la condition qui assure que les structures de niveau U sont assez rigides pour éliminer les automorphismes non triviaux. Il suffit par exemple (voir [Bo]) que U soit contenu dans $U(M)$ pour M un entier ≥ 3. Lorsque U est de la forme $U_p^0 \cdot U^p$, il suffit évidemment de supposer U^p assez petit pour que U le soit : dans la mesure où le théorème de Čerednik que nous voulons prouver est "invariant" par le remplacement de U^p par un sous-groupe, nous pourrons toujours dans la suite supposer que la condition est satisfaite.

1.4. — Le problème de modules que nous venons de décrire est en fait défini et représentable sur le corps $\mathbb{Q}$, et l'on peut le prendre comme définition de la $\mathbb{Q}$-structure sur S_U. Dans [Mi] et [Bo], on explique comment il se prolonge et définit un schéma en courbes propre et lisse au-dessus de $\mathbb{Z}\left[\frac{1}{\delta N}\right]$, où N est un entier tel que $U(N) \subset U$. Ici au contraire notre objectif est d'étudier ce qui se passe en p (rappelons que $p|\delta$). Nous définirons donc dans la suite un problème de modules au-dessus de $\mathbb{Z}_p$, qui s'avèrera représentable par un schéma en courbes propre et plat (mais non lisse !).

1.5. — *Polarisations.*

Rappelons (*cf.* loc. cit.) que, pour chaque triplet $(A, \iota, \overline{\nu})$ comme plus haut, une $*$-polarisation est une polarisation λ de A telle que, en chaque point géométrique s de S, l'involution de Rosati correspondante sur $\mathrm{End}^0(A_s)$ induise sur $\mathcal{O}_\Delta$ (via ι) l'involution $*$. Il revient au même d'exiger que, pour tout $d \in \mathcal{O}_\Delta$, le diagramme suivant soit commutatif :

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A^* \\ {\scriptstyle \iota(d^*)}\downarrow & & \downarrow{\scriptstyle \iota(d)^*} \\ A & \xrightarrow{\lambda} & A^* \end{array}$$

PROPOSITION (1.5). — *Soit S un schéma de caractéristique 0 et $(A, \iota, \overline{\nu}) \in \mathcal{M}_U(S)$. Alors il existe sur A une $*$-polarisation principale. Une telle polarisation est unique.*

Preuve : On se ramène aussitôt au cas où $S = \mathrm{Spec}(\mathbb{C})$. Dans loc. cit. (*cf.* par exemple [Mi], Lemma 1.1 ou [Bo] §8), on avait montré l'existence d'une $*$-polarisation, et son unicité à un nombre rationnel près. Ce que nous avons en plus ici, c'est la possibilité de la choisir principale (et, évidemment, un tel choix est unique). Cela résulte clairement du

lemme suivant, compte tenu de l'existence d'un isomorphisme $\mathcal{O}_\Delta$-linéaire $T_\ell A \simeq W_\ell$:

LEMME (1.6). — *Pour tout nombre premier ℓ, considérons l'ensemble des applications bilinéaires antisymétriques :*

$$\psi : W_\ell \times W_\ell \longrightarrow \mathbb{Z}_\ell,$$

qui vérifient :

$$\forall d \in \mathcal{O}_{\Delta_\ell} \qquad \psi(dx, y) = \psi(x, d^* y).$$

Cet ensemble constitue un $\mathbb{Z}_\ell$-module libre de rang 1, et tout générateur ψ_0 de ce module définit une auto-dualité parfaite sur W_ℓ.

Preuve du lemme : (*cf.* la preuve du lemme 1.1 de [Mi]). Soit ψ comme dans l'énoncé du lemme. Se rappelant que W_ℓ peut être identifié à $\mathcal{O}_{\Delta_\ell}$, on peut écrire :

$$\psi(x, y) = \varphi(x^* y)$$

où φ est la forme linéaire $\varphi(u) = \psi(1, u)$. On peut exprimer φ au moyen de la trace réduite tr, par l'expression :

$$\varphi(u) = tr(d_0 t u^*) = tr(d_0 \overline{u} t),$$

avec d_0 un élément de Δ_ℓ. L'antisymétrie de ψ se traduit par l'identité $\varphi(u^*) = -\varphi(u)$, et un bref calcul montre que cela équivaut encore à : $\overline{d_0} = d_0$, soit $d_0 \in \mathbb{Q}_\ell$. On en déduit que le lemme résultera du :

Sous-lemme (1.7). L'application $\psi_0 : W_\ell \times W_\ell \to \mathbb{Q}_\ell$ définie par :

$$\begin{cases} si \quad \ell \not| \delta \ \psi_0(x, y) = tr(t y^* x) \\ si \quad \ell \mid \delta \ \psi_0(x, y) = \ell^{-1} tr(t y^* x) \end{cases}$$

prend ses valeurs dans $\mathbb{Z}_\ell$, et induit sur W_ℓ une autodualité parfaite.

Ce sous-lemme se vérifie immédiatement : dans le premier cas ($\ell \not| \delta$), on peut supposer que $\mathcal{O}_{\Delta_\ell} = M_2(\mathbb{Z}_\ell)$, et il est bien connu que la trace y définit une autodualité parfaite. Or l'involution $*$ définit un automorphisme de $M_2(\mathbb{Z}_\ell)$, et nos hypothèses sur t entraînent que $t \in Gl_2(\mathbb{Z}_\ell)$, d'où le résultat dans ce cas. Dans l'autre cas ($\ell | \delta$), $\mathcal{O}_{\Delta_\ell}$ est l'ordre maximal d'un corps de quaternions et t une "uniformisante" de cet ordre ; or il est bien connu dans ce cas que la trace met en dualité $\mathcal{O}_{\Delta_\ell}$ et $t^{-1}\mathcal{O}_{\Delta_\ell}$. Le sous-lemme en résulte.

Remarque : On notera que la validité du lemme 1, et donc de la proposition 1, dépend entièrement du choix très particulier que nous avons effectué de l'élément t, et donc de l'involution $*$.

2. Application du théorème de Tate-Honda.

Le prochain paragraphe sera consacré à étendre le problème de modules précédent $\mathcal{M}_U$ (avec $U = U_p^0 U^p$) en un problème de modules $\mathbf{M}_U$ défini au-dessus de $\mathbb{Z}_p$. La proposition suivante, que nous plaçons ici pour la commodité de l'exposition, signifiera que tous les points à valeurs dans $\overline{\mathbb{F}}_p$ sont dans la même classe d'isogénie.

PROPOSITION 2. — *Il n'y a qu'une seule classe d'isogénie de couples (A, ι) où A est une variété abélienne de dimension 2 sur $\overline{\mathbb{F}}_p$ munie d'une action ι de l'ordre $\mathcal{O}_\Delta$. En particulier, la variété A est isogène au produit de deux courbes elliptiques supersingulières. L'algèbre* $\mathrm{End}^0_{\mathcal{O}_\Delta}(A) = \mathrm{End}_{\mathcal{O}_\Delta}(A) \otimes \mathbb{Q}$ *des endomorphismes d'un tel couple (dans la catégorie "à isogénie près") est isomorphe à l'algèbre de quaternions $\overline{\Delta}$ déduite de Δ en changeant les invariants en p et à l'infini (c'est-à-dire que $\overline{\Delta}$ est définie, non ramifiée en p, et que $\overline{\Delta}_\ell$ est isomorphe à Δ_ℓ pour tout $\ell \neq p, \infty$).*

La preuve de cette proposition est une application standard du théorème de Tate-Honda.

(a) On commence par montrer que A est isogène au produit de deux courbes elliptiques supersingulières :

– Le groupe p-divisible A_{p^∞} de A ne possède pas de partie étale (et donc, par dualité, pas de partie multiplicative) ; en effet, si la composante étale était non triviale, elle serait de dimension 1 ou 2. Mais $\mathcal{O}_\Delta$ ne saurait y opérer, car il n'existe pas d'homomorphisme d'algèbres : $\Delta_p \to \mathbb{Q}_p$, ni $\Delta_p \to M_2(\mathbb{Q}_p)$. Cette contradiction prouve donc que A_{p^∞} est isogène au produit de deux copies du groupe p-divisible d'une courbe elliptique supersingulière.

– On applique alors le théorème de Tate-Honda (*cf.* [Br] ou [Ta 2]) : Si A n'est pas isogène au produit de deux courbes elliptiques (nécessairement supersingulières d'après ce qui précède), elle est simple. Supposons la définie sur une extension finie $\mathbb{F}_q$ de $\mathbb{F}_p$, et notons π l'endomorphisme de Frobenius F_q. De la structure du groupe p-divisible, on déduit que l'élément π^2/q est une unité du corps $\mathbb{Q}(\pi)$: parce que cette unité est de valeur absolue 1 à chaque place, c'est une racine de l'unité : quitte à étendre le corps $\mathbb{F}_q$, on peut donc supposer que $\pi = \sqrt{q} \in \mathbb{Q}$. Mais alors A serait une courbe elliptique supersingulière ! Cette contradiction prouve que A est bien, comme annoncé, isogène au produit de deux courbes elliptiques supersingulières.

(b) Il en résulte que $\mathrm{End}^0(A)$ est isomorphe à l'algèbre $M_2(H)$, où H désigne le corps de quaternions sur $\mathbb{Q}$ qui se ramifie exactement en p et ∞. L'unicité à isogénie près d'un couple (A, ι) signifie que tous les

plongements $\Delta \hookrightarrow M_2(H)$ sont conjugués, et cela résulte du théorème de Skolem-Noether.

(c) Place par place, on vérifie que $\Delta \otimes \overline{\Delta}$ est isomorphe à $M_2(H)$. Cela prouve à la fois l'existence d'un plongement $\Delta \hookrightarrow M_2(H)$, et le fait que l'algèbre $\mathrm{End}^0_{\mathcal{O}_\Delta}(A)$ (laquelle s'identifie au commutant de Δ dans $M_2(H)$) est isomorphe à $\overline{\Delta}$.

Remarque : Pour A comme ci-dessus, et $\ell \neq p$, on voit que $V_\ell(A)$ est un Δ_ℓ-module isomorphe à V_ℓ (car de dimension 4 sur $\mathbb{Q}_\ell$), muni d'une action (Δ_ℓ-linéaire) de l'algèbre $\mathrm{End}^0_{\mathcal{O}_\Delta}(A)$. Or il est clair que $\mathrm{End}_{\Delta_\ell}(V_\ell)$ s'identifie naturellement à l'algèbre Δ_ℓ^{opp} *opposée* à Δ_ℓ (opérant par multiplication à droite). Le choix d'isomorphismes $V_\ell(A) \simeq V_\ell$ et $\overline{\Delta} \simeq \mathrm{Aut}^0_{\mathcal{O}_\Delta}(A)$ détermine donc un isomorphisme, pour chaque $\ell \neq p$: $\overline{\Delta}_\ell \simeq \Delta_\ell^{opp}$, d'où un isomorphisme :

$$\overline{\Delta} \otimes \mathbb{A}_f^p \simeq \Delta^{opp} \otimes \mathbb{A}_f^p.$$

3. Le problème de modules au-dessus de $\mathbb{Z}_p$.

3.1. — Nous nous plaçons dans la situation où le sous-groupe compact U est de la forme $U_p^0 U^p$, i.e. est "maximal en p", et nous allons dans ce cas étendre le problème de modules précédent en un problème de modules défini au-dessus de $\mathbb{Z}_p$ (ou, ce qui revient exactement au même, au-dessus du localisé $\mathbb{Z}_{(p)}$ de $\mathbb{Z}$ en p). Commençons par remarquer que, dans cette situation, il existe un entier N *premier à* p tel que l'on ait : $U(N) \subset U$ (*cf.* §1.2). De ce fait, il résulte que la notion de structure de niveau U, rappelée au §1, garde un sens en caractéristique p. Cela va nous permettre de définir un problème de modules $\mathbf{M}_U$ au-dessus de $\mathbb{Z}_p$, dans les mêmes termes que celui que nous avons défini en caractéristique 0 ; la seule différence est l'introduction d'une condition supplémentaire portant sur les points de caractéristique p.

DÉFINITION. — *Si S est un $\mathbb{Z}_p$-schéma, $\mathbf{M}_U(S)$ est l'ensemble des classes d'isomorphie de triplets $(A, \iota, \overline{\nu})$ tels que :*

(i) *A est un schéma abélien sur S de dimension relative 2.*

(ii) *$\iota : \mathcal{O}_\Delta \to \mathrm{End}_S(A)$ est une action de $\mathcal{O}_\Delta$ sur A.*

On impose la condition suivante, pour chaque point géométrique $s = \mathrm{Spec}\, k(s)$ de caractéristique p de S : Notons $\mathbb{Z}_p^{(2)}$ l'anneau des entiers de l'extension quadratique non ramifiée de $\mathbb{Q}_p$. Cet anneau se plonge dans $\mathcal{O}_{\Delta_p}$ (plongement bien défini à conjugaison près). On exige que l'action

de $\mathbf{Z}_p^{(2)}$ *sur* $\mathrm{Lie}(A_s)$ *se décompose comme la somme des deux plongements* $\mathbf{Z}_p^{(2)} \otimes \mathbf{F}_p \simeq \mathbf{F}_{p^2} \hookrightarrow k(s)$.

(On dit alors que le couple (A, ι) *est "spécial").*

(iii) $\overline{\nu}$ *est une structure de niveau* U *sur* A.

3.2. *Quelques remarques sur la condition "spéciale".*

(a) On voit que la condition porte en fait sur le complété formel de A à l'origine – ou si l'on préfère sur le groupe p-divisible A_{p^∞} ; ce n'est rien d'autre que la condition que nous avons déjà rencontrée au chapitre précédent : Dire que A est une $\mathcal{O}_\Delta$-variété spéciale équivaut à dire que le groupe formel associé est un $\mathcal{O}_{\Delta_p}$-module formel spécial (chap. II §2.1).

(b) Supposons que S soit un $\mathbf{Z}_p^{(2)}$-schéma (une condition que l'on peut toujours, quitte à effectuer un changement de base étale, supposer satisfaite). Le $\mathcal{O}_S$-module $\mathrm{Lie}(A)$ est alors muni d'une action de l'anneau $\mathbf{Z}_p^{(2)} \otimes \mathbf{Z}_p^{(2)}$, isomorphe à $\mathbf{Z}_p^{(2)} \oplus \mathbf{Z}_p^{(2)}$. Cette action décompose $\mathrm{Lie}(A)$ en la somme directe de deux $\mathcal{O}_S$-modules projectifs $\mathrm{Lie}^1(A) \oplus \mathrm{Lie}^2(A)$, de telle sorte que $\mathbf{Z}_p^{(2)} \subset \mathcal{O}_{\Delta_p}$ opère sur le premier via le morphisme structural $\mathbf{Z}_p^{(2)} \to \mathcal{O}_S$, et sur le second via le composé de ce morphisme par la conjugaison de $\mathbf{Z}_p^{(2)}$. La condition "spéciale", telle qu'elle est reformulée dans la variante ci-dessus, signifie que le rang de chacun de ces deux $\mathcal{O}_S$-modules est égal à 1 en chaque point géométrique de caractéristique p de S. Cela a aussi un sens en un point de caractéristique 0, et la condition est alors automatique [car, pour l'unique représentation $\Delta_p \hookrightarrow M_2(\overline{\mathbf{Q}}_p)$, il est vrai que l'action de $\mathbf{Z}_p^{(2)} \hookrightarrow \Delta_p$ fait intervenir chacun des deux plongements $\mathbf{Z}_p^{(2)} \hookrightarrow \overline{\mathbf{Q}}_p$].

Parce que le rang d'un $\mathcal{O}_S$-module projectif est localement constant, on voit que, *pour* S *connexe, la condition est satisfaite dès qu'elle l'est en un seul point géométrique.* En particulier, *la condition est automatique pour* S *un* $\mathbf{Z}_p$*-schéma plat* (en effet, elle est satisfaite en les points de caractéristique 0). Autrement dit, elle est satisfaite pour tout couple (A, ι) qui "provient de la caractéristique 0". Elle est donc nécessaire si l'on veut que $\mathbf{M}_U$ soit représentable par un schéma plat sur $\mathbf{Z}_p$.

3.3. *Représentabilité.*

Pour établir la représentabilité du foncteur $\mathbf{M}_U$, nous aurons besoin de la proposition suivante, qui généralise la proposition 1. La notion de $*$-polarisation se définit comme au §1 (*cf.* aussi ([Bo] §8)).

PROPOSITION (3.3). — *Soit $(A, \iota, \overline{\nu}) \in \mathbf{M}_U(S)$, pour S un quelconque $\mathbb{Z}_p$-schéma. Alors il existe sur A une $*$-polarisation principale, et cette dernière est uniquement déterminée.*

Nous allons provisoirement admettre ce résultat – dont la démonstration fera l'objet du prochain paragraphe. En l'utilisant, nous allons commencer par prouver le :

THÉORÈME (3.4). — *Le foncteur $\mathbf{M}_U$ défini précédemment est représentable – si U^p est assez petit – par un $\mathbb{Z}_p$-schéma projectif $\mathbf{S}_U$ de fibre générique $S_U \otimes \mathbb{Q}_p$.*

Remarque : On peut montrer, par exemple en utilisant le théorème de Čerednik que nous allons prouver, que $\mathbf{S}_U$ est *plat* sur $\mathbb{Z}_p$.

Preuve du théorème :

(a) La proposition qui précède définit un morphisme de foncteurs de $\mathbf{M}_U$ vers le foncteur "variétés abéliennes principalement polarisées". Pour prouver la représentabilité de $\mathbf{M}_U$ par un schéma quasi-projectif, il nous suffit de prouver qu'il est relativement représentable au-dessus du champ modulaire de Siegel. Mais ceci est une conséquence facile de la théorie des schémas de Hilbert.

(b) La projectivité résultera, compte tenu du critère valuatif de propreté, du lemme suivant ("potentiellement bonne réduction") :

LEMME (3.5). — *Soit V une $\mathbb{Z}_p$-algèbre de valuation discrète de corps des fractions noté L, et soit $x = (A, \iota, \overline{\nu})$ un point de $\mathbf{M}_U(L)$. Alors il existe une extension finie L' de L et un point $\tilde{x} = (\tilde{A}, \tilde{\iota}, \tilde{\overline{\nu}})$ de $\mathbf{M}_U$ à valeurs dans la clôture intégrale V' de V dans L', tel que l'image de $\tilde{x}$ dans $\mathbf{M}_U(L')$ coïncide avec celle de x.*

La preuve de ce lemme est standard : D'après le théorème de réduction semi-stable, il existe une extension finie L' de L telle que le modèle de Néron de $A_{L'}$ admette comme fibre spéciale une extension d'une variété abélienne par un tore T.

On commence par montrer que *T est trivial* : En effet $\mathcal{O}_\Delta$ y opère par fonctorialité du modèle de Néron. Si T n'est pas trivial, $X_*(T)$ est un $\mathbb{Z}$-module de rang 1 ou 2 muni d'une action de $\mathcal{O}_\Delta$, ce qui est visiblement impossible.

Donc le modèle de Néron est un schéma abélien $\widetilde{A}$ sur V'. Par fonctorialité, il est muni d'une action $\tilde{\iota}$ de $\mathcal{O}_\Delta$, qui vérifie la condition "spéciale" en vertu de la remarque (3.2.b). Quant à la structure de niveau, elle s'étend de façon unique, et tout cela prouve le lemme.

4. Polarisations [Preuve de la proposition (3.3)].

4.1. — Commençons par établir l'existence d'une $*$-polarisation (non nécessairement principale) lorsque la base est $\overline{\mathbf{F}}_p$.

LEMME (4.1). — *Soit A une variété abélienne sur $\overline{\mathbf{F}}_p$, munie d'une action de $\mathcal{O}_\Delta$. Alors il existe sur A une $*$-polarisation. Une telle polarisation est unique à multiplication près par un rationnel positif.*

Preuve : Il suffit de montrer l'existence, et l'unicité à un scalaire ($\in \mathbf{R}^{*+}$) près, d'un élément de $NS(A) \otimes \mathbf{R}$, contenu dans le cône positif des polarisations, tel que l'involution associée de $\mathrm{End}(A) \otimes \mathbf{R}$ induise l'involution $*$ sur Δ.

D'après le §2, A est isogène au produit de deux courbes elliptiques supersingulières. Il en résulte qu'on peut identifier $\mathrm{End}(A) \otimes \mathbf{R}$ à l'algèbre $M_2(\mathbf{H})$, et $NS(A) \otimes \mathbf{R}$ au sous-espace des éléments de $M_2(\mathbf{H})$ qui sont fixés par l'involution $z \to {}^t\overline{z}$ [où $z \to \overline{z}$ provient de l'involution canonique de $\mathbf{H}$]. Avec cette identification, l'involution "de Rosati" de $M_2(\mathbf{H})$ associée à un élément symétrique ($\beta = {}^t\overline{\beta}$) est donnée par :

$$z \longrightarrow \beta {}^t\overline{z} \beta^{-1}.$$

Supposons choisi de plus un isomorphisme entre $\Delta \otimes \mathbf{R}$ et $M_2(\mathbf{R})$, de sorte que l'involution positive $*$ corresponde à la transposition $m \to {}^t m$. L'action de $\mathcal{O}_\Delta$ sur A définit un plongement $\iota : M_2(\mathbf{R}) \to M_2(\mathbf{H})$, lequel est conjugué par un certain $\alpha \in GL_2(\mathbf{H})$ au plongement évident $M_2(\mathbf{R}) \hookrightarrow M_2(\mathbf{H})$ (autrement dit : $\iota(m) = \alpha m \alpha^{-1}$).

La condition pour que l'involution associée à β, symétrique, induise sur Δ l'involution $*$ s'écrit alors :

$$\forall m \in M_2(\mathbf{R}) : \alpha {}^t m \alpha^{-1} = \beta {}^t\overline{(\alpha m \alpha^{-1})} \beta^{-1}$$

soit :

$$(\alpha^{-1} \beta {}^t\overline{\alpha}^{-1}) m ({}^t\overline{\alpha} \beta^{-1} \alpha) = m.$$

Elle est satisfaite si et seulement si β est de la forme :

$$\beta = \lambda \alpha {}^t\overline{\alpha} \ (\lambda \in \mathbf{R}^*).$$

De plus, β appartient au cône positif des polarisations si et seulement si $\lambda \in \mathbf{R}^{+*}$ (pour tout ceci, voir ([Mu 1], §21)), et le lemme en résulte.

4.2. *Le lemme suivant est crucial.*

LEMME (4.2). — *Soit X un groupe formel de dimension 2 et de hauteur 4 sur un anneau local artinien B de corps résiduel $\overline{\mathbf{F}}_p$. Supposons*

X muni d'une action ι de l'anneau $\mathcal{O}_\Delta \otimes \mathbb{Z}_p = \mathcal{O}_{\Delta_p}$, telle que la condition "spéciale" soit satisfaite. On considère alors l'ensemble des morphismes symétriques $X \xrightarrow{\lambda} X^*$ de X dans son dual de Cartier, qui sont compatibles à l'involution $*$, autrement dit tels que le diagramme analogue à celui de (1.5) commute (si l'on préfère : des polarisations formelles). Alors cet ensemble est un $\mathbb{Z}_p$-module libre de rang 1, dont les générateurs sont des isomorphismes $X \xrightarrow{\sim} X^*$.

Admettons provisoirement ce lemme et expliquons comment la proposition (3.3) en résulte.

(i) Dans le cas particulier de la base $S_0 = \mathrm{Spec}\,\overline{\mathbb{F}}_p$, le lemme (4.1) affirme l'existence d'une polarisation, qu'il s'agit d'"ajuster" pour la rendre principale. Comme dans le cas de la proposition (1.5), la possibilité d'effectuer cet ajustement se contrôle place par place : en $\ell \neq p$, on procède exactement comme dans le cas du corps $\mathbf{C}$, en faisant usage du lemme (1.6) ; tandis que, pour $\ell = p$, on remplace le lemme (1.6) par le lemme ci-dessus.

(ii) On passe ensuite au cas où la base S est le spectre d'un anneau artinien de corps résiduel $\overline{\mathbb{F}}_p$. La possibilité de déformer la $*$- polarisation principale qui existe au-dessus du point fermé de S résulte alors, en vertu du théorème de Serre et Tate, du lemme précédent. Par passage à la limite, cela règle aussi le cas où la base est le spectre d'un anneau local complet de corps résiduel $\overline{\mathbb{F}}_p$.

(iii) Le cas général se ramène aisément au cas où S est de type fini sur $\mathbb{Z}_p$. Il résulte alors de ce qui précède que le problème posé admet une solution unique au voisinage formel de chaque point géométrique algébrique. Utilisant l'unicité, on voit que ces solutions locales formelles sont algébriques et se recollent.

4.3. — Il nous reste à prouver le lemme (4.2). Drinfeld utilise ici une méthode très originale, dont le principe est de vérifier ce lemme dans le cas particulier d'un certain groupe formel $\Phi/\overline{\mathbb{F}}_p$, puis d'utiliser le théorème de représentabilité (chap. II, §8) pour le prouver en général.

Commençons par définir Φ : notons $\mathcal{E}$ "le" groupe formel sur $\overline{\mathbb{F}}_p$ de dimension 1 et de hauteur 2, et choisissons un isomorphisme $\mathrm{End}(\mathcal{E}) \simeq \mathcal{O}_{\Delta_p}$. On peut choisir une "polarisation formelle" $\mu_0 : \mathcal{E} \xrightarrow{\sim} \mathcal{E}^*$ (comme dans l'énoncé du lemme), et l'involution de Rosati associée s'identifie alors à l'involution canonique de Δ_p (pour fixer les idées, on pourra voir $\mathcal{E}$ comme le groupe formel d'une courbe elliptique supersingulière, et prendre la polarisation formelle associée à la polarisation principale de la courbe). On considère alors le produit $\Phi = \mathcal{E} \times \mathcal{E}$ de deux copies de $\mathcal{E}$, sur lequel

on fait agir $\mathcal{O}_{\Delta_p}$ de la façon suivante : un élément $u \in \mathcal{O}_{\Delta_p}$ agit (via l'isomorphisme $\mathcal{O}_{\Delta_p} \simeq \mathrm{End}(\mathcal{E})$) par u sur le premier facteur, et par tut^{-1} sur le second (rappelons que l'élément $t \in \Delta^*$ est une "uniformisante" de Δ_p). De cette façon, la condition "spéciale" est remplie : Φ est donc bien un $\mathcal{O}_{\Delta_p}$-module formel spécial, au sens du chapitre précédent (noter qu'ici les deux indices 0 et 1 sont critiques).

Vérifions que le lemme (4.2) est vrai pour Φ : utilisant les identifications ci-dessus entre $\mathcal{E}$ et $\mathcal{E}^*$, et entre $\mathcal{O}_{\Delta_p}$ et $\mathrm{End}(\mathcal{E})$, on voit que l'ensemble des polarisations formelles compatibles à l'involution $*$ s'identifie à l'ensemble des matrices :

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathcal{O}_{\Delta_p})$, qui sont à symétrie hermitienne :

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \overline{\alpha} & \overline{\gamma} \\ \overline{\beta} & \overline{\delta} \end{pmatrix}$, et qui vérifient, pour $u \in \mathcal{O}_{\Delta_p}$, la relation :

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} u^* & \\ & tu^*t^{-1} \end{pmatrix} = \begin{pmatrix} \overline{u} & \\ & \overline{tut}^{-1} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Utilisant les formules : $u^* = t^{-1}\overline{u}t = t\overline{u}t^{-1} = \overline{tut}^{-1}$, on voit que les conditions précédentes sont équivalentes à : $\alpha = \delta = 0$, $\beta = \gamma \in \mathbb{Z}_p$. L'ensemble cherché est donc bien un $\mathbb{Z}_p$-module libre de rang 1, engendré par exemple par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Noux *fixons* un tel générateur $\lambda_0 : \Phi \xrightarrow{\sim} \Phi^*$, c'est-à-dire une "$*$-polarisation formelle principale".

Remarque : on sait, d'après le chap.II,§5 que $\mathrm{End}^0_{\Delta_p}(\Phi)$ est isomorphe à $M_2(\mathbb{Q}_p)$. Cet isomorphisme peut ici se réaliser via le plongement de $M_2(\mathbb{Q}_p)$ dans $M_2(\Delta_p) = \mathrm{End}^0(\Phi)$ défini par : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \begin{pmatrix} a & bt \\ ct^{-1} & d \end{pmatrix}$. Un calcul immédiat montre alors que l'involution de Rosati associée à λ_0 induit sur $M_2(\mathbb{Q}_p)$ l'involution canonique de cette algèbre.

4.4. — Venons-en maintenant au cas général : en vertu de ce que l'on vient de voir, il suffit d'établir – utilisant les notations du lemme (4.2) – l'existence d'une $*$-polarisation formelle principale $\lambda : X \xrightarrow{\sim} X^*$. Elargissant quelque peu les hypothèses de ce lemme, donnons-nous une $\mathbb{Z}_p^{nr}$-algèbre B où l'image de p est nilpotente, ainsi qu'un groupe formel X, de dimension 2 et de hauteur 4 sur B, muni d'une action spéciale de l'anneau $\mathcal{O}_{\Delta_p}$. Supposons de plus donnée une quasi-isogénie ρ (compatible à l'action de $\mathcal{O}_{\Delta_p}$), de hauteur 0, de $\Phi_{B/pB}$ vers $X_{B/pB}$. Noter que ρ existe bien sous les hypothèses du lemme (4.2) : pour $B = \overline{\mathbb{F}}_p$ cela résulte du fait que tous les $\mathcal{O}_{\Delta_p}$-modules formels spéciaux sur $\overline{\mathbb{F}}_p$ sont isogènes à Φ

(chap. II, §5), et qu'on peut choisir (en composant avec un endomorphisme convenable de Φ) une quasi-isogénie de hauteur 0. Pour B artinien de corps résiduel $\overline{\mathbf{F}}_p$, cela en découle car on peut déformer les quasi-isogénies (voir par exemple [Zi 3] 5.31).

Le lemme résultera alors clairement de l'assertion plus précise suivante : *il existe un isomorphisme $\lambda : X \xrightarrow{\sim} X^*$ dont la restriction $\lambda_{B/pB}$ aux fibres spéciales fait commuter le diagramme :*

$$\begin{array}{ccc} X_{B/pB} & \xrightarrow{\lambda_{B/pB}} & X^*_{B/pB} \\ \uparrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho^*} \\ \Phi_{B/pB} & \xrightarrow{\lambda_0} & \Phi^*_{B/pB} \end{array}$$

(si un tel λ existe, il est unique, et symétrique (car λ_0 l'est) ; de même, il est nécessairement compatible à l'involution $*$).

On se souvient alors que, d'après les définitions du chap. II, §8, la donnée de la classe d'isomorphie du couple (X, ρ) revient à la donnée d'un point à valeurs dans B du foncteur $\overline{G}$ (lequel est représentable par le $\widehat{\mathbf{Z}}_p^{nr}$-schéma formel $\widehat{\Omega}\widehat{\otimes}\widehat{\mathbf{Z}}_p^{nr}$). L'assertion précédente revient à dire que les couples (X, ρ) et $(X^*, (\rho^*)^{-1} \circ \lambda_0)$ sont isomorphes. Or la formule :

$$j(X, \rho) = (X^*, (\rho^*)^{-1} \circ \lambda_0)$$

définit un automorphisme du foncteur $\overline{G}$. Pour vérifier en effet que X^* est spécial quand X l'est, on peut se placer sur un corps algébriquement clos k de caractéristique p, et on utilise le fait que la réduction modulo p du module de Dieudonné de X est une extension de $\mathrm{Lie}(X^*)$ par le dual de $\mathrm{Lie}(X)$; or on voit aisément que, dans l'action de $\mathbf{Z}_p^{(2)}$ sur le module de Dieudonné, chacun des deux plongements $\mathbf{Z}_p^{(2)} \hookrightarrow W(k)$ apparaît deux fois (on peut d'ailleurs vérifier cette dernière assertion sur Φ, car tous les $\mathcal{O}_{\Delta_p}$-modules formels spéciaux sur k sont isogènes).

On obtient ainsi un automorphisme, noté encore j, du $\widehat{\mathbf{Z}}_p^{nr}$-schéma formel $\widehat{\Omega}\widehat{\otimes}\widehat{\mathbf{Z}}_p^{nr}$. Pour prouver l'assertion précédente, et donc finalement le lemme (4.2), *il nous faut montrer que cet automorphisme est l'identité.*

4.5. — Or on constate que cet automorphisme – qui est d'ailleurs involutif – *commute à l'action naturelle de $SL(2, \mathbf{Q}_p)$* sur $\widehat{\Omega}\widehat{\otimes}\widehat{\mathbf{Z}}_p^{nr}$: en effet,

il résulte du chap. II §(9.3) que l'action d'un élément $g \in SL(2, \mathbb{Q}_p)$ sur le foncteur $\overline{G}$ est donnée par : $g(X, \rho) = (X, \rho \circ g^{-1})$. D'où :

$$j \circ g(X, \rho) = (X^*, ((\rho \circ g^{-1})^*)^{-1} \circ \lambda_0) = (X^*, (\rho^*)^{-1} \circ g^* \circ \lambda_0);$$
$$g \circ j(X, \rho) = (X^*, (\rho^*)^{-1} \circ \lambda_0 \circ g^{-1}).$$

La commutation résulte alors de la relation : $\lambda_0^{-1} g^* \lambda_0 = \overline{g} = g^{-1}$ pour $g \in SL(2, \mathbb{Q}_p)$ (voir la remarque de (4.3)).

Le lemme suivant nous permet de conclure :

LEMME (4.5). — *Un automorphisme j du $\widehat{\mathbb{Z}}_p^{nr}$-schéma formel $\widehat{\Omega} \widehat{\otimes} \widehat{\mathbb{Z}}_p^{nr}$, qui commute à l'action du groupe $SL(2, \mathbb{Q}_p)$, est nécessairement l'identité.*

En effet, j opère sur la fibre spéciale $\widehat{\Omega} \otimes \overline{\mathbb{F}}_p$, et donc aussi sur son "graphe dual", isomorphe à l'arbre de $PGL(2, \mathbb{Q}_p)$. Or c'est un exercice immédiat de vérifier qu'un automorphisme de l'arbre qui commute à l'action de $SL(2, \mathbb{Q}_p)$ est nécessairement l'identité : par suite, j stabilise chaque composante irréductible de la fibre spéciale, et fixe tous les points d'intersection de ces composantes. Or chacune de ces composantes est une droite projective, et porte $p+1 \geq 3$ points d'intersection avec ses voisines : d'où il résulte que j opère trivialement sur la fibre spéciale.

La "déviation" de j à l'identité sur le premier voisinage infinitésimal $\widehat{\Omega} \otimes (\mathbb{Z}_p^{nr}/(p^2))$ de la fibre spéciale est mesurée par une dérivation du faisceau structural de la fibre spéciale; cela équivaut à la donnée d'un champ de vecteurs tangents, s'annulant en chaque point singulier. Un tel champ est nécessairement nul, et donc j est l'identité sur le premier voisinage. De proche en proche sur les voisinages successifs, le même raisonnement prouve que j est bien l'identité.

Remarque : un résultat analogue à la proposition (3.3) est prouvé dans un cadre plus général dans [Zi 2]. La méthode utilisée par Zink est plus directe que celle que l'on vient d'exposer.

5. Le théorème de Čerednik-Drinfeld : énoncé, variantes, commentaires.

5.1. — Nous nous plaçons toujours dans le cas où notre sous-groupe compact ouvert U est de la forme $U_p^0 U^p$, avec U^p un sous-groupe compact ouvert de $\Delta^*(\mathbb{A}_f^p)$. Pour U^p de plus en plus petit, les courbes $\mathbf{S}_U$ correspondantes constituent un système projectif (muni d'une action du groupe $\Delta^*(\mathbb{A}_f^p)$).

Nous notons d'autre part $\overline{\Delta}^*$ le groupe réductif sur $\mathbb{Q}$ défini – de la même façon que Δ^* l'était à partir de Δ – comme le groupe multiplicatif

de l'algèbre $\overline{\Delta}$ considérée au §2. Nous fixons par la suite un isomorphisme entre les groupes :

$$\Delta^*(\mathbb{A}_f^p) = (\Delta \otimes \mathbb{A}_f^p)^* \text{ et } \overline{\Delta}^*(\mathbb{A}_f^p) = (\overline{\Delta} \otimes \mathbb{A}_f^p)^*,$$

obtenu à partir d'un *anti-isomorphisme* entre les algèbres $\Delta \otimes \mathbb{A}_f^p$ et $\overline{\Delta} \otimes \mathbb{A}_f^p$ (en composant avec l'inversion $g \to g^{-1}$). Via cet isomorphisme, le groupe U^p pourra donc être considéré comme un sous-groupe de $\overline{\Delta}^*(\mathbb{A}_f^p)$.

Nous fixons également un isomorphisme $\overline{\Delta}^*(\mathbb{Q}_p) \simeq GL(2, \mathbb{Q}_p)$ obtenu cette fois à partir d'un isomorphisme entre $\overline{\Delta} \otimes \mathbb{Q}_p$ et $M_2(\mathbb{Q}_p)$.

Considérons d'autre part l'ensemble suivant de doubles classes, noté Z_U ou Z_{U^p} :

$$Z_U = U^p \backslash \overline{\Delta}^*(\mathbb{A}_f) / \overline{\Delta}^*(\mathbb{Q}).$$

Cet ensemble est muni d'une action à gauche évidente du groupe $\overline{\Delta}^*(\mathbb{Q}_p)$, et le quotient par cette action est fini. Toute orbite contient la double classe d'un élément x dont la p-composante x_p est égale à 1. Le stabilisateur Γ_x de x est alors donné par :

$$\Gamma_x = \overline{\Delta}^*(\mathbb{Q}) \cap x^{-1} U^p x,$$

où l'intersection est prise dans $\overline{\Delta}^*(\mathbb{A}_f^p)$ puis, vue comme sous-groupe de $\overline{\Delta}^*(\mathbb{Q})$, injectée dans $\overline{\Delta}^*(\mathbb{Q}_p) \simeq GL(2, \mathbb{Q}_p)$. On vérifie sans mal que ces stabilisateurs sont des sous-groupes discrets et co-compacts dans $\overline{\Delta}^*(\mathbb{Q}_p)$, et qu'ils contiennent une puissance positive de la matrice $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$.

Pour U^p de plus en plus petit, ces ensembles Z_U constituent un système projectif où opère le groupe $\overline{\Delta}^*(\mathbb{A}_f^p)$.

5.2. *Le théorème de Čerednik-Drinfeld.*

Conservons les notations et les conventions précédentes, en particulier les isomorphismes :

$$\Delta^*(\mathbb{A}_f^p) \simeq \overline{\Delta}^*(\mathbb{A}_f^p), \quad \overline{\Delta}^*(\mathbb{Q}_p) \simeq GL(2, \mathbb{Q}_p).$$

THÉORÈME (5.2). — *Pour chaque sous-groupe compact ouvert assez petit $U^p \subset \Delta^*(\mathbb{A}_f^p)$, on a (posant $U = U_p^0 U^p$) un isomorphisme de $\mathbb{Z}_p$-schémas formels :*

$$\widehat{\mathbf{S}}_U \simeq GL(2, \mathbb{Q}_p) \backslash [(\widehat{\Omega} \widehat{\otimes} \widehat{\mathbb{Z}}_p^{nr}) \times Z_U]$$

où $\widehat{\mathbf{S}}_U$ désigne le complété formel de $\mathbf{S}_U$ le long de sa fibre spéciale. Ces isomorphismes sont compatibles, lorsque U^p varie, avec les opérations de projection. L'isomorphisme des deux systèmes projectifs ainsi obtenu est compatible à l'action sur les deux membres du groupe $\Delta^*(\mathbb{A}_f^p) \simeq \overline{\Delta}^*(\mathbb{A}_f^p)$. Enfin, ces isomorphismes se relèvent en des isomorphismes entre les $\mathcal{O}_{\Delta_p}$-modules formels spéciaux naturellement portés par les deux membres.

L'énoncé qui précède appelle un certain nombre de commentaires : nous allons commencer par quelques rappels et précisions peut-être nécessaires à sa compréhension formelle ; puis, nous expliquerons pourquoi le quotient qui figure, avec une apparence un peu monstrueuse, dans l'énoncé de ce théorème, n'est rien d'autre qu'une réunion finie de formes tordues de courbes de Mumford. Nous dirons ensuite comment calculer le graphe des composantes irréductibles de la fibre spéciale. Nous généraliserons finalement le théorème au cas des sous-groupes de la forme $U = U_p^n U^p$.

Commençons par quelques éclaircissements sur l'énoncé qui précède :

a) Rappelons que l'action de $GL(2, \mathbb{Q}_p)$ sur $\widehat{\Omega}\widehat{\otimes}\widehat{\mathbb{Z}}_p^{nr}$ que nous considérons est obtenue à partir de l'action naturelle sur $\widehat{\Omega}$ et de l'action $g \to \widetilde{Fr}^{-v(\det g)}$ sur $\widehat{\mathbb{Z}}_p^{nr}$ (*cf.* chap. II, §9). Cette action est définie seulement au-dessus de $\mathbb{Z}_p$ et non pas de $\mathbb{Z}_p^{nr}$.

b) L'action naturelle du groupe $\Delta^*(\mathbb{A}_f^p)$ sur le système projectif des $\mathbf{S}_U$ est une action à droite, tandis que celle du groupe $\overline{\Delta}^*(\mathbb{A}_f^p)$ sur le système des Z_U est une action à gauche. Pour pouvoir les comparer, il faut donc changer le sens d'une de ces actions : on le fait à l'aide de l'anti-isomorphisme entre les deux groupes associé à l'anti-isomorphisme choisi entre les deux algèbres.

c) Le $\mathcal{O}_{\Delta_p}$-module formel porté par $\widehat{\mathbf{S}}_U$ est le complété formel de la variété abélienne universelle donnée par le problème de modules $\mathbf{M}_U$. Celui porté par le membre de droite provient de la description modulaire de $\widehat{\Omega}\widehat{\otimes}\widehat{\mathbb{Z}}_p^{nr}$ (chap. II, §8).

5.3. *Commentaires (suite).*

5.3.1. — Parce que l'action de $\overline{\Delta}^*(\mathbb{Q}_p) \simeq GL(2, \mathbb{Q}_p)$ sur Z_U décompose ce dernier ensemble en un nombre fini d'orbites, on voit que le quotient qui figure dans l'énoncé du théorème apparaît comme la réunion d'un nombre fini de quotients de la forme :

$$\Gamma_i \backslash \widehat{\Omega}\widehat{\otimes}\widehat{\mathbb{Z}}_p^{nr},$$

où les $\Gamma_i = \Gamma_{x_i}$ sont les différents stabilisateurs, décrits en (5.1). Comme chacun de ces stabilisateurs contient une puissance $p^{n_i} \cdot \mathbf{1}$ de $p \cdot \mathbf{1}$, on

peut commencer par passer au quotient par l'action de $p^{n_i} \cdot \mathbf{1}$ (qui agit trivialement sur $\widehat{\Omega}$), obtenant ainsi le produit tensoriel de $\widehat{\Omega}$ par l'extension non ramifiée de degré $2n_i$, notée $\mathbf{Z}_p^{(2n_i)}$, de $\mathbf{Z}_p$. Le quotient ci-dessus peut encore s'écrire :

$$\Gamma_i \backslash \widehat{\Omega} \widehat{\otimes} \mathbf{Z}_p^{(2n_i)}.$$

Après extension des scalaires à $\mathbf{Z}_p^{(2n_i)}$, cela devient isomorphe à une réunion finie de quotients "à la Mumford", de la forme $\Gamma_i' \backslash \widehat{\Omega}$ (*cf.* [Mu 2] ou [Ra 2]), où Γ_i' désigne l'image dans le groupe $PGL(2, \mathbf{Q}_p)$ du sous-groupe de Γ_i constitué des éléments dont le déterminant est une unité. Sous l'hypothèse que U^p est assez petit (il suffit par exemple que la même condition qu'en (1.3) soit remplie), on voit que ces groupes Γ_i' sont des sous-groupes de Schottky de $PGL(2, \mathbf{Q}_p)$ – en particulier, ils opèrent librement sur l'arbre I et sur $\widehat{\Omega}$. Si on suppose même que U^p est suffisamment petit pour que les Γ_i' opèrent très librement sur I (tout sommet étant expédié, par tout élément $\neq 1$, à une distance ≥ 2), alors les quotients à la Mumford qui interviennent s'obtiennent simplement par un recollement des ouverts affines standard, indexés par les sommets de l'arbre, qu'on a décrits au chapitre I.

Pour nous résumer, on voit donc que le quotient qui figure dans l'énoncé du théorème est la réunion de formes tordues galoisiennes (sur des extensions non ramifiées) de quotients à la Mumford.

5.3.2. — *Le théorème (5.2) garde un sens partiel même sans l'hypothèse "U^p assez petit"* : il existe en effet dans tous les cas un sous-groupe distingué d'indice fini $U_1^p \subset U^p$ qui est assez petit. Appliquant le théorème au groupe U_1^p, puis passant au quotient par le groupe fini U^p/U_1^p, on obtient un isomorphisme analogue :

$$\widehat{\mathbf{S}}_U \simeq GL(2, \mathbf{Q}_p) \backslash [(\widehat{\Omega} \widehat{\otimes} \widehat{\mathbf{Z}}_p^{nr}) \times Z_U]$$

où $\mathbf{S}_U$ est le quotient $\mathbf{S}_{U_1}/(U/U_1)$, tandis que le membre de droite apparaît comme la réunion de formes tordues de quotients de courbes de Mumford par des groupes finis. Autrement dit, le membre de droite est toujours isomorphe au complété formel d'un modèle entier de S_U. On prendra garde toutefois que, sans l'hypothèse que U^p est assez petit, aucun des deux membres de la formule ne porte naturellement un $\mathcal{O}_{\Delta_p}$-module formel.

Remarquons enfin que, dans tous les cas, l'isomorphisme du théorème peut s'exprimer comme une uniformisation p-adique :

$$S_U^{an} \simeq GL(2, \mathbf{Q}_p) \backslash [(\Omega \widehat{\otimes} \widehat{\mathbf{Q}}_p^{nr}) \times Z_U]$$

(où S_U^{an} désigne l'espace rigide-analytique sur $\mathbb{Q}_p$ sous-jacent à S_U). On voit d'ailleurs sans peine qu'il n'est pas nécessaire de compléter (i.e. écrire seulement $\otimes \mathbb{Q}_p^{nr}$ dans la formule ci-dessus).

5.3.3. — Il est un cas particulier où le quotient ci-dessus prend une forme plus simple; parce que ce cas – étudié dans [Jo-Li] – est celui qui intervient dans le travail de Ribet ([Ri 2]), nous allons en dire quelques mots. On suppose ici que sont remplies les hypothèses suivantes sur le groupe U^p (dont on ne suppose plus qu'il est "assez petit") :

a) L'image de U^p par la norme réduite est maximale, i.e. égale à $\prod_{\ell \neq p} \mathbb{Z}_\ell^*$.

b) La valuation p-adique envoie surjectivement sur $\mathbb{Z}$ l'intersection de U^p et du centre $\mathbb{Q}^*$ de $\Delta^*(\mathbb{Q})$.

Sous l'hypothèse a), il est facile de voir, en utilisant le théorème d'approximation forte, que $\overline{\Delta}^*(\mathbb{Q}_p)$ opère transitivement sur Z_U. Le quotient qui nous intéresse prend donc la forme :

$\Gamma \backslash \widehat{\Omega} \widehat{\otimes} \widehat{\mathbb{Z}}_p^{nr}$, avec $\Gamma = \overline{\Delta}^*(\mathbb{Q}) \cap U^p$ (vu comme sous-groupe de $\overline{\Delta}^*(\mathbb{Q}_p) \simeq GL(2, \mathbb{Q}_p)$). D'autre part, en vertu de la seconde hypothèse, le quotient de $\mathrm{Spf}\mathbb{Z}_p^{nr}$ par l'intersection $\Gamma \cap \mathbb{Q}^*$ s'identifie à $\mathrm{Spf}\mathbb{Z}_p^{(2)}$.

Notons Γ_+ le sous-groupe de Γ constitué des éléments dont la valuation en p de la norme réduite est paire : on vérifie que Γ_+ est d'indice 2 dans Γ. Notant $W = \Gamma/\Gamma_+$ (un groupe à deux éléments), on voit que le quotient ci-dessus peut encore s'écrire :

$$W \backslash [(\Gamma_+ \backslash \widehat{\Omega}) \otimes \mathbb{Z}_p^{(2)}].$$

Autrement dit, on obtient une forme tordue du quotient $\Gamma_+ \backslash \widehat{\Omega}$ (lequel est le quotient par un groupe fini d'une courbe de Mumford). Le cocycle qui décrit la torsion dans $H^1(\mathrm{Gal}(\mathbb{Q}_p^{(2)}/\mathbb{Q}_p), \mathrm{Aut}(\Gamma_+ \backslash \widehat{\Omega}))$ envoie l'élément non trivial du groupe de Galois sur l'automorphisme de $\Gamma_+ \backslash \widehat{\Omega}$ défini par un quelconque $w \in \Gamma - \Gamma_+$. Tout cela peut d'ailleurs aussi bien s'exprimer en langage adélique : notre quotient prend alors la forme

$$W \backslash [\overline{\Delta}^*(\mathbb{Q}_p)_+ \backslash \widehat{\Omega} \times Z_U] \otimes \mathbb{Z}_p^{(2)},$$

où $\overline{\Delta}^*(\mathbb{Q}_p)_+$ est le sous-groupe de $\overline{\Delta}^*(\mathbb{Q}_p)$ constitué des éléments dont la valuation du déterminant est paire, et où W (isomorphe à $\mathbb{Z}/2\mathbb{Z}$) désigne le quotient $\overline{\Delta}^*(\mathbb{Q}_p)/\overline{\Delta}^*(\mathbb{Q}_p)_+$. On obtient ainsi la forme tordue du quotient

$$\overline{\Delta}^*(\mathbb{Q}_p)_+ \backslash \widehat{\Omega} \times Z_U$$

où l'automorphisme qui décrit la torsion est celui défini par n'importe quel élément $w \in \overline{\Delta}^*(\mathbb{Q}_p) - \overline{\Delta}^*(\mathbb{Q}_p)_+$.

5.4. *Graphes.*

5.4.1. — On sait – voir le chap. I – que le "graphe dual" de la fibre spéciale de $\widehat{\Omega}$ s'identifie à l'arbre I de $PGL(2, \mathbb{Q}_p)$. Si l'on considère un quotient à la Mumford $\Gamma\backslash\widehat{\Omega}$, donc tel que l'image $\overline{\Gamma}$ de Γ dans le groupe projectif opère librement sur I, alors il est bien connu, et facile de voir, que le graphe de la fibre spéciale de $\Gamma\backslash\widehat{\Omega}$ s'identifie au graphe quotient $\Gamma\backslash I$. Kurihara ([Ku], voir aussi [Jo-Li]) a expliqué comment obtenir un résultat analogue dans la situation un peu plus générale (comme en (5.3.2)) d'un sous-groupe $\overline{\Gamma}$, discret et co-compact dans $PGL(2, \mathbb{Q}_p)$, qui n'est pas nécessairement de Schottky (mais un sous-groupe d'indice fini dans $\overline{\Gamma}$ l'est toujours). Nous allons ci-dessous rappeler les résultats de Kurihara.

5.4.2. — Soit R un anneau de valuation discrète, de corps résiduel κ, dont on note ϖ une uniformisante. Suivant une terminologie due à Jordan et Livné, nous dirons qu'un schéma en courbes $\mathcal{C}/\mathrm{Spec}(R)$ est *admissible* s'il vérifie les conditions suivantes :

a) $\mathcal{C}$ est propre et plat sur $\mathrm{Spec}(R)$, de fibre générique lisse.

b) La fibre spéciale $\mathcal{C}_\kappa$ est réduite; ses singularités sont des points doubles ordinaires, rationnels sur κ ainsi que les branches qui en sont issues. Les normalisées des composantes irréductibles de $\mathcal{C}_\kappa$ sont des courbes rationnelles.

c) Pour tout point singulier $x \in \mathcal{C}_\kappa$, il existe un entier m tel que le complété $\widehat{\mathcal{O}}_{\mathcal{C},\kappa}$ de l'anneau local en x soit R-isomorphe au complété de l'anneau local $R[[X,Y]]/(XY - \varpi^m)$; il est facile de voir que m est bien déterminé par x.

A une telle courbe admissible, on associe un *graphe* de la façon suivante : les sommets du graphe sont les composantes irréductibles de $\mathcal{C}_\kappa$; ses arêtes sont les branches issues des différents points doubles; l'inverse d'une arête a est l'autre branche $\overline{a}$ issue du même point singulier. Enfin, l'origine de a est la composante qui contient a, tandis que son extrémité est l'origine de $\overline{a}$. On obtient bien ainsi une structure de graphe au sens de Serre ([Se]). Ce graphe admet ici une structure supplémentaire, à savoir une application m de l'ensemble des arêtes dans l'ensemble des entiers ≥ 1 : c'est simplement l'application qui envoie une arête a sur l'entier $m = m(a)$ associé, par la condition c) ci-dessus, au point singulier correspondant. On appelle *longueur* d'une arête a cet entier $m(a)$, qui vérifie : $m(\overline{a}) = m(a)$. Nous obtenons ainsi sur le *graphe dual* de la fibre spéciale une structure

supplémentaire, c'est ce que Kurihara appelle *un graphe avec longueurs.*

5.4.3. — Définissons maintenant une structure quotient de ce type, associée à un sous-groupe $\overline{\Gamma} \subset PGL(2, \mathbb{Q}_p)$, discret et co-compact, opérant sur l'arbre I : l'idée naturelle est de considérer l'objet combinatoire $\overline{\Gamma}\backslash I$ dont l'ensemble de sommets (resp. d'arêtes) est le quotient par $\overline{\Gamma}$ de l'ensemble de sommets (resp. d'arêtes) de I, avec les relations d'incidence et d'inversion évidentes. Toutefois, on n'obtient pas toujours ainsi un graphe au sens de Serre, dans la mesure où, s'il existe dans $\overline{\Gamma}$ un élément qui transforme une arête en son inverse, le quotient contient une arête égale à son inverse. *On note* $(\overline{\Gamma}\backslash I)^*$ *le graphe obtenu en ôtant de* $(\overline{\Gamma}\backslash I)$ *les arêtes qui sont leurs propres inverses* (noter que cela n'empêche pas $(\overline{\Gamma}\backslash I)^*$ de contenir éventuellement des lacets).

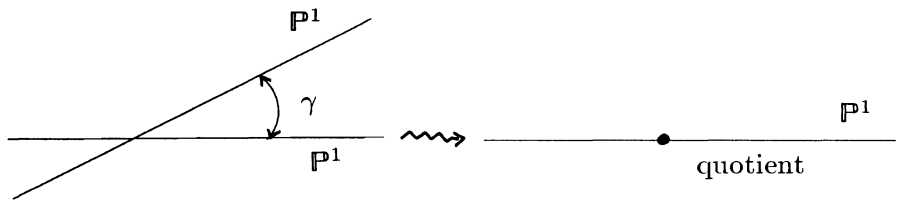
On définit ensuite la longueur $m(a)$ d'une arête a de $(\overline{\Gamma}\backslash I)^*$: c'est l'ordre du stabilisateur $\overline{\Gamma}_{\tilde{a}}$ d'un quelconque relèvement $\tilde{a}$ de a en une arête de I.

Nous sommes maintenant en mesure d'énoncer le résultat de Kurihara : soit donc comme ci-dessus $\overline{\Gamma} \subset PGL(2, \mathbb{Q}_p)$ un sous-groupe discret co-compact, et $(\overline{\Gamma}\backslash\widehat{\Omega})$ la courbe associée (quotient par un groupe fini d'une courbe de Mumford).

THÉORÈME [KURIHARA]. — *La courbe* $(\overline{\Gamma}\backslash\widehat{\Omega})$ *est une courbe admissible sur* $\mathbb{Z}_p$. *Le graphe dual "avec longueurs" associé coïncide avec le quotient* $(\overline{\Gamma}\backslash I)^*$ *défini ci-dessus*

Pour la démonstration, nous renvoyons à l'article de Kurihara, où on explique aussi comment obtenir le graphe dual d'un modèle régulier de la courbe (voir aussi [Jo-Li]). Bornons-nous à illustrer ce résultat, en expliquant de façon intuitive pourquoi il est nécessaire d'ôter de $(\overline{\Gamma}\backslash I)$ les arêtes qui sont leur propre inverse, et pourquoi la "longueur" est donnée par l'ordre du stabilisateur :

a) S'il existe une inversion $\gamma \in \overline{\Gamma}$ qui échange deux sommets voisins de l'arbre, alors le passage au quotient "replie l'une sur l'autre" deux composantes de la fibre spéciale de $\widehat{\Omega}$:



On voit donc que la singularité disparaît dans le quotient.

b) Un exemple de stabilisateur opérant sur la singularité d'équation $XY = p$ est celui d'un groupe cyclique d'ordre m, un générateur de ce groupe opérant par :

$$\begin{cases} X & \longrightarrow & \zeta X \\ Y & \longrightarrow & \zeta^{-1} Y \end{cases},$$

où ζ est une racine primitive $m^{\text{ième}}$de 1.

Alors on voit que le quotient est la singularité d'équation $X'Y' = p^m$, la projection étant donnée par : $X' = X^m, Y' = Y^m$.

5.4.4. Appliquons ce qui précède à une courbe S_U associée à un sous-groupe U vérifiant les hypothèses simplificatrices de (5.3.3), dont on conserve les notations. On obtient un modèle entier (défini sur $\mathbb{Z}_p$) de la courbe, et ce modèle est admissible après extension des scalaires à $\mathbb{Z}_p^{(2)}$. Le graphe "avec longueurs" associé à la fibre spéciale est alors égal à $(\overline{\Gamma}_+\backslash I)^*$. Que l'on ait affaire à une forme tordue du quotient $(\overline{\Gamma}_+\backslash\widehat{\Omega})$ se traduit par une action non triviale sur le graphe de l'automorphisme de Frobenius Frob_p : cette action sur $(\overline{\Gamma}_+\backslash I)^*$ est celle définie par un quelconque élément $w \in \Gamma - \Gamma_+$. Si l'on préfère une expression adélique, le graphe ci-dessus peut encore s'écrire :

$$[\overline{\Delta}^*(\mathbb{Q}_p)_+\backslash(I \times Z_U)]^*,$$

l'action de Frobenius étant celle définie par un élément $w \in \overline{\Delta}^*(\mathbb{Q}_p) - \overline{\Delta}^*(\mathbb{Q}_p)_+$.

5.5. *Généralisation au cas où U_p n'est pas maximal.*

5.5.1. — Un des avantages de l'approche de Drinfeld est qu'elle permet également d'uniformiser p-adiquement les courbes S_U, pour U de la forme $U_p^n U^p$ (*cf.* (0.2)), en termes des revêtements Σ_n de $\Omega\widehat{\otimes}\widehat{K}^{nr}$ définis au chap. II §13.

THÉORÈME (5.5). — *Pour U de la forme $U_p^n U^p$, il existe un isomorphisme d'espaces rigides-analytiques :*

$$S_U^{an} \simeq GL(2, \mathbb{Q}_p)\backslash[\Sigma_n \times Z_{U^p}].$$

Ces isomorphismes sont compatibles, lorsque U et n varient, aux opérations de projection, et l'isomorphisme ainsi obtenu entre les deux systèmes projectifs est équivariant par l'action du groupe $\Delta^*(\mathbb{A}_f)$.

Remarque 1 : Comme plus haut, on voit que le membre de droite de la formule est une réunion finie de quotients $\Gamma_i\backslash\Sigma_n$, pour des sous-groupes

de congruence $\Gamma_i \subset GL(2, \mathbb{Q}_p)$. On s'aperçoit facilement, de même, qu'il ne change rien de considérer Σ_n comme le revêtement de $\Omega \widehat{\otimes} \widehat{K}^{nr}$ ou bien de $\Omega \otimes K^{nr}$ (*cf.* II,13.3, Rem. (a)).

Remarque 2 : Dans l'article [Ca 2], on indique comment utiliser le théorème (5.5) pour calculer la cohomologie rigide – analytique des espaces Σ_n.

5.5.2. — Expliquons maintenant comment le th. (5.5) se déduit du th. (5.2). On peut évidemment se ramener à supposer que U^p est assez petit. Notant $U_0 = U_p^0 \times U^p$, le problème de modules $\mathbf{M}_{U_0}$ définit sur le $\mathbb{Z}_p$-schéma $\mathbf{S}_{U_0}$ une variété abélienne "universelle" $\mathbf{A}$. Alors S_U (qui n'existe qu'en caractéristique 0), vu comme S_{U_0}-schéma, classifie les isomorphismes $\mathcal{O}_\Delta$-linéaires $\overline{\nu}$ entre la p^n-torsion A_{p^n} de la fibre générale A de $\mathbf{A}$, et $\mathcal{O}_\Delta \otimes (\mathbb{Z}/p^n\mathbb{Z})$. La donnée d'un tel isomorphisme revient plus simplement à la donnée d'un point exactement d'ordre p^n dans A_{p^n}.

Utilisant les notations et définitions du chap. II, §13, on a, d'après la dernière assertion du th. (5.2), un isomorphisme de $\mathcal{O}_{\Delta_p}$-modules formels sur $\widehat{\mathbf{S}}_{U_0}$:

$$\widehat{\mathbf{A}} \simeq GL(2, \mathbb{Q}_p) \backslash [X \times Z_{U^p}],$$

et donc :

$$\widehat{\mathbf{A}}_{p^n} \simeq GL(2, \mathbb{Q}_p) \backslash [X_n \times Z_{U^p}].$$

D'où un isomorphisme au-dessus de $S_{U_0}^{an}$:

$$\widehat{\mathbf{A}}_{p^n}^{an} \simeq GL(2, \mathbb{Q}_p) \backslash [\mathcal{X}_n \times Z_{U^p}].$$

Finalement, on a donc bien :

$$S_U^{an} \simeq GL(2, \mathbb{Q}_p) \backslash [\Sigma_n \times Z_{U^p}].$$

5.6. — Pour terminer ces commentaires du théorème (5.2) signalons l'article [Ri 1] où est donnée une description plus canonique de l'ensemble des composantes et des points sur $\overline{\mathbb{F}}_p$ de la courbe $\mathbf{S}_U$: on y explique en particulier comment l'ensemble des composantes irréductibles est paramètré par l'ensemble des $\mathcal{O}_\Delta$-variétés abéliennes de dimension 2 sur $\overline{\mathbb{F}}_p$, munies de structures de niveau U^p, et qui *ne vérifient pas la condition "spéciale"*.

6. Preuve du théorème de Čerednik-Drinfeld.

6.1. — Nous commençons par fixer une variété abélienne A_0 sur $\overline{\mathbb{F}}_p$, de dimension 2, munie d'une action "spéciale" de l'anneau $\mathcal{O}_\Delta$ (pour voir

que A_0 existe, on peut prendre la variété abélienne associée à un point sur $\overline{\mathbf{F}}_p$ de $\mathbf{S}_U$; ou bien la construire explicitement, partant du produit de deux courbes elliptiques supersingulières, et définir l'action de façon analogue à ce que nous avions fait en (4.3) pour exhiber un $\mathcal{O}_{\Delta_p}$-module formel spécial). Notons Φ le groupe formel associé, qui est donc un $\mathcal{O}_{\Delta_p}$-module formel spécial. Nous choisissons d'autre part une identification (*cf.* §2) : $\overline{\Delta} = \mathrm{End}^0_{\Delta}(A_0)$ (et donc : $\overline{\Delta}^*(\mathbf{Q}) = \overline{\Delta}^* = \mathrm{Aut}^0_{\Delta}(A_0)$).

Cela induit une identification :

$$\overline{\Delta}_p = \overline{\Delta} \otimes \mathbf{Q}_p = M(2, \mathbf{Q}_p) = \mathrm{End}^0_{\Delta_p}(\Phi)$$

$$(\text{d'où : } \overline{\Delta}^*(\mathbf{Q}_p) = \overline{\Delta}_p^* = GL(2, \mathbf{Q}_p) = \mathrm{Aut}^0_{\Delta_p}(\Phi)).$$

Nous fixons enfin des isomorphismes, pour $\ell \neq p$:

$$\nu_{0,\ell} : V_\ell(A_0) \xrightarrow{\sim} V_\ell,$$

compatibles (au sens de la remarque finale du §2) à l'isomorphisme fixé entre $\Delta \otimes \mathbf{A}_f^p$ et $(\overline{\Delta} \otimes \mathbf{A}_f^p)^{opp}$: cela signifie que, via $\nu_{0,\ell}$, l'action de $\overline{\Delta} = \mathrm{End}^0_{\Delta}(A_0)$ sur V_ℓ est donnée par le composé :

$$\overline{\Delta} \hookrightarrow \overline{\Delta}_\ell \simeq \Delta_\ell^{opp} \longrightarrow \mathrm{End}_{\Delta_\ell}(V_\ell)$$

[action par multiplication à droite].

6.2. *Algébrisations.*

6.2.1. — Soit S un $\mathbf{Z}_p$-schéma où l'image de p est nilpotente, et X un $\mathcal{O}_{\Delta_p}$-module formel spécial sur S.

DÉFINITION. — *Une algébrisation de X est la donnée d'un couple (A, ε) constitué d'un schéma abélien A sur S, muni d'une action de $\mathcal{O}_\Delta$, et d'un isomorphisme $\mathcal{O}_\Delta$-équivariant ε : $\widehat{A} \xrightarrow{\sim} X$ entre X et le groupe formel associé à A. Lorsque A est de plus muni d'une structure de niveau U (ou U^p, cela revient au même), on parle d'algébrisation avec structure de niveau U.*

(On notera que l'action de $\mathcal{O}_\Delta$ sur A est alors spéciale).

6.2.2. — En particulier, on note $\mathcal{A}\ell g_U(\Phi)$ l'ensemble des classes d'isomorphie d'algébrisations, avec structure de niveau U, de Φ. Il est fondamental pour la suite de déterminer cet ensemble : c'est donc l'ensemble des classes d'isomorphie de triplets $(A, \varepsilon, \overline{\nu})$ où A est une $\mathcal{O}_\Delta$-variété abélienne

sur $\overline{\mathbf{F}}_p$, où ε est un isomorphisme équivariant entre $\widehat{A}$ et Φ, et $\overline{\nu}$ une classe modulo U^p d'isomorphismes $\mathcal{O}_\Delta$-linéaires :

$$\nu : \prod_{\ell \neq p} T_\ell(A) \xrightarrow{\sim} \prod_{\ell \neq p} W_\ell.$$

Le yoga habituel (voir par exemple [Mi]) permet de voir encore cet ensemble comme l'ensemble des classes d'isogénie de triplets $(A, \varepsilon, \overline{\nu})$ où A est une variété abélienne, munie d'une action à isogénie près de Δ, où ε est une *quasi-isogénie* (équivariante) entre $\widehat{A}$ et Φ, et où enfin $\overline{\nu}$ est une classe modulo U^p d'isomorphismes Δ-linéaires :

$$\nu : \prod_{\ell \neq p} V_\ell(A) \xrightarrow{\sim} \prod_{\ell \neq p} V_\ell.$$

La limite projective $\mathcal{A}\ell g_\infty(\Phi)$ des $\mathcal{A}\ell g_U(\Phi)$ est l'ensemble des tels triplets (A, ε, ν) ; cette description met en évidence une action à gauche sur $\mathcal{A}\ell g_\infty(\Phi)$ du groupe $\overline{\Delta}^*(\mathbf{A}_f) = \overline{\Delta}^*(\mathbf{Q}_p) \times \overline{\Delta}^*(\mathbf{A}_f^p)$, telle que la composante suivant $\overline{\Delta}^*(\mathbf{Q}_p)$ agisse par composition sur ε, et celle suivant $\overline{\Delta}^*(\mathbf{A}_f^p)$ par composition sur ν. Cette action est *transitive*, ainsi qu'il résulte de l'unicité de la classe d'isogénie de A (§2).

Utilisant les identifications de (6.1), on considère l'élément de $\mathcal{A}\ell g_\infty(\Phi)$ donné par le triplet :

$$A_0 \ , \ \varepsilon_0 : \widehat{A}_0 = \Phi \ , \ \prod \nu_{0,\ell}.$$

On voit alors que le *stabilisateur* de cet élément est le sous-groupe $\overline{\Delta}^*(\mathbf{Q}) \subset \overline{\Delta}^*(\mathbf{A}_f)$. Cela ressort de la commutativité des diagrammes ci-dessous, où γ désigne un élément de $\overline{\Delta}^*(\mathbf{Q})$, et γ_ℓ ses images dans les $\overline{\Delta}^*(\mathbf{Q}_\ell)$:

$$\begin{array}{ccccccc}
A_0 & \widehat{A}_0 & = & \Phi & V_\ell(A_0) & \xrightarrow[\nu_{0,\ell}]{\sim} & V_\ell \\
\downarrow{\scriptstyle \gamma} & \downarrow{\scriptstyle \widehat{\gamma}} & & \downarrow{\scriptstyle \gamma_p} & \downarrow{\scriptstyle V_\ell(\gamma)} & & \downarrow{\scriptstyle \gamma_\ell} \\
A_0 & \widehat{A}_0 & = & \Phi & V_\ell(A_0) & \xrightarrow[\nu_{0,\ell}]{\sim} & V_\ell
\end{array}$$

6.2.3. — On en déduit une bijection entre $\mathcal{A}\ell g_\infty(\Phi)$ et l'espace homogène $\overline{\Delta}^*(\mathbf{A}_f)/\overline{\Delta}^*(\mathbf{Q})$. D'où il résulte une bijection :

$$\mathcal{A}\ell g_U(\Phi) \simeq U^p \backslash \overline{\Delta}^*(\mathbf{A}_f)/\overline{\Delta}^*(\mathbf{Q}) = Z_U.$$

6.3. — L'étape suivante consiste à définir un *morphisme* Θ *de la fibre spéciale* $[(\widehat{\Omega}\widehat{\otimes}\widehat{\mathbf{Z}}_p^{nr})\otimes\mathbf{F}_p]\times Z_U = (\widehat{\Omega}\otimes\overline{\mathbf{F}}_p)\times Z_U$ vers la fibre spéciale $\mathbf{S}_U\otimes\mathbf{F}_p$.

6.3.1. — Soit S un schéma de caractéristique p. Si A_1 et A_2 sont deux schémas abéliens sur S, nous appellerons "*p-quasi-isogénie*" une quasi-isogénie $g : A_1 \to A_2$ telle que le produit de g par une puissance assez grande de p soit une isogénie d'ordre une puissance de p. Une telle quasi-isogénie induit, pour tout $\ell \neq p$, un isomorphisme entre $T_\ell(A_1)$ et $T_\ell(A_2)$.

Nous allons utiliser le lemme suivant :

LEMME. — *Soient* X_1 *et* X_2 *deux* $\mathcal{O}_{\Delta_p}$*-modules formels spéciaux sur* S, *et* $f : X_1 \to X_2$ *une quasi-isogénie. Soit d'autre part* (A_1, ε_1) *une algébrisation de* X_1. *Il existe alors une algébrisation* (A_2, ε_2) *de* X_2, *et une p-quasi-isogénie* $h : A_1 \to A_2$, *telles que le diagramme suivant soit commutatif :*

$$\begin{array}{ccc} \widehat{A}_1 & \xrightarrow{\varepsilon_1} & X_1 \\ \downarrow{\scriptstyle \hat{h}} & & \downarrow{\scriptstyle f} \\ \widehat{A}_2 & \xrightarrow{\varepsilon_2} & X_2 \end{array}$$

Le triplet (A_2, ε_2, h) *est uniquement déterminé à isomorphisme près par cette propriété. Si de plus* A_1 *est muni d'une structure de niveau* U, *alors (via* h*) il en est de même de* A_2.

On laisse au lecteur le soin de se convaincre de ce lemme plus ou moins évident : si par exemple f est une isogénie, alors en prendra pour A_2 le quotient $A_1/\varepsilon_1^{-1}(\mathrm{Ker}\, f)$.

6.3.2. — Utilisant le théorème fondamental du chapitre II (§8.4), ainsi que (6.2.3) ci-dessus, on voit que se donner une section de $(\widehat{\Omega}^2\otimes\overline{\mathbf{F}}_p)\times Z_U$ au-dessus d'un schéma connexe $S = \mathrm{Spec}\, B$ de caractéristique p revient à se donner :

a) Un homomorphisme $\psi : \overline{\mathbf{F}}_p \to B$.

b) Une classe d'isomorphie de couples (X, ρ) avec :

* X un $\mathcal{O}_{\Delta_p}$-module formel spécial sur S ;

* $\rho : \psi_*\Phi \to X$ une quasi-isogénie de hauteur 0.

c) Une algébrisation $(A, \varepsilon, \overline{\nu})$ de Φ avec structure de niveau U.

Partant de ces données, on applique le lemme ci-dessus avec $X_1 = \psi_*\Phi$, $X_2 = X$, $f = \rho$, $A_1 = \psi_*A$, $\varepsilon_1 = \psi_*\varepsilon$; on trouve ainsi une algébrisation de X avec structure de niveau U, c'est-à-dire un point de $\mathbf{S}_U(B)$. On

a ainsi défini un morphisme de foncteurs, d'où le morphisme cherché de $\mathbf{F}_p$-schémas :

$$\Theta : (\widehat{\Omega} \otimes \overline{\mathbf{F}}_p) \times Z_U \to \mathbf{S}_U \otimes \mathbf{F}_p.$$

6.3.3. — Vérifions que Θ est *invariant par l'action sur le membre de gauche du groupe* $GL(2, \mathbb{Q}_p)$; on se souvient pour cela que, d'après (chap. II, (9.3)), l'action d'un élément g de ce groupe sur le foncteur G est donnée par (en posant $n = v(\det g)$) :

$$g(\psi, X, \rho) = (\psi \circ Fr^{-n}, X, \rho \circ \psi_*(g^{-1}\mathrm{Frob}^n)).$$

D'autre part, l'action sur Z_U dont il a été question en (6.2.2) peut également être décrite en terme du lemme (6.3.1) : l'image $(A_1, \varepsilon_1, \overline{\nu}_1) = g(A, \varepsilon, \overline{\nu})$ est caractérisée par l'existence d'une p-quasi-isogénie $h_g : A \to A_1$ rendant commutatif le diagramme :

$$\begin{array}{ccc} \widehat{A} & \xrightarrow[\sim]{\varepsilon} & \Phi \\ {\scriptstyle \hat{h}_g}\downarrow & & \downarrow{\scriptstyle g} \\ \widehat{A}_1 & \xrightarrow[\sim]{\varepsilon_1} & \Phi. \end{array}$$

Notons (A_2, ε_2) l'algébrisation de X associée au point défini par $(\psi, X, \rho, A, \varepsilon, \overline{\nu})$; on a donc un diagramme commutatif :

$$\begin{array}{ccc} \psi_*\widehat{A} & \xrightarrow[\sim]{\psi_*\varepsilon} & \psi_*\Phi \\ {\scriptstyle \hat{h}}\downarrow & & \downarrow{\scriptstyle \rho} \\ \widehat{A}_2 & \xrightarrow[\sim]{\varepsilon_2} & X. \end{array}$$

Le point défini par :

$$(\psi_1 = \psi \circ Fr^{-n}, X, \rho_1 = \rho \circ \psi_*(g^{-1}\mathrm{Frob}^n), A_1, \varepsilon_1, \overline{\nu}_1)$$

a pour image la même algébrisation de X, ainsi qu'il résulte de la commutativité du diagramme :

$$\begin{array}{ccc}
\psi_{1*}\widehat{A}_1 & \xrightarrow[\sim]{\psi_{1*}\varepsilon_1} & \psi_{1*}\Phi \\
\downarrow{\scriptstyle \psi_*\mathrm{Frob}^n} & & \downarrow{\scriptstyle \psi_*\mathrm{Frob}^n} \\
\psi_*\widehat{A}_1 & \xrightarrow[\sim]{\psi_*\varepsilon_1} & \psi_*\Phi \\
\downarrow{\scriptstyle \psi_*\hat{h}_g^{-1}} & & \downarrow{\scriptstyle \psi_* g^{-1}} \\
\psi_*\widehat{A} & \xrightarrow[\sim]{\psi_*\varepsilon} & \psi_*\Phi \\
\downarrow{\scriptstyle \hat{h}} & & \downarrow{\scriptstyle \rho} \\
\widehat{A}_2 & \xrightarrow[\sim]{\varepsilon_2} & X
\end{array}$$

Finalement, on voit donc que Θ se *factorise* en un morphisme de $\mathbb{F}_p$-schémas :

$$\overline{\Theta} : GL(2, \mathbb{Q}_p)\backslash[(\widehat{\Omega} \otimes \overline{\mathbb{F}}_p) \times Z_U] \to \mathbf{S}_U \otimes \mathbb{F}_p.$$

6.4. *On veut maintenant montrer que $\overline{\Theta}$ est un isomorphisme.*

6.4.1. — Le quotient ci-dessus n'est rien d'autre que la fibre spéciale du quotient qui figure dans l'énoncé du théorème de Čerednik-Drinfeld (rappelons que U est supposé assez petit, et que par conséquent les groupes qui interviennent agissent librement) ; des commentaires analogues à ceux de (5.3) s'appliquent ici. Il est commode d'étendre les scalaires de $\mathbb{F}_p$ à $\overline{\mathbb{F}}_p$, et l'on voit facilement que le schéma obtenu à partir du quotient ci-dessus s'identifie au quotient :

$$GL'(2, \mathbb{Q}_p)\backslash(\widehat{\Omega}_{\overline{\mathbb{F}}_p} \times Z_U),$$

où l'on a noté GL' le sous-groupe de $GL(2, \mathbb{Q}_p)$ constitué des g tels que $v(\det g) = 0$. En termes modulaires, $\widehat{\Omega}_{\overline{\mathbb{F}}_p}$ représente le foncteur $\overline{G}$ qui classifie les couples (X, ρ), et GL' y opère par composition sur ρ.

Le morphisme $\overline{\Theta}_{\overline{\mathbb{F}}_p}$ déduit de $\overline{\Theta}$ par l'extension des scalaires provient d'un morphisme de $\overline{\mathbb{F}}_p$-schémas :

$$\Theta_1 : \widehat{\Omega}_{\overline{\mathbb{F}}_p} \times Z_U \to \mathbf{S}_U \otimes \overline{\mathbb{F}}_p.$$

Ce dernier associe à un point $(X, \rho, A, \varepsilon, \overline{\nu})$ défini sur une $\overline{\mathbf{F}}_p$-algèbre B l'algébrisation de X obtenue par application du lemme (6.3.1) avec $X_1 = \Phi_B$, $X_2 = X$, $f = \rho$, $A_1 = A_B$, $\varepsilon_1 = \varepsilon_B$.

6.4.2. — Montrons que $\overline{\Theta}_{\overline{\mathbf{F}}_p}$ induit une *bijection entre les ensembles de $\overline{\mathbf{F}}_p$-points des deux schémas* :

Injectivité : supposons que deux $\overline{\mathbf{F}}_p$-points $(X, \rho, A, \varepsilon, \overline{\nu})$ et $(X', \rho', A', \varepsilon', \overline{\nu}')$ admettent par Θ_1 la même image A_2 (une $\mathcal{O}_\Delta$-variété abélienne spéciale sur $\overline{\mathbf{F}}_p$, munie d'une structure de niveau). Alors, parce que A_2 est à la fois une algébrisation de X et de X', on voit que X s'identifie naturellement à X'. On voit ensuite que ρ et ρ' diffèrent par composition par un élément $g \in GL'(2, \mathbf{Q}_p)$: on peut donc supposer que $\rho = \rho'$. On constate enfin que $(A, \varepsilon, \overline{\nu})$ [resp. $(A', \varepsilon', \overline{\nu}')$] est l'algébrisation de Φ obtenue par application du lemme (6.3.1) à l'algébrisation A_2 de X et à ρ^{-1} [resp. l'algébrisation A_2 de X' et à ρ'^{-1}].

Les deux points sont donc bien déduits l'un de l'autre par l'action d'un élément de $GL'(2, \mathbf{Q}_p)$.

Surjectivité : A_2 étant donnée, notons X son complété formel. Parce que tous les $\mathcal{O}_{\Delta_p}$-modules formels spéciaux de hauteur 4 sur $\overline{\mathbf{F}}_p$ sont isogènes (chap. II, §5), il existe une quasi-isogénie $\rho : \Phi \to X$. On peut même supposer, par composition avec un endomorphisme convenable de Φ, que ρ est de hauteur 0.

Appliquant le lemme (6.3.1) à l'algébrisation A_2 de X et à ρ^{-1}, on obtient une algébrisation $(A, \varepsilon, \overline{\nu})$ de Φ avec structure de niveau : il est clair que A_2 est l'image de $(X, \rho, A, \varepsilon, \overline{\nu})$ par Θ_1.

6.4.3. — Prouvons maintenant que Θ_1 est *étale* : soit B une $\overline{\mathbf{F}}_p$-algèbre, et $B' \to B$ un épaisissement de B, de noyau un idéal de carré nul; soit $x = (X, \rho, A, \varepsilon, \overline{\nu})$ un point à valeurs dans B de $\widehat{\Omega}_{\overline{\mathbf{F}}_p} \times Z_U$, et $y = A_2$ son image par Θ_1. Déformer x en un B'-point x' revient à déformer le $\mathcal{O}_{\Delta_p}$-module formel X : en effet, la quasi-isogénie ρ se déforme uniquement (*cf.* par exemple [Zi 3] 5.31), et le schéma Z_U est constant. On voit donc que Θ_1 met en bijection les déformations x' de x et celles y' de y : la bijection réciproque associe à une déformation de A_2 la déformation sous-jacente du groupe formel $\widehat{A}_2 \simeq X$.

Par suite, $\overline{\Theta}_{\overline{\mathbf{F}}_p}$ est étale; comme il est aussi bijectif sur les $\overline{\mathbf{F}}_p$-points, c'est finalement un isomorphisme.

Donc $\overline{\Theta}$ est un isomorphisme.

6.5. — On vient ainsi d'obtenir un isomorphisme comme celui prédit par le théorème (5.2), mais *seulement pour l'instant entre les fibres*

spéciales; remarquer que, par construction, il se relève aux $\mathcal{O}_{\Delta_p}$-modules formels naturellement portés par les deux membres. Il est immédiat et formel de vérifier que ces isomorphismes sont compatibles entre eux quand U^p varie, et que le système de ces isomorphismes est $\Delta^*(\mathbb{A}_f^p)$-équivariant.

La possibilité de prolonger $\overline{\Theta}$ en un isomorphisme entre les deux schémas formels va résulter du théorème de Serre et Tate.

Soit B une $\mathbb{Z}_p$-algèbre où p est nilpotent, et $B_0 = B/pB$. La donnée d'un B_0-point x_0 du schéma $GL(2,\mathbb{Q}_p)\backslash[(\widehat{\Omega}\widehat{\otimes}\widehat{\mathbb{Z}}_p^{nr}) \times Z_U]$ munit (par image réciproque) B_0 d'un $\mathcal{O}_{\Delta_p}$-module formel spécial X_0. On voit que *déformer ce point x_0 à B revient à déformer X_0* : la question étant en effet locale, on est ramené à la résoudre pour le foncteur G, ce qui est évident.

En définitive, se donner un B-point x du schéma quotient ci-dessus revient à se donner sa restriction x_0 à B_0, plus une déformation X sur B de X_0. De même il est clair que se donner un B-point y de $\widehat{\mathbf{S}}_U$ revient à se donner sa restriction y_0 et une déformation A de A_0 (le $\mathcal{O}_\Delta$-schéma abélien spécial sur B_0 défini par y_0). Or si x_0 et y_0 se correspondent par l'isomorphisme $\overline{\Theta}, X_0$ s'identifie au complété $\widehat{A}_0$. Le théorème de Serre et Tate ([Me],[Dr2]) affirme que les déformations de A_0 correspondent bijectivement à celles de $\widehat{A}_0$, et donc de X : cela définit de façon naturelle un isomorphisme entre les schémas formels $GL(2,\mathbb{Q}_p)\backslash[(\widehat{\Omega}\widehat{\otimes}\widehat{\mathbb{Z}}_p^{nr}) \times Z_U]$ et $\widehat{\mathbf{S}}_U$, qui prolonge $\overline{\Theta}$, et qui possède visiblement toutes les propriétés souhaitées.

La preuve du théorème de Čerednik-Drinfeld est donc achevée.

Bibliographie

[A] M. ARTIN : *Versal Deformations and Algebraic Stacks.* Invent. Math. 27 (1974), 165–189.

[B-G-R] S. BOSCH, U. GÜNTZER, R. REMMERT : *Non Archimedean Analysis : a Systematic Approach to Rigid Analytic Geometry.* Grundlehren der mathematischen Wissenschaften 261, Springer-Verlag (1984).

[Bo] J.-F. BOUTOT : *Variétés de Shimura : Le Problème de Modules en Inégale Caractéristique.* Dans [Br-La] ci-dessous, exposé III, 43–62.

[Br] L. BREEN : *Calcul des Classes d'Isogénie.* Dans [Br-La] ci-dessous, exposé IV, 63–72.

[Br-La] L. BREEN, J.-P. LABESSE : *Variétés de Shimura et Fonctions L.* Publications Mathématiques de l'Université Paris VII, 6 (1979).

[Ca 1] H. CARAYOL : *Sur la Mauvaise Réduction des Courbes de Shimura.* Compositio Math. 59 (1986), 151–230.

[Ca 2] H. CARAYOL : *Non-Abelian Lubin-Tate Theory.* Dans : Automorphic Forms, Shimura Varieties, and L-functions, Vol II (L. Clozel and J.S. Milne, Ed.), Perspectives in Math. Vol. 11, Academic Press (1990), 15–39.

[Cat 1] P. CARTIER : *Modules Associés à un Groupe Formel Commutatif. Courbes Typiques.* C.R. Acad. Sci. Paris 265 Ser A (1967), 129–132.

[Cat 2] P. CARTIER : *Relèvement des Groupes Formels Commutatifs.* Sém. Bourbaki n° 359 (1968–1969). Lect. Notes in Math. 179, Springer-Verlag (1971), 217–230.

[Če] I.V. ČEREDNIK : *Uniformization of Algebraic curves by Discrete Arithmetic Subgroups of $PGL_2(k_w)$ with Compact Quotients.* Math. U.S.S.R. Sbornik 29 (1976) n° 1, 55–78.

[De] P. DELIGNE : *Travaux de Shimura. Sém. Bourbaki n° 389 (*1970-1971*).* Lect. Notes in Math. 244, Springer-Verlag (1971), 123–165.

[De-Hu] P. DELIGNE, D. HUSEMÖLLER : *Survey of Drinfeld Modules.* Dans : Current Trends in Arithmetical Algebraic Geometry (K. Ribet,

Ed.), Contemporary Mathematics Vol. 67, American Math. Soc., Providence (1987), 25–91.

[De-Ra] P. DELIGNE, M. RAPOPORT : *Les Schémas de Modules des Courbes Elliptiques.* Dans : Modular Functions of one Variable II (P. Deligne et W. Kuyk Ed.). Lect. Notes in Math. 349, Springer-Verlag (1973), 143–316.

[Dem] M. DEMAZURE : *Lectures on p-Divisible Groups.* Lect. Notes in Math. 302, Springer-Verlag (1972).

[Dr1] V.G. DRINFELD : *Elliptic Modules.* Math. U.S.S.R. Sbornik 23 (1974) n° 4, 561–592.

[Dr2] V.G. DRINFELD : *Coverings of p-Adic Symmetric Regions.* Functional Analysis and its Applications 10 (1976) n° 2, 107–115.

[Dr3] V.G. DRINFELD : *Elliptic Modules II.* Math. U.S.S.R. Sbornik 31 (1977) n° 2, 159–170.

[El] R. ELKIK : *Solutions d'Equations à Coefficients dans un Anneau Hensélien.* Ann. Sci. E.N.S. 4^e sér., 6 (1973), 553–604.

[Fr-VdP] J. FRESNEL, M. VAN DER PUT : *Géométrie Analytique Rigide et Applications.* Progress in Math. 18, Birkhaüser (1981).

[Ge] E.U. GEKELER : *Drinfeld Modular Curves.* Lect. Notes in Math. 1231, Springer-Verlag (1986).

[G-VdP] L. GERRITZEN, M. VAN DER PUT : *Schottky Groups and Mumford Curves.* Lect. Notes in Math. 817, Springer-Verlag (1980).

[Gi] J. GIRAUD : *Modules de Variétés Abéliennes et Variétés de Shimura.* Dans [Br-La] ci-dessus, exposé II, 21-42.

[G-Iw] O. GOLDMAN, N. IWAHORI : *The Space of p-Adic Norms.* Acta Math. 109 (1963), 137–177.

[Go] D. GOSS : *The Algebraist's Upper Half Plane.* Bull. (New Ser.) of the A.M.S., 2 (1980) n° 3, 391–415.

[Ha] M. HAZEWINKEL : *Formal Groups and Applications.* Academic Press (1978).

[Jo-Li] B. JORDAN, R. LIVNÉ : *Local Diophantine Properties of Shimura Curves.* Math Ann. 270 (1985), 235–248.

[K-M] N.M. KATZ, B. MAZUR : *Arithmetic Moduli of Elliptic Curves.* Annals of Math. Studies 108, Princeton University Press (1985).

[Ku] A. KURIHARA : *On some Examples of Equations defining Shimura Curves and the Mumford Uniformization.* J. Fac. Sci. Univ. Tokyo, Sec. IA, 25 (1979), 277–300.

[La] M. LAZARD : *Commutative Formal Groups.* Lect. Notes in Math. 443, Springer-Verlag (1975).

[Me] W. MESSING : *The Crystals associated to Barsotti-Tate Groups : with Applications to Abelian Schemes.* Lect. Notes in Math. 264, Springer-Verlag (1972).

[Mi] J.S. MILNE : *Points of Shimura Varieties mod. p.* Dans : Automorphic Forms, Representations and L-Functions, Proc. of Symp. in Pure Math. vol. 33 Part 2, Amer. Math. Soc., Providence (1979), 165–184.

[Mu 1] D. MUMFORD : *Abelian Varieties.* Oxford University Press (1970).

[Mu 2] D. MUMFORD : *An Analytic Construction of Degenerating Curves over Complete Local Rings.* Compositio Math. 24 (1972), Fasc. 3, 239–272.

[No] P. NORMAN : *An Algorithm for Computing Local Moduli of Abelian Varieties.* Ann. of Math. 101 (1975), 499–509.

[R] M. RAPOPORT : *On the Bad Reduction of Shimura Varieties.* Dans : Automorphic Forms, Shimura Varieties and L-Functions, Vol II, (L. Clozel and J.S. Milne Ed.), Perspectives in Math. Vol. 11, Academic Press (1990), 253–322.

[Ra 1] M. RAYNAUD : *Géométrie Analytique Rigide d'après Tate, Kiehl...* Table Ronde Anal. non Archim., Bull. Soc. Math. Fr., Mém. 39–40 (1974) 319–327.

[Ra 2] M. RAYNAUD : *Construction Analytique de Courbes en Géométrie non Archimédienne (d'après David Mumford).* Sém. Bourbaki n° 427 (1972-1973), Lect. Notes in Math. 383, Springer-Verlag (1974), 171–185.

[Ri 1] K.A. RIBET : *Bimodules and Abelian Surfaces.* Alg. Number Th. – In Honor of K. Iwasawa. Advanced Studies in Pure Math. 17, Academic Press (1989), 359–407.

[Ri 2] K.A. RIBET : *On Modular Representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *Arising from Modular Forms.* Inv. Math. 100 (1990), n° 2, 431–476.

[Sc] M. SCHLESSINGER : *Functors of Artin Rings.* Trans. A.M.S., vol. 130 (1968), 208–222.

[Se] J.- P. SERRE : *Arbres, Amalgames,* SL_2. Astérisque 46, Soc. Math. de France (1977).

[Ta 1] J. TATE : *Rigid Analytic Spaces.* Inv. Math. 12 (1971), 257–289.

[Ta 2] J. TATE : *Classes d'Isogénie des Variétés Abéliennes sur un Corps Fini (d'après Honda).* Sém. Bourbaki n° 352 (1968-1969), Lect. Notes in Math. 179, Springer-Verlag (1971), 95–109.

[Te] J. TEITELBAUM : *On Drinfeld's Universal Formal Group over the p-Adic Upper Half Plane.* Math. Ann. 284 (1989), 647–674.

[Zi 1] Th. ZINK : *Isogenien Formaler Gruppen über einem Lokal Noetherschen Schema.* Math. Nachr 99 (1980), 273–283.

[Zi 2] Th. ZINK : *Über die Schlechte Reduktion einiger Shimuramannigfaltigkeiten.* Compositio Math. 45 (1982) Fasc. 1, 15–107.

[Zi 3] Th. ZINK : *Cartiertheorie Kommutativer Formaler Gruppen.* Teubner-Texte zur Mathematik, Leipzig, Teubner (1984).

Jean-François BOUTOT
Henri CARAYOL
Département de Mathématique
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg Cedex
France

L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein".

Bas Edixhoven

le 19 mai 1988

1 Introduction.

Pour N un nombre entier positif soit $X_0(N)_{\mathbf{Q}}$ la courbe modulaire sur $\mathbf{Q}$ paramétrant les N-isogénies cycliques entre courbes elliptiques, et $J_0(N)_{\mathbf{Q}}$ sa jacobienne. L'algèbre de Hecke agit sur $J_0(N)_{\mathbf{Q}}$ donc aussi sur son modèle de Néron $J_0(N)$ sur $\mathbf{Z}$. Soit p un nombre premier et $\Phi_{N,p}$ le groupe de composantes connexes de la fibre géometrique $J_0(N)_p$ de $J_0(N)$ en caractéristique p.

Dans cet article nous démontrons que pour $p > 3$ l'action de l'algèbre de Hecke sur $\Phi_{N,p}$ est "Eisenstein". Cela veut dire que pour tout nombre premier l ne divisant pas N l'opérateur de Hecke T_l agit sur $\Phi_{N,p}$ par multiplication par $l+1$ (cf. [Ma], p.95). Ce résultat est une généralisation d'un théorème de K. Ribet [Ri 1],[Ri 2](Theorem 2.24), qui prouve le même résultat en supposant que la valuation de N en p est au plus 1. À dire vrai, Ribet prouve son théorème aussi pour $p = 2, 3$. Parce que dans ce cas la méthode de Ribet est plus efficace nous nous restreindrons au cas $p > 3$.

Pour prouver son théorème Ribet utilise la description donnée par A. Grothendieck [Gro 1] des groupes $\Phi_{N,p}$ en termes de l'accouplement de monodromie sur le groupe de caractères de la partie torique de la réduction (semistable) de $J_0(N)$ sur $\mathbf{Z}_p$. En se servant des résultats de [De-Ra] sur la réduction de $X_0(N)$ modulo p il obtient une description combinatoire de $\Phi_{N,p}$ en termes de points supersinguliers en caractéristique p. Ce qui reste alors à démontrer est une proposition sur les automorphismes des courbes elliptiques supersingulières.

Comme la méthode de Ribet ne marche qu'en cas de réduction semistable nous nous servons de la description donnée par M. Raynaud [Ray] des groupes $\Phi_{N,p}$ en termes de modèles sur $\mathbf{Z}$ des $X_0(N)_{\mathbf{Q}}$ qui sont réguliers. De tels modèles sont connus dans le cas où la valuation en p de N est au plus 1 [De-Ra], et dans le cas où $p > 3$ [Ed]. Pour l un nombre premier ne divisant pas N il faut montrer que l'opérateur de Hecke T_l agit sur $\Phi_{N,p}$ par multiplication par $l+1$. Cet opérateur T_l est défini en termes des deux morphismes standards de $X_0(Nl)_{\mathbf{Q}}$ vers $X_0(N)_{\mathbf{Q}}$. Afin de calculer l'action de T_l sur $\Phi_{N,p}$ nous étendons ces deux morphismes à certains modèles convenables sur $\mathbf{Z}_p$. Ces calculs nous conduisent à démontrer la proposition (déjà prouvée par Ribet dans le cas supersingulier) mentionnée plus haut (cf. Lemme 2 de (4.2)).

L'intérêt de ce théorème de Ribet est le rôle qu'il joue dans [Ri 2], où il est démontré que la conjecture de Taniyama et Weil implique celle de Fermat. Il est peut-être utile de remarquer que dans la démonstration que Taniyama-Weil implique Fermat [Ri 2] on n'a besoin que d'une version faible du théorème de Ribet. Cette version dit que l'action de l'algèbre de Hecke sur

le sous-groupe de q-torsion de $\Phi_{N,p}$ est Eisenstein pour tout nombre premier $q > 3$. D'après Mazur et Rapoport [Ma-Ra] ce sous-groupe est cyclique et on a un générateur explicite: c'est un multiple de $Z - Z'$ (dans leur notation). Il est très facile de calculer l'action d'un T_l sur $Z - Z'$. Bien sûr, il n'est pas utile d'affaiblir le théorème de Ribet quand il s'agit des conjectures de Serre.

Finissons par remarquer le fait que l'action de l'algèbre de Hecke sur les groupes de composantes des modèles de Néron des jacobiennes des courbes de Shimura n'est pas toujours "Eisenstein". Ceci est une conséquence du Théorème 4.3 de Ribet ([Ri 2], version d'octobre 1988).

J'aimerais remercier K. Ribet de m'avoir demandé si la généralisation de son théorème était vraie, de m'avoir envoyé une version préliminaire de son article [Ri 1], de m'avoir stimulé d'écrire ce texte, et de ses commentaires. J'aimerais aussi remercier J. Oesterlé de m'avoir suggéré beaucoup d'améliorations.

2 Description du groupe de composantes.

Soit S un trait strictement hensélien de point fermé s et de point générique t, et $\mathcal{C} \to S$ une courbe. Supposons que $\mathcal{C}$ est régulier et que $\mathcal{C}_t$ est lisse et géométriquement irréductible sur t. Nous allons rappeler la description que donne Raynaud ([Ray], (8.1)) du modèle de Néron de $\mathrm{Pic}^0_{\mathcal{C}_t/t}$ en termes du foncteur de Picard $\mathrm{Pic}_{\mathcal{C}/S}$.

Notons par C les composantes irréductibles réduites de $\mathcal{C}_s$, et par m_C la multiplicité de C dans $\mathcal{C}_s$. Alors on a l'égalité de diviseurs (de Weil ou Cartier) sur $\mathcal{C}$:

$$\mathcal{C}_s = \sum_C m_C C.$$

Pour ne pas avoir des ennuis nous supposons que $k(s)$ est algébriquement clos et que le plus grand commun diviseur des m_C est 1.

Soit $\mathrm{Pic}^{[0]}_{\mathcal{C}/S}$ le sous-foncteur de $\mathrm{Pic}_{\mathcal{C}/S}$ des faisceaux inversibles de degré total 0. Rappelons ([De-Ra]I(3.3.3) ou [Ray](8.1.1)) que le degré total d'un faisceau inversible $\mathcal{L}$ sur $\mathcal{C}_s$ est donné par:

$$\deg \mathcal{L} = \sum_C m_C \deg_C(\mathcal{L} \mid_C).$$

D'après théorème (8.1.4) de [Ray] le modèle de Néron de $\mathrm{Pic}^0_{\mathcal{C}_t/k(t)}$ est égal à $\mathrm{Pic}^{[0]}_{\mathcal{C}/S}/E$, où E est l'adhérence schématique de la section unité dans $\mathrm{Pic}^{[0]}_{\mathcal{C}/S}$. Ce faisceau en groupes E mesure le défaut de séparation de $\mathrm{Pic}^{[0]}_{\mathcal{C}/S}$ sur S. Puisque $\mathcal{C}/S$ satisfait la propriété $(\mathrm{N})^*$ ([Ray](6.1.4),(6.1.6)), $\mathcal{C}/S$ est cohomologiquement plat ([Ray](7.2.1)) et E est représenté par un schéma en groupes étale sur S ([Ray](5.2)). Ce schéma en groupes est "le schéma étalé sur S" correspondant au faisceau gratte-ciel de support s et de groupe $E(S)$. Le groupe $E(S)$ est formé des faisceaux inversibles sur $\mathcal{C}$ qui sont triviaux sur $\mathcal{C}_t$. Soit D le groupe abélien libre qui a pour base les composantes irréductibles C de $\mathcal{C}_s$, on a donc:

$$D = \bigoplus_C \mathbf{Z}[C].$$

Alors $E(S)$ est l'image du morphisme:

$$D \xrightarrow{\mathrm{div}} \mathrm{Pic}^{[0]}_{\mathcal{C}/S}(S) \qquad [C] \mapsto \mathcal{L}_C,$$

où $\mathcal{L}_C$ est l'inverse du faisceau d'idéaux sur $\mathcal{C}$ définissant le diviseur C. Comme $\mathrm{Pic}^0_{\mathcal{C}/S}$ est la composante neutre du modèle de Néron de $\mathrm{Pic}^0_{\mathcal{C}_t/t}$ ([Ray](8.1.2)) on a:

$$\Phi = \mathrm{Pic}^{[0]}_{\mathcal{C}/S}(s)/(E(s) + \mathrm{Pic}^0_{\mathcal{C}/S}(s)) = \mathrm{Pic}^{[0]}_{\mathcal{C}/S}(S)/(E(S) + \mathrm{Pic}^0_{\mathcal{C}/S}(S)),$$

où Φ est le groupe de composantes de la fibre sur s de ce modèle de Néron. Définissons un morphisme: $\mathrm{Pic}_{\mathcal{C}/S}(S) \xrightarrow{\text{multideg}} D$ par: $\mathcal{L} \mapsto \sum_C \deg(\mathcal{L} \mid_C)[C]$. Maintenant nous avons un diagramme où la ligne est exacte:

$$\begin{array}{ccccccccccc} & & & & & & D & & & & \\ & & & & & & \downarrow \mathrm{div} & \searrow^{\alpha} & & & \\ 0 & \to & \mathrm{Pic}^0_{\mathcal{C}/S}(S)) & \to & \mathrm{Pic}^{[0]}_{\mathcal{C}/S}(S) & \xrightarrow{\text{multideg}} & D & \xrightarrow{\deg} & \mathbf{Z} & \to & 0. \end{array}$$

Le morphisme $\alpha = \text{multideg} \circ \text{div}$ se calcule par:

$$\alpha : \quad [C] \mapsto \sum_{C'} \deg(\mathcal{L}_C \mid_{C'})[C'] = \sum_{C'} (C \cdot C')[C'],$$

où $(C \cdot C')$ est le nombre d'intersection de C et C' sur la surface régulière $\mathcal{C}$. De ce qui précède il s'ensuit que ([Ray](8.1.2)):

$$\Phi = \ker(\deg)/\mathrm{im}(\alpha).$$

Un élément de Φ est donc une classe modulo $\mathrm{im}(\alpha)$ de multidegrés de faisceaux inversibles sur $\mathcal{C}$.

3 Le groupe de composantes et morphismes.

Les notations sont celles de la Section 2. Soit $\tilde{\mathcal{C}}/S$ une courbe satisfaisant aux hypothèses faites sur $\mathcal{C}$, et $\tilde{\mathcal{C}} \xrightarrow{\pi} \mathcal{C}$ un S-morphisme. Nous allons calculer les deux morphismes induits par π sur les groupes de composantes: $\Phi \xrightarrow{\pi^*} \tilde{\Phi}$ et $\tilde{\Phi} \xrightarrow{\pi_*} \Phi$.

3.1 Calcul de π^*.

D'après (2), le groupe Φ est l'homologie du complexe: $D \xrightarrow{\alpha} D \xrightarrow{\deg} \mathbf{Z}$. On a un complexe analogue pour $\tilde{\Phi}$. Tenant compte des deux interprétations de D (groupe de diviseurs sur $\mathcal{C}$ à support dans $\mathcal{C}_s$ et groupe de multidegrés de faisceaux inversibles sur $\mathcal{C}$), on voit facilement que le morphisme $\pi^* : \Phi \to \tilde{\Phi}$ est induit par un morphisme de complexes:

$$\begin{array}{ccccc} D & \xrightarrow{\alpha} & D & \xrightarrow{\deg} & \mathbf{Z} \\ \downarrow \pi^*_{\mathrm{div}} & & \downarrow \pi^*_{\deg} & & \downarrow \deg(\pi) \\ \tilde{D} & \xrightarrow{\tilde{\alpha}} & \tilde{D} & \xrightarrow{\deg} & \mathbf{Z} \end{array}$$

$$\pi^*_{\mathrm{div}} : \quad [C] \mapsto \pi^{-1}C \quad \text{(diviseur sur } \tilde{\mathcal{C}})$$

$$\pi^*_{\deg} : \quad [C] \mapsto \sum_{\tilde{C} \overset{\pi}{\mapsto} C} \deg(\pi|_{\tilde{C}})[\tilde{C}].$$

3.2 Calcul de π_*.

Les notations sont toujours les mêmes, mais dans cette section il nous faut une hypothèse supplémentaire: $\tilde{\mathcal{C}} \xrightarrow{\pi} \mathcal{C}$ est quasi-fini. Parce que $\tilde{\mathcal{C}}/S$ et $\mathcal{C}/S$ sont propres, π est alors fini, et parce que $\tilde{\mathcal{C}}$ et $\mathcal{C}$ sont réguliers, π est plat. Le morphisme π est donc fini et plat, ce qui reste vrai après tout changement de base. La construction "norme d'un faisceau inversible" nous donne un morphisme: $\mathrm{Pic}_{\tilde{\mathcal{C}}/S} \xrightarrow{\pi_*} \mathrm{Pic}_{\mathcal{C}/S}$. En termes de diviseurs ce morphisme est l'image directe.

En regardant les valuations que donnent les composantes irréductibles des fibres fermées on trouve l'égalité de diviseurs sur $\tilde{\mathcal{C}}$:

$$\pi^{-1}C = \sum_{\tilde{C} \mapsto C} (m_{\tilde{C}}/m_C)\tilde{C}.$$

Localisation au point générique d'un C nous donne:

$$\deg(\pi) = \sum_{\tilde{C} \mapsto C} (m_{\tilde{C}}/m_C)\deg(\tilde{C}/C).$$

Pour l'image directe d'un $\tilde{C}$ on a par définition ([Gro 2] (21.10.14.1)): $\pi_*(\tilde{C}) = \deg(\tilde{C}/\pi\tilde{C})\pi\tilde{C}$. Pour voir ce qui arrive aux multidegrés appliquons le corollaire (7.1.2) de [Ray], ce corollaire dit que pour chaque $\tilde{C}$ il existe un diviseur effectif horizontal Z sur $\tilde{\mathcal{C}}$ qui a degré 1 sur $\tilde{C}$ et degré 0 sur les autres composantes de $\tilde{\mathcal{C}}_s$. Le degré de π_*Z sur $\pi\tilde{C}$ se calcule par la formule de projection: $(\pi_*Z \cdot \pi\tilde{C}) = (Z \cdot \pi^*\pi\tilde{C}) = (Z \cdot (m_{\tilde{C}}/m_{\pi\tilde{C}})\tilde{C}) = m_{\tilde{C}}/m_{\pi\tilde{C}}$. Maintenant nous savons tout du morphisme de complexes qui induit π_* sur les groupes de composantes:

$$\begin{array}{ccccccc} \mathbf{Z} & \to & \tilde{D} & \xrightarrow{\tilde{\alpha}} & \tilde{D} & \xrightarrow{\deg} & \mathbf{Z} \\ \downarrow \deg(\pi) & & \downarrow \pi_*^{\mathrm{div}} & & \downarrow \pi_*^{\deg} & & \downarrow 1 \\ \mathbf{Z} & \to & D & \xrightarrow{\alpha} & D & \xrightarrow{\deg} & \mathbf{Z} \end{array}$$

$$\pi_*^{\mathrm{div}} : \quad [\tilde{C}] \mapsto \deg(\tilde{C}/\pi\tilde{C})[\pi\tilde{C}]$$
$$\pi_*^{\deg} : \quad [\tilde{C}] \mapsto (m_{\tilde{C}}/m_{\pi\tilde{C}})[\pi\tilde{C}].$$

Remarque. Comme l'a suggéré J. Oesterlé, on peut calculer le morphisme induit par π sur les groupes de composantes sans supposer que π est quasi-fini. Le morphisme $\pi : \tilde{\Phi} \to \Phi$ est alors induit par un morphisme de complexes commme ci-dessus, où $\pi_*^{\deg}$ est donné par la formule:

$$\pi_*^{\deg} : \quad [\tilde{C}] \mapsto \sum_{\tilde{C} \subset \pi^{-1}C} m_{\tilde{C},C}[C]$$

avec $m_{\tilde{C},C}$ la multiplicité de $\tilde{C}$ dans $\pi^{-1}C$. La formule pour π_*^{div} est toujours la même.

3.3 Éclatements.

Il peut être nécessaire de travailler avec des modèles non minimaux, par exemple pour avoir des morphismes entre modèles réguliers. Bien sûr, le groupe de composantes ne dépend pas du modèle (régulier) qu'on choisit, mais c'est sa description qui change quand on change de modèle. Nous avons donc besoin de traduire une description en une autre. Soit alors $\tilde{\mathcal{C}} \xrightarrow{\pi} \mathcal{C}$ obtenu en faisant éclater $\mathcal{C}$ en un point $x \in \mathcal{C}(s)$. Nous notons E la courbe exceptionnelle et $\tilde{C}$ le transformé strict d'une composante irréductible C de $\mathcal{C}_s$.

Dans ce cas on a: $\pi^*_{\deg}$: $[C] \mapsto [\tilde{C}]$. Cette formule donne l'isomorphisme: $\Phi \xrightarrow{\pi^*} \tilde{\Phi}$, nous voulons aussi une formule pour son inverse. Pour cela il faut éliminer les $[E]$ d'un élément de $\tilde{\Phi}$. La relation voulue nous est fournie par $\tilde{\alpha}([E])$:

$$\tilde{\alpha}([E]) = -[E] + \sum_{x \in C(s)} m_{C,x}[\tilde{C}]$$

où $m_{C,x}$ est la multiplicité de C en x. L'isomorphisme $\tilde{\Phi} \to \Phi$ est donc induit par:

$$(\pi^*_{\deg})^{-1} : \tilde{D} \to D \qquad [\tilde{C}] \mapsto [C] \quad [E] \mapsto \sum_{x \in C(s)} m_{C,x}[C].$$

4 Le cas des courbes modulaires $X_0(N)$.

Pour N un entier positif soit $X_0(N)$ la courbe modulaire sur $\mathbf{Z}$ paramétrant les N-isogénies cycliques entre courbes elliptiques: $X_0(N)$ est le schéma grossier de modules compactifié associé au problème de modules $[\Gamma_0(N)]$ (cf. [Ka-Maj(8.6)). Cette courbe $X_0(N)/\mathbf{Z}$ est un modèle normal de sa fibre générique $X_0(N)_{\mathbf{Q}}/\mathbf{Q}$, mais malheureusement ce n'est pas toujours un modèle régulier. Notons par $J_0(N)$ le modèle de Néron sur $\mathbf{Z}$ de $\mathrm{Pic}^0_{X_0(N)_{\mathbf{Q}}/\mathbf{Q}}$. Soit p un nombre premier, S le spectre de l'anneau des vecteurs de Witt sur $\overline{\mathbf{F}_p}$ et $\widetilde{X_0(N)}_S$ la résolution minimale de $X_0(N)_S$. Deligne et Rapoport [De-Ra] ont donné une description de $\widetilde{X_0(N)}_S$ dans le cas où la valuation de N en p est au plus 1. Utilisant les résultats de Katz et Mazur [Ka-Ma] on peut décrire $\widetilde{X_0(N)}_S$ pour $p > 3$ [Ed]. Dans ces deux cas on connaît donc la table d'intersection de la fibre spéciale de $\widetilde{X_0(N)}_S$, et d'après la Section 2 cela suffit pour calculer le groupe de composantes $\Phi_{N,p}$ de $J_0(N)_s$. Nous donnerons quelques exemples de ces groupes en (4.4).

4.1 Action de l'algèbre de Hecke sur $\Phi_{N,p}$.

Soit l un nombre premier ne divisant pas N. Pour une isogénie cyclique de degré Nl entre courbes elliptiques (sur une base quelconque): $E_1 \xrightarrow{\phi_{Nl}} E_2$ il existe des factorisations uniques (à isomorphisme près):

$$E_1 \xrightarrow{\phi_{N,1}} E_3 \xrightarrow{\phi_{l,2}} E_2 \qquad E_1 \xrightarrow{\phi_{l,1}} E_4 \xrightarrow{\phi_{N,2}} E_2$$

où $\phi_{*,i}$ a degré $*$ (cf. [Ka-Ma] (6.7)).

Au niveau de problèmes de modules cela donne deux morphismes:

$$\mathrm{S}, \mathrm{T} : [\Gamma_0(Nl)] \to [\Gamma_0(N)] : \quad \mathrm{S}(\phi_{Nl}) = \phi_{N,1} \quad \mathrm{T}(\phi_{Nl}) = \phi_{N,2},$$

et une involution:

$$\mathrm{W}_l : [\Gamma_0(Nl)] \to [\Gamma_0(Nl)] \quad \phi_{Nl} \mapsto \phi_{N,1}\phi^t_{l,1}.$$

Par construction on a: $\mathrm{T} = \mathrm{S} \circ \mathrm{W}_l$. On obtient des morphismes induits: $\mathrm{S}, \mathrm{T} : X_0(Nl) \to X_0(N)$, $X_0(Nl)_{\mathbf{Q}} \to X_0(N)_{\mathbf{Q}}$, un endomorphisme $\mathrm{T}_l = \mathrm{T}_*\mathrm{S}^*$ de $J_0(N)$, et finalement un endomorphisme T_l de $\Phi_{N,p}$. Le fait que S, T et W_l se prolongent aux pointes est démontré dans [De-Ra] Ch. IV Prop. 3.16, 3.18, Prop. 3.19 et ex. 4.4.

Théorème 1 *L'endomorphisme* T_l *de* $\Phi_{N,p}$ *est multiplication par* $l + 1$ *si* $p > 3$.

Dans ce cas ($p > 3$) on connaît des modèles réguliers, alors avec les methodes des Sections 2 et 3 on pourrait simplement calculer $S^* : \Phi_{N,p} \to \Phi_{Nl,p}$ et $T_* : \Phi_{Nl,p} \to \Phi_{N,p}$, mais on peut faire un peu mieux. C'est à dire qu'il suffit de prouver que $S^* = T^* : \Phi_{N,p} \to \Phi_{Nl,p}$, parce que cela implique que $T_l = T_*T^* : \Phi_{N,p} \to \Phi_{N,p}$, et T_*T^* agit sur $J_0(N)_{\mathbf{Q}}$ (et donc aussi sur $\Phi_{N,p}$) par $\deg(T) = l + 1$. Cette astuce est due à Ribet, (d'après Ribet, le vrai résultat est cette égalité, et le Théorème 1 en est un corollaire). On aurait pu faire beaucoup mieux si l'action de W_l sur $\Phi_{Nl,p}$ était triviale (cela réduirait le théorème à une proposition sur une seule courbe), mais cela n'est pas vrai. Alors le plus grand problème dans la démonstration de $S^* = T^*$ est de décrire des modèles réguliers de $X_0(Nl)_S$ et $X_0(N)_S$ auxquels les morphismes S et T se prolongent. On donnera quelques exemples de ces modèles en (4.3).

Soit maintenant $\mathcal{P}$ une structure de niveau supplémentaire convenable (par exemple $[\Gamma(3)]_S$), tel qu'on a des morphismes de schémas de modules compactifiés sur S:

$$\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(Nl)]) \xrightarrow{S,T} \overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(N)]),$$

avec une action (fidèle, d'un groupe G) tel que le quotient par cette action est:

$$X_0(Nl)_S \xrightarrow{S,T} X_0(N)_S.$$

Pour simplifier nous supprimons dans la suite les indices inférieures "S".

Soit $x \in \mathcal{M}(\mathcal{P}, [\Gamma_0(N)])(s)$ un point à stabilisateur G_x non trivial. Comme en [Ed] on fait éclater $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(N)])$ en x jusqu'à ce que l'action de G_x sur les points fixes au dessus de x est par pseudo-réflexions (il faut donc 0,1 ou 3 éclatements). On fait éclater $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(Nl)])$ en tout $y \in S^{-1}(x)$ de la même manière qu'on a fait éclater $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(N)])$ en x. Notons les modèles obtenus par $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(N)])^*$ et $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(Nl)])^{*S}$. Nous avons maintenant un grand diagramme:

$$\begin{array}{ccc}
\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(Nl)])^{*S} & \xrightarrow{S} & \overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(N)])^* \\
\downarrow & & \downarrow \qquad \text{quotient par G-action} \\
X_0(Nl)^{*S} & \xrightarrow{S} & X_0(N)^* \\
\downarrow \pi^S & & \downarrow \pi \qquad \text{composé d'éclatements} \\
\widetilde{X_0(Nl)} & & \widetilde{X_0(N)} \\
\downarrow & & \downarrow \qquad \text{composé d'éclatements} \\
X_0(Nl) & \xrightarrow{S} & X_0(N)
\end{array}$$

Il y a des morphismes induits sur les groupes abéliens libres engendrés par les composantes des fibres fermées, nous n'écrivons que les deux lignes au milieu:

$$\begin{array}{ccc}
\tilde{D}^{*S} & \xleftarrow{S^*_{\deg}} & D^* \\
\downarrow (\pi^{S*}_{\deg})^{-1} & & \uparrow \pi^*_{\deg} \\
\tilde{D} & & D
\end{array}$$

où $S^*_{\deg}$ et $\pi^*_{\deg}$ sonts induits par S et π comme en (3.1), et $(\pi^{S*}_{\deg})^{-1}$ par π^S comme en (3.3).

La composition de ces trois morphismes, qu'on notera $S^* : D \to \tilde{D}$, induit $S^* : \Phi_{N,p} \to \Phi_{Nl,p}$. De la même manière on trouve des morphismes:

$$T^* : \ D \xrightarrow{\pi^*_{\deg}} D^* \xrightarrow{T^*_{\deg}} \tilde{D}^{*T} \xrightarrow{(\pi^{T*}_{\deg})^{-1}} \tilde{D}.$$

Le théorème à démontrer est maintenant une conséquence de la proposition suivante.

Proposition 1 $S^* = T^* : D \longrightarrow \tilde{D}$.

On prouvera l'égalité $S^*([C]) = T^*([C])$ pour tout élément de base de D. Pour C le transformé strict d'une composante de $X_0(N)_s$ cela résulte de la description par [Ka-Ma]: si C est de type (a,b) alors $S^*([C]) = T^*([C]) = (l+1)[(a,b)\text{-composante de } X_0\widetilde{(Nl)}_s]$.

Soit $x \in (\text{Sing } X_0(N))(s)$, et C_x une composante de $X_0\widetilde{(N)}_s$ dans l'image réciproque de x. Par (3.1) on a: $\pi^*_{\deg}[C_x] = [\tilde{C}_x]$, où $\tilde{C}_x$ est le transformé strict de C_x dans $X_0(N)^*$. Encore par (3.1) on a:

$$S^*([\tilde{C}_x]) = \sum_{Sy=x} [C_y^*] \qquad T^*([\tilde{C}_x]) = \sum_{Ty=x} [C_y^*]$$

où les sommes sont sur les $y \in X_0(Nl)(s)$ avec $Sy = x$ (resp. $Ty = x$), et C_y^* est la composante unique de $X_0(Nl)_s^*$ au dessus de y avec S (ou T)-image $\tilde{C}_x$. Les coefficients sont 1 parce que les $\deg(C_y^*/\tilde{C}_x)$ sont 1, ce qui à son tour résulte de ce que l'action de G_x sur chaque composante de $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(N)])_s^*$ au dessus de $\tilde{C}_x$ est triviale (cf. [Ed](ch.1)).

Par (3.3) on a:

$$(\pi^{S*}_{\deg})^{-1} S^*[\tilde{C}_x] = \sum_C a_{\tilde{C}}[\tilde{C}] + \sum_{Sy=x} [\tilde{C}_y]$$

où le deuxième terme est une somme sur les $y \in (\text{Sing } X_0(Nl))(s)$ seulement, et le premier terme est une somme sur les composantes de $X_0(Nl)_s$ ($\tilde{C}$ est le transformé strict dans $X_0\widetilde{(Nl)}$ de C). Ce premier terme est le résultat de l'élimination des $[C_y^*]$ avec $Sy = x$ mais $y \in (\text{Reg } X_0(Nl))(s)$. Pour T on a une somme analogue:

$$(\pi^{T*}_{\deg})^{-1} T^*[\tilde{C}_x] = \sum_C b_{\tilde{C}}[\tilde{C}] + \sum_{Ty=x} [\tilde{C}_y].$$

Il nous faut prouver que ces deux sommes sont identiques. Il est clair (cf. (3.3)) que les $a_{\tilde{C}}$ et $b_{\tilde{C}}$ dépendent seulement (et de la même manière) du nombre de $[C_y^*]$ éliminés, donc il suffit de prouver l'égalité des deuxièmes termes. Cela revient à démontrer que:

$$(\text{Sing } X_0(Nl))(s) \cap S^{-1}x = (\text{Sing } X_0(Nl))(s) \cap T^{-1}x,$$

ce qui est une conséquence du Lemme 2 de (4.2).

4.2 Un lemme sur les automorphismes des courbes elliptiques.

Soit p un nombre premier, $k := \overline{\mathbf{F}_p}$, N un nombre entier positif qui n'est pas divisible par p, et $X_0(N) \xrightarrow{S} X_0(1)$ le morphisme donné par: $(E_1 \to E_2) \mapsto E_1$. (Dans cette section nous ne supposons *pas* que $p > 3$.)

Soit $x \in X_0(N)(k)$, $\sigma \in \text{Aut}_k(x)$ correspondant au diagrammes suivants:

$$E_1 \xrightarrow{\phi} E_2 \qquad \begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow \sigma_1 & & \downarrow \sigma_2 \\ E_1 & \xrightarrow{\phi} & E_2 \end{array}$$

Notons que σ_1 et σ_2 ont même ordre que σ, donc la connaissance des courbes elliptiques à automorphismes $\neq \pm 1$ nous apprend que si $\sigma \neq \pm 1$ alors l'ordre de σ est 3,4 ou 6, et E_2 est isomorphe à E_1. Ceci implique que dans nos considérations sur les points de $X_0(N)$ à automorphismes nous aurons affaire aux endomorphismes seulement.

Soit maintenant $y \in X_0(1)(k)$ (disons $y \sim E$) et $\pm 1 \neq \sigma \in \mathrm{Aut}_k(y)$, alors :

$$\{x \in \mathrm{S}^{-1}y \mid \sigma \in \mathrm{Aut}_k(x)\} = \{E \xrightarrow{\phi} E_1 \mid \sigma \ker\phi = \ker\phi\}$$

Il s'agit donc de sous-groupes σ-invariants cycliques d'ordre N de

$$E[N](k) \cong (\mathbf{Z}/N)^2 = \prod_{q|N} (\mathbf{Z}/q^{n_q})^2,$$

où $N = \prod_{q|N} q^{n_q}$ est la factorisation de N en facteurs premiers. Sachant que pour tout $q \neq 2, 3$ l'action de σ sur $E[q](k)$ a deux valeurs propres distinctes il est facile de démontrer le lemme suivant.

Lemme 1 *Écrivons $N = 2^{n_2} \prod_{q \neq 2} q^{n_q}$. Pour $y \in X_0(1)(k)$ et $\sigma_4 \in \mathrm{Aut}_k(y)$ d'ordre 4 on a:*

$$\#\{x \in \mathrm{S}^{-1}y \mid \sigma_4 \in \mathrm{Aut}_k(x)\} = \begin{cases} 0 & \text{si } n_2 > 1 \text{ ou } \exists q \equiv -1(4) \\ 2^{\#\{q|q\neq 2\}} & \text{sinon.} \end{cases}$$

Écrivons $N = 3^{n_3} \prod_{q \neq 3} q^{n_q}$. Pour $y \in X_0(1)(k)$ et $\sigma_3 \in \mathrm{Aut}_k(y)$ d'ordre 3 on a:

$$\#\{x \in \mathrm{S}^{-1}y \mid \sigma_3 \in \mathrm{Aut}_k(x)\} = \begin{cases} 0 & \text{si } n_3 > 1 \text{ ou } \exists q \equiv -1(3) \\ 2^{\#\{q|q\neq 3\}} & \text{sinon.} \end{cases}$$

Nous savons déjà que les points de $X_0(N)(k)$ à automorphismes $\neq \pm 1$ correspondent aux endomorphismes (= isogénies dont la source et le but coïncident). Il se trouve même que ces endomorphismes appartiennent à l'un des sous-anneaux $\mathbf{Z}[\sigma_4]$ et $\mathbf{Z}[\sigma_3]$ de $\mathrm{End}_k(E)$. Cela résulte du fait que $\mathbf{Z}[\sigma_4]$ et $\mathbf{Z}[\sigma_3]$ sont de factorisation unique et que la factorisation de N donne exactement le même nombre d'endomorphismes cycliques de degré N que le lemme précédent.

Lemme 2 *Soit $N = lM$ avec l un nombre premier qui ne divise pas M, et $x \in X_0(N)(k)$ avec $\sigma \in \mathrm{Aut}_k(x)$ d'ordre 3 ou 4. Alors on a $\mathrm{S}x = \mathrm{T}x$ pour S et T les deux morphismes $X_0(N) \to X_0(M)$ de (4.1).*

Disons que x correspond à $E \xrightarrow{\phi_N} E$, et $\phi_N \in \mathbf{Z}[\sigma]$. Ce ϕ_N se factorise en deux facteurs de degrés M et l: $\phi_N = \phi_M \phi_l$. Alors de $\phi_M \phi_l = \phi_l \phi_M$ il résulte que $\mathrm{S}x = \phi_M = \mathrm{T}x$.

4.3 Quelques exemples des modèles utilisés en (4.1).

Dans cette section on trouve des dessins des fibres fermées de quelques modèles utilisés en (4.1). Pour obtenir ces dessins on se sert de la description des points à automorphismes de (4.2) et de [Ed] ch.1.

Traitons le cas: $X_0(2 \cdot 11)_S \xrightarrow{\mathrm{S}} X_0(11)_S$ où S est de caractéristique résiduelle 11. Les dessins sont dans la Figure 1.

Le deuxième exemple est: $X_0(2 \cdot 13^2)_S \xrightarrow{\mathrm{S}} X_0(13^2)_S$, avec S de caractéristique résiduelle 13. Les dessins sont dans la Figure 2.

Figure 1: Le cas $X_0(2 \cdot 11)_S \xrightarrow{s} X_0(11)_S$.

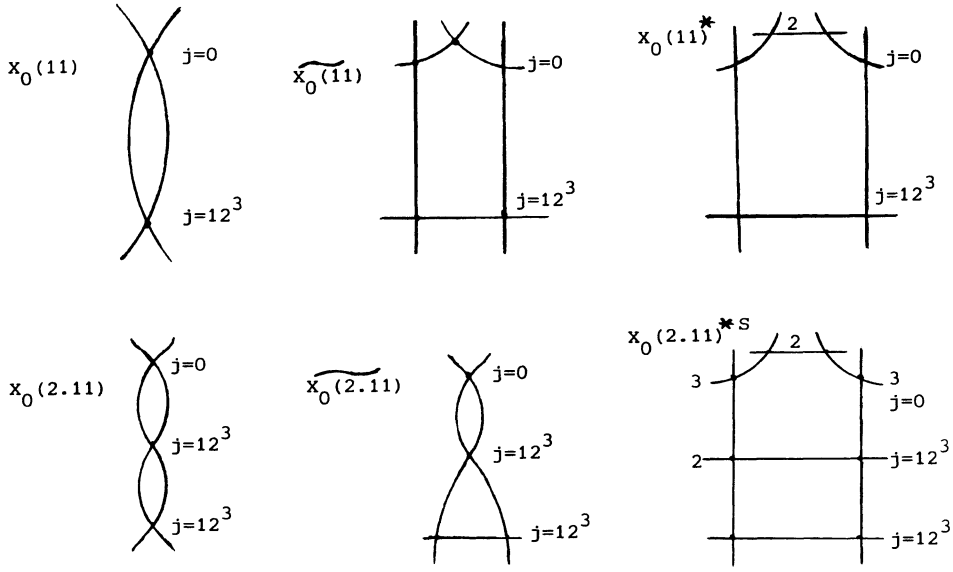
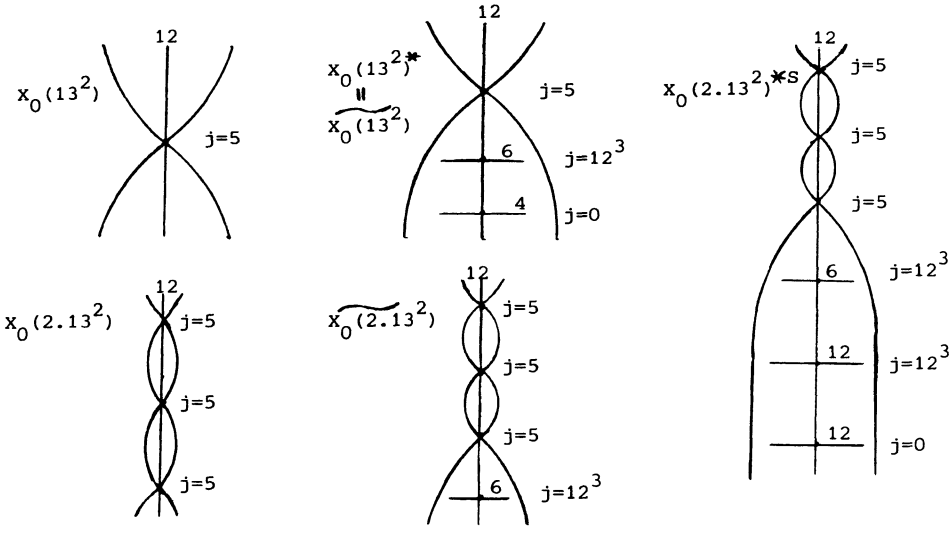


Figure 2: Le cas $X_0(2 \cdot 13^2)_S \xrightarrow{s} X_0(13^2)_S$.



4.4 Quelques exemples des groupes $\Phi_{N,p}$.

4.4.1 Le cas traité par Mazur et Rapoport.

Il y a quelques petites erreurs dans les calculs de [Ma-Ra]. Dans cette section, nous nous permettons de refaire ces calculs. Il y a trois choses à dire. Premièrement: les $1/d_i$ qui se trouvent dans leur Proposition (1.4) ne doivent pas être là, apparemment ils n'ont pas tenu compte du fait que les X_i dans [Ray], (8.1.1) ne sont pas nécessairement réduits. D'ailleurs cela n'affecte pas leurs résultats parce que tous les d_i y sont 1. Deuxièmement: le nombre de points supersinguliers n'est pas comme il est écrit dans la Proposition (1.2): $(Q-2^\nu)/2$ doit être $(Q+2^\nu)/2$ et $(Q-2^\nu)/3$ doit être $(Q+2^{\nu+1})/3$. Troisièmement: il y a une erreur dans la structure du groupe Φ (leurs Φ modulo 2-torsion et 3-torsion ne sont pas cycliques (cf. Table 2, page 174), tandis que cela doit être bien le cas). Dans cette section nous tentons de donner les tables correctes.

Rappelons les notations: $N = pM$ est un nombre entier positif , $p > 3$ un nombre premier qui ne divise pas M. Notons par s_2, s_4 et s_6 les nombres de points supersinguliers $x \in X_0(M)(\overline{\mathbf{F}_p})$ tel que $\#\mathrm{Aut}(x) = 2, 4, 6$. Alors notre calcul de $\Phi_{N,p}$ donne:

s_4	s_6	$\Phi_{N,p}$
0	0	$\mathbf{Z}/s_2$
>1	0	$\mathbf{Z}/(2(2s_2+s_4)) \oplus (\mathbf{Z}/2)^{s_4-2}$
0	>1	$\mathbf{Z}/(3(3s_2+s_6)) \oplus (\mathbf{Z}/3)^{s_6-2}$
>1	>1	$\mathbf{Z}/(6(6s_2+3s_4+2s_6)) \oplus (\mathbf{Z}/2)^{s_4-2} \oplus (\mathbf{Z}/3)^{s_6-2}$

Pour obtenir $\Phi_{N,p}$ dans le cas où $s_4 = 1$ il faut faire comme suit: prendre le cas $s_4 > 1$, supprimer le terme avec exposant "$s_4 - 2$" et supprimer le facteur "2" du premier terme. Si $s_6 = 1$ on supprime le terme d'exposant "$s_6 - 2$" et le facteur "3" du premier terme.

Soit maintenant $M = \prod_q q^{n_q}$ la factorisation de M en facteurs premiers ($n_q > 0$), $\nu = \#\{q \mid q \neq 2, 3\}$ et $Q = \deg(X_0(M)/X_0(1)) = \prod_q (q+1)q^{n_q-1}$. Alors les nombres s_2, s_4, s_6 sont donnés par:

p		s_2	s_4	s_6
$p \equiv 1(12)$		$Q\frac{p-1}{12}$	0	0
$p \equiv 5(12)$	$s_6 = 0$	$Q\frac{p-1}{12}$	0	0
	$s_6 \neq 0$	$\frac{Q(p-1)-4\cdot 2^\nu}{12}$	0	2^ν
$p \equiv 7(12)$	$s_4 = 0$	$Q\frac{p-1}{12}$	0	0
	$s_4 \neq 0$	$\frac{Q(p-1)-6\cdot 2^\nu}{12}$	2^ν	0
$p \equiv 11(12)$	$(s_4 = 0) \wedge (s_6 = 0)$	$Q\frac{p-1}{12}$	0	0
	$(s_4 \neq 0) \wedge (s_6 = 0)$	$\frac{Q(p-1)-6\cdot 2^\nu}{12}$	2^ν	0
	$(s_4 = 0) \wedge (s_6 \neq 0)$	$\frac{Q(p-1)-4\cdot 2^\nu}{12}$	0	2^ν
	$(s_4 \neq 0) \wedge (s_6 \neq 0)$	$\frac{Q(p-1)-10\cdot 2^\nu}{12}$	2^ν	2^ν

$$s_4 = 0 \Longleftrightarrow n_2 > 1 \ \vee \ \exists q \equiv -1(4)$$

$$s_6 = 0 \Longleftrightarrow n_3 > 1 \ \vee \ \exists q \equiv -1(3)$$

Notons que les nombres s_2, s_4 et s_6 dans la table ci-dessus satisfont à la formule de masse ([Ka-Ma](12.4.5, 12.4.6)):

$$s_2/2 + s_4/4 + s_6/6 = \sum_{x=s.s.} 1/\#\mathrm{Aut}(x) = Q(p-1)/24.$$

4.4.2 Les groupes $\Phi_{p^2,p}$ pour $p > 3$.

Donnons d'abord un exemple: $p = 13$. Dans (4.3) on trouve le "graphe" de la fibre fermée de $X_0(13^2)$. Les nombres d'intersection s'en déduisent facilement et on obtient le morphisme α de la Section 2:

$$\alpha = \begin{pmatrix} -13 & 1 & 1 & 0 & 0 \\ 1 & -13 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 & -3 \end{pmatrix}.$$

Un calcul facile donne: $\Phi_{13^2,13} \cong \mathbf{Z}/7$.

Dans le cas général on trouve:

Proposition 2 *Pour $p > 3$ on a $\Phi_{p^2,p} \cong \mathbf{Z}/\frac{p^2-1}{24}$.*

Bibliographie

[De-Ra] Deligne, P. et Rapoport, M. *Les schémas de modules de courbes elliptiques.* Lecture Notes in Mathematics 349, 143–316 (1973).

[Ed] Edixhoven, S.J. *Minimal resolution and stable reduction of $X_0(N)$.* University Utrecht Dep. Math. preprint #438 (1986).

[Gro 1] Grothendieck, A. *Modèles de Néron et monodromie.* Séminaire de Géométrie Algébrique 7, Exposé IX, Lecture Notes in Mathematics 288, 313–523 (1972).

[Gro 2] Grothendieck, A. *Eléments de géométrie algébrique IV.* Publications Mathématiques de l'IHES 32 (1967).

[Ka-Ma] Katz, N. and Mazur, B. *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies, Study 108 (1985).

[Ma] Mazur, B. *Modular curves and the Eisenstein ideal.* Publications Mathématiques de l'IHES 47, 33–186 (1977).

[Ma-Ra] Mazur, B. and Rapoport, M. *Behavior of the Néron model of the jacobian of $X_0(N)$ at bad primes.* Appendice de [Ma].

[Ray] Raynaud, M. *Spécialisation du foncteur de Picard.* Publications Mathématiques de l'IHES 38, 27–76 (1970).

[Ri 1] Ribet, K.A. *On the component groups and the Shimura subgroup of $J_0(N)$.* Séminaire de théorie des nombres de Bordeaux 1988.

[Ri 2] Ribet, K.A. *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms.* MSRI preprint #06420-87 (June, 1987).

Bas Edixhoven
Mathematisch Instituut
Budapestlaan 6
Postbus 80.010
3508 TA Utrecht
The Netherlands.

The Shimura Subgroup of $J_0(N)$

San Ling* and Joseph Oesterlé†

SUMMARY. — *To the natural morphism $X_1(N) \to X_0(N)$ of modular curves corresponds, by Picard functoriality, a morphism $J_0(N) \to J_1(N)$ between their Jacobian varieties. Its kernel $\Sigma(N)$, called the Shimura subgroup of $J_0(N)$, is finite. We determine the group structure of $\Sigma(N)$ together with the action of Galois and the action of the Hecke algebra. This extends previous results obtained by B. Mazur and K. Ribet.*

Let $N \geq 1$ be an integer and let $\Gamma_0(N)$ be the subgroup of $SL_2(\mathbf{Z})$ consisting of the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ such that N divides c. It acts on the Poincaré half-plane $\mathcal{H} = \{\tau \in \mathbf{C} |\ \mathrm{Im}\,\tau > 0\}$ and on $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ by

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \tau \right) \mapsto \frac{a\tau + b}{c\tau + d}.$$

The quotient $X_0(N) = \Gamma_0(N)\backslash\overline{\mathcal{H}}$ has a natural structure of compact connected Riemann surface.

One defines in a similar way a Riemann surface $X_1(N) = \Gamma_1(N)\backslash\overline{\mathcal{H}}$, where $\Gamma_1(N)$ is the subgroup of $\Gamma_0(N)$ consisting of the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a \equiv d \equiv 1 \bmod N$. Let $u : X_1(N) \to X_0(N)$ be the holomorphic map deduced from the identity on $\overline{\mathcal{H}}$ by passing to the quotients.

*This research was financially supported by the National University of Singapore Overseas Graduate Scholarship. The author wishes to thank Ken Ribet for helpful discussion.

†This work was completed while the author was a visiting professor at the Miller Institute for Basic Research in Science in Berkeley.

Let $J_0(N)$ and $J_1(N)$ be the Jacobian varieties of $X_0(N)$ and $X_1(N)$, viewed as the connected components of 0 in the corresponding Picard varieties. Let

$$u^* : J_0(N) \longrightarrow J_1(N)$$

be the morphism of abelian varieties deduced from u by Picard functoriality. Its kernel, called the *Shimura subgroup* of $J_0(N)$, is a finite group; we denote it by $\Sigma(N)$.

In this paper, we give a complete description of $\Sigma(N)$: group structure, exponent, order, action of Galois, of Atkin-Lehner involutions and of Hecke operators (including those associated to the primes dividing N), behaviour under degeneracy maps, etc. This extends previous results obtained by B. Mazur ([3], II, 11) and K. Ribet ([5]). Our proofs are of complex analytic nature and would apply in situations where $\Gamma_0(N)$ and $\Gamma_1(N)$ are replaced by discrete subgroups of $SL_2(\mathbf{R})$ of finite covolume, even when the corresponding Riemann surfaces have no modular interpretation.

Let $\mathbf{U}$ be the group of complex numbers of modulus 1. We define in §1 a canonical injective group homomorphism

$$\psi : J_0(N) \longrightarrow \mathrm{Hom}(\Gamma_0(N), \mathbf{U}). \tag{1}$$

Throughout the paper, we identify the group $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma_1(N) \mapsto d + N\mathbf{Z}.$$

We show that an element x of $J_0(N)$ belongs to the Shimura subgroup $\Sigma(N)$ if and only if the kernel of $\psi(x)$ contains $\Gamma_1(N)$. Therefore, we deduce from ψ a canonical injective homomorphism

$$\psi' : \Sigma(N) \longrightarrow \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}). \tag{2}$$

We determine its image in §2 and obtain:

THEOREM 1 .— *The Shimura subgroup $\Sigma(N)$ of $J_0(N)$ is canonically isomorphic to the group of homomorphisms $g : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{U}$ such that $g(d) = 1$ if $d = -1$, $d^2 + 1 = 0$, $d^2 + d + 1 = 0$ or $(d-1)^2 = 0$.*

By using thm. 1, we compute in §3 the order and the exponent of the group $\Sigma(N)$:

COROLLARY 1 .— *Let $\phi(N)$ denote the number of elements of $(\mathbf{Z}/N\mathbf{Z})^\times$ and:*

(i) let m be the largest integer such that m^2 divides N;

(ii) let k be the number of prime divisors of N distinct from 2 and 3;

(iii) let m_2 be equal to 2 if -1 is a square mod N *(i.e., if $4 \nmid N$ and each prime factor $p \neq 2$ of N is congruent to* 1 mod 4*), and let m_2 be equal to* 1 *otherwise;*

(iv) let m_3 be equal to 3 if X^2+X+1 has a root mod N *(i.e., if $9 \nmid N$ and each prime factor $p \neq 3$ of N is congruent to* 1 mod 3*), and let m_3 be equal to* 1 *otherwise.*

Then we have

$$\mathrm{Card}(\Sigma(N)) = \begin{cases} \phi(N)/(2mm_2^k m_3^k) & \text{if } N \geq 5 \\ 1 & \text{if } N \leq 4. \end{cases}$$

EXAMPLE.— If N is of the form p^n, with p a prime number and $n \geq 1$, then $\Sigma(N)$ is a cyclic group (thm. 1). If $p \neq 2$, its order is the product of $p^{n-1-[n/2]}$ and the numerator of $\frac{p-1}{12}$; if $p = 2$, its order is $2^{\max(0,n-2-[n/2])}$.

COROLLARY 2 .— *Let $N = \prod p^{r_p}$ be the prime power decomposition of N and:*

(i) let r'_p be equal to $r_p - 1 - [r_p/2]$ if $p \neq 2$;

(ii) let r'_2 be equal to $\max(0, r_2 - 2 - [r_2/2])$;

(iii) let e_0 be equal to $\operatorname{lcm}_{p|N}((p-1)p^{r'_p})$;

(iv) let m_1 be equal to 2 if N is the product of 1, 2 *or* 4 *by a power of an odd prime, and let m_1 be equal to* 1 *otherwise;*

(v) let m_2 and m_3 be as in cor. 1.

Then the exponent of the group $\Sigma(N)$ (i.e., the smallest integer e such that $e\Sigma(N) = 0$) is given by

$$e = \begin{cases} e_0/(m_1 m_2 m_3) & \text{if } N \geq 5 \\ 1 & \text{if } N \leq 4. \end{cases}$$

COROLLARY 3 .— *The only integers N for which the order of $\Sigma(N)$ is* 1 *are* 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25, 36, 49, 50 *and* 169.

In fact, for all these values of N except 36, 49, 50 and 169, the genus of the Riemann surface $X_0(N)$ is 0 and we therefore have $J_0(N) = 0$.

COROLLARY 4 .— *When N approaches infinity, the exponent and a fortiori the order of $\Sigma(N)$ go to infinity.*

The Riemann surface $X_0(N)$ is the group of complex points of a modular curve $X_0(N)_{\mathbf{Q}}$ defined over $\mathbf{Q}$. Therefore, $J_0(N)$ is naturally defined over $\mathbf{Q}$ and the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, where $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, acts on the group of torsion points of $J_0(N)$. It acts, in particular, on the Shimura subgroup $\Sigma(N)$. We determine this action in §4, and obtain:

THEOREM 2 .— *Let e be the exponent of the group $\Sigma(N)$ (see* cor. 2 *of* thm. 1*). The smallest common field of definition of the points of $\Sigma(N)$ is the cyclotomic field $\mathbf{Q}(\mu_e)$. The Galois group $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q})$ acts on $\Sigma(N)$ via the cyclotomic character $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q}) \to (\mathbf{Z}/e\mathbf{Z})^\times$.*

COROLLARY 1 .— *A point x of $\Sigma(N)$ is rational over $\mathbf{Q}$ if and only if we have $2x = 0$. The number of those points is $2^{\mathrm{Card}(P)+\epsilon}$, where P is the set of odd primes dividing N and ϵ is given by*

$$\epsilon = \begin{cases} -1 & \text{if } 4 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 8; \\ -1 & \text{if } 4 \mid N,\ 8 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 4; \\ 1 & \text{if } 32 \mid N; \\ 0 & \text{otherwise.} \end{cases}$$

COROLLARY 2 .— *The only integers N for which all points of $\Sigma(N)$ are rational over $\mathbf{Q}$ are:*

(i) those for which $\Sigma(N)$ is of order 1, *listed in* cor. 3 *of* thm. 1*;*

(ii) the integers 20, 21, 24, 32, 48, 64, 72, 100, 144 *and* 147, *for which $\Sigma(N)$ is of order* 2*;*

(iii) the integers 96, 192, 288 *and* 576, *for which $\Sigma(N)$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$.*

To each divisor N_1 of N, such that N_1 is prime to N/N_1, is associated an *Atkin-Lehner involution* w_{N_1} of $X_0(N)$: for the definition, see §5. The involutions ${w_{N_1}}^*$ and $(w_{N_1})_*$ of $J_0(N)$ deduced by Picard and Albanese functorialities respectively coincide. The behaviour of the Shimura subgroup of $J_0(N)$ under these maps is studied in §5. We obtain:

THEOREM 3 .— *The Shimura subgroup $\Sigma(N)$ of $J_0(N)$ is stable under ${w_{N_1}}^*$. Moreover, we have the commutative diagram*

$$\begin{array}{ccc} \Sigma(N) & \xrightarrow{\psi'} & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}) \\ \alpha \downarrow & & {}^t\alpha' \downarrow \\ \Sigma(N) & \xrightarrow{\psi'} & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}), \end{array} \tag{3}$$

where α is the map induced by ${w_{N_1}}^*$, ψ' is the canonical injection (2), *and ${}^t\alpha'$ is the transpose of the involution $\alpha' : (\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/N\mathbf{Z})^\times$ which coincides with $t \mapsto t^{-1}$ modulo N_1 and with the identity modulo N/N_1.*

The following particular case of thm. 3 was previously obtained by K. Ribet ([5], lemma 1):

COROLLARY .— *The involution ${w_N}^*$ acts on the Shimura subgroup $\Sigma(N)$ by multiplication by -1.*

Let M be a divisor of N. For each divisor D of N/M, we have a holomorphic degeneracy map $v_D : X_0(N) \to X_0(M)$. It is the map deduced from the transformation $\tau \mapsto D\tau$ of $\overline{\mathcal{H}}$ by passing to the quotients; a modular definition of v_D is given in §6. By Picard and Albanese functorialities respectively, we get morphisms of abelian varieties

$$\begin{aligned} {v_D}^* &: J_0(M) \longrightarrow J_0(N), \\ (v_D)_* &: J_0(N) \longrightarrow J_0(M), \end{aligned} \tag{4}$$

the latter being the dual of the former. The behaviour of the Shimura subgroups under these maps is studied in §6. We obtain:

THEOREM 4 .— *We have ${v_D}^*(\Sigma(M)) \subseteq \Sigma(N)$. Moreover, we have the commutative diagram*

$$\begin{array}{ccc} \Sigma(M) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/M\mathbf{Z})^\times, \mathbf{U}) \\ \beta \downarrow & & {}^t\beta' \downarrow \\ \Sigma(N) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}), \end{array} \tag{5}$$

where β is the map induced by ${v_D}^*$, the horizontal arrows represent the canonical injections (2), *and ${}^t\beta'$ is the transpose of the canonical surjection $\beta' : (\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/M\mathbf{Z})^\times$.*

THEOREM 5 .— *We have $(v_D)_*(\Sigma(N)) \subseteq \Sigma(M)$. Moreover, we have the commutative diagram*

$$\begin{array}{ccc} \Sigma(N) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}) \\ \delta \downarrow & & {}^t\delta' \downarrow \\ \Sigma(M) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/M\mathbf{Z})^\times, \mathbf{U}), \end{array} \tag{6}$$

where δ is the map induced by $(v_D)_*$, the horizontal arrows represent the canonical injections (2), *and ${}^t\delta'$ is the transpose of the homomorphism*

$\delta' : (\mathbf{Z}/M\mathbf{Z})^\times \to (\mathbf{Z}/N\mathbf{Z})^\times$ *defined in the following way: we write* $N = N_1N_2$ *with* N_2 *the greatest divisor of* N *prime to* M*; if* d *is an integer prime to* M*, then* $\delta'(d + M\mathbf{Z})$ *is the class of the integers congruent to* 1 mod N_2 *and to* $d^{[\Gamma_0(M):\Gamma_0(N)]}$ mod N_1.

REMARK. — Theorems 4 and 5 imply that the map $\beta : \Sigma(M) \to \Sigma(N)$ induced by ${v_D}^*$ and the map $\delta : \Sigma(N) \to \Sigma(M)$ induced by $(v_D)_*$ are independent of the divisor D of N/M.

To each prime number p is associated a *Hecke correspondence* T_p on $X_0(N)$. If $[\tau]$ denotes the image in $X_0(N)$ of an element τ of $\overline{\mathcal{H}}$, then T_p is defined by

$$[\tau] \mapsto [p\tau] + \sum_{0 \le i \le p-1} [\tfrac{\tau+i}{p}] \qquad \text{if } p \nmid N,$$

$$[\tau] \mapsto \sum_{0 \le i \le p-1} [\tfrac{\tau+i}{p}] \qquad \text{if } p|N.$$

To these correspondences are associated (by suitably generalising Picard and Albanese functorialities) endomorphisms ${T_p}^*$ and $(T_p)_*$ of $J_0(N)$: for the precise definitions, see §7. One has ${T_p}^* = (T_p)_*$ when $p \nmid N$, but not necessarily so when $p|N$.

THEOREM 6 .— *Both the endomorphisms* ${T_p}^*$ *and* $(T_p)_*$ *stabilise the Shimura subgroup* $\Sigma(N)$ *of* $J_0(N)$ *and, on* $\Sigma(N)$*, they coincide with multiplication by* $p + 1$ *if* $p \nmid N$*, and with multiplication by* p *if* $p|N$.

REMARKS.— 1) Theorem 6 was first proved by B. Mazur when N is a prime not equal to p ([3], II, 11.7), then by K. Ribet when p does not divide N([5], thm. 1). For p not dividing eN, where e is the exponent of $\Sigma(N)$, thm. 6 could also be deduced from thm. 2 by using the Eichler-Shimura congruences (see [3], p.89).

2) Theorem 6 can be generalised to the Hecke correspondences T_n, where $n \ge 1$ is not necessarily a prime (see §7): then ${T_n}^*$ and $(T_n)_*$ coincide on $\Sigma(N)$ with multiplication by $a_N(n)$, where $a_N(n)$ denotes the sum of the divisors d of n satisfying the condition $\gcd(N, \frac{n}{d}) = 1$.

1 Some results on Riemann surfaces and their Jacobian varieties

Let X be a compact connected non-empty Riemann surface.

1.1 The Jacobian variety

We shall view the Jacobian variety $J(X)$ of X as the connected component of 0 in the Picard variety of X: it parametrises the isomorphism classes of holomorphic line bundles of degree 0 on X.

1.2 The Albanese variety

The Albanese variety $\mathrm{Alb}(X)$ of X parametrises the classes, modulo principal divisors, of divisors of degree 0 on X. We have a canonical isomorphism $J(X) \to \mathrm{Alb}(X)$: to the class of a holomorphic line bundle of degree 0 corresponds the class of the divisors of its meromorphic sections.

1.3 The group isomorphism $J(X) \to \mathbf{Hom}(H_1(X, \mathbf{Z}), \mathbf{U})$

Let $\mathbf{U}$ be the group of complex numbers of modulus 1 and let $\underline{\mathbf{U}}$ be the sheaf on X of locally constant functions with values in $\mathbf{U}$. The group homomorphism $H^1(X, \underline{\mathbf{U}}) \to H^1(X, \mathcal{O}_X^\times)$ deduced from the injection $\underline{\mathbf{U}} \to \mathcal{O}_X^\times$ defines, when $H^1(X, \mathcal{O}_X^\times)$ is identified with the Picard group of X, a group isomorphism

$$H^1(X, \underline{\mathbf{U}}) \longrightarrow J(X). \tag{7}$$

(This is proved by comparing the exact sequences in Čech cohomology associated to $0 \to \underline{\mathbf{Z}} \to \underline{\mathbf{R}} \to \underline{\mathbf{U}} \to 0$ and $0 \to \underline{\mathbf{Z}} \to \mathcal{O}_X \to \mathcal{O}_X^\times \to 0$; see [4], p.316-05)

We can restate this result as follows:

PROPOSITION 1 .— *Let L be a holomorphic line bundle of degree 0 on X. There exists a principal covering E of the topological space X, with structure group $\mathbf{U}$ (viewed as a discrete group), such that L is isomorphic to the associated holomorphic line bundle $E \times_{\mathbf{U}} \mathbf{C}$. Furthermore, L determines E up to isomorphism.*

We recall that $E \times_{\mathbf{U}} \mathbf{C}$ denotes the quotient of $E \times \mathbf{C}$ by the equivalence relation which identifies $(y, \lambda\mu)$ with $(y\lambda, \mu)$ for $y \in E$, $\lambda \in \mathbf{U}$, $\mu \in \mathbf{C}$. The image of (y, μ) in $E \times_{\mathbf{U}} \mathbf{C}$ will be denoted by $[y, \mu]$.

Let $H_1(X, \mathbf{Z})$ be the first singular homology group of X with coefficients in $\mathbf{Z}$. We shall now deduce from (7) a canonical group isomorphism

$$\phi : J(X) \longrightarrow \mathrm{Hom}(H_1(X, \mathbf{Z}), \mathbf{U}). \tag{8}$$

Let L be a holomorphic line bundle of degree 0 on X and $[L]$ its class in $J(X)$. Let E be as in prop. 1, and let x be a point of X. Since $\pi_1(X,x)^{\mathrm{ab}}$ is canonically isomorphic to $H_1(X,\mathbf{Z})$, the monodromy map $\pi_1(X,x) \to \mathbf{U}$ of the principal covering E factorises through a homomorphism $H_1(X,\mathbf{Z}) \to \mathbf{U}$. This homomorphism depends only on $[L]$ and is, by definition, $\phi([L])$. The fact that ϕ is an isomorphism is seen by combining isomorphism (7) with the comparison between Čech cohomology and singular cohomology. (Remark: In fact, ϕ is an isomorphism of real Lie groups.)

We shall now give an explicit description of the group isomorphism

$$\phi' : \mathrm{Alb}(X) \longrightarrow \mathrm{Hom}(H_1(X,\mathbf{Z}),\mathbf{U}) \tag{9}$$

obtained by composing ϕ with the canonical isomorphism $\mathrm{Alb}(X) \to J(X)$ (see 1.2).

PROPOSITION 2 .— *Let $D = \sum n_i P_i$ be a divisor of degree 0 on X. There exists a unique meromorphic differential form ω_D on X satisfying the two following conditions:*

(i) The only poles of ω_D are simple poles at the points P_i, with residues n_i;

(ii) For each singular 1-cycle c on X, with support disjoint from the support of D, the real part of $\int_c \omega_D$ is 0.

Let $[D]$ denote the class of D in $\mathrm{Alb}(X)$, and for c as in (ii), let $[c]$ denote the class of c in $H_1(X,\mathbf{Z})$. We then have

$$\phi'([D])([c]) = \exp(-\int_c \omega_D). \tag{10}$$

The existence of a meromorphic differential form on X satisfying condition (i) is a consequence of Riemann-Roch theorem. Such a form is unique up to addition of a holomorphic differential form on X, and the $\mathbf{R}$-linear map $H^0(X,\Omega^1) \to \mathrm{Hom}(H_1(X,\mathbf{Z}),\mathbf{R})$ defined by $\omega \mapsto ([c] \mapsto \mathrm{Re}(\int_c \omega))$ is known to be bijective. This establishes the existence and the uniqueness of ω_D.

We consider now a holomorphic line bundle L of degree 0 on X having a meromorphic section s with divisor D. Let E be as in prop. 1. We identify L with $E \times_{\mathbf{U}} \mathbf{C}$. We define a meromorphic differential form ω on X as follows: locally, s can be written as $[h,f]$, with h a continuous section of E and f a meromorphic function, and ω is given by $\omega = df/f$. The form

ω satisfies condition (i) of prop. 2. Let c be a singular 1-cycle on X with support disjoint from the support of D. We shall prove the equality

$$\phi([L])([c]) = \exp(-\int_c \omega). \tag{11}$$

It implies that ω satisfies condition (ii) of prop. 2, hence is equal to ω_D, and (10) follows because $[L]$ corresponds to $[D]$ by the canonical isomorphism $J(X) \to \mathrm{Alb}(X)$. By the residue theorem, the right hand side of (11) depends only on the homology class $[c]$ of c, and it is sufficient to prove (11) when c is a smooth loop. Let $\tilde{c} : [0,1] \to E$ be a path which lifts c. By definition, $\phi([L])([c])$ is the complex number $\lambda \in \mathbf{U}$ such that $\tilde{c}(1) = \tilde{c}(0)\lambda$. We can write $s \circ c$ as $t \mapsto [\tilde{c}(t), f(t)]$ with $f : [0,1] \to \mathbf{C}$ a smooth function and we have, by definition of ω,

$$\exp(-\int_c \omega) = \exp(-\int_0^1 \frac{f'}{f}(t)dt) = \frac{f(0)}{f(1)}.$$

Finally, the equalities $[\tilde{c}(0), f(0)] = s(c(0)) = s(c(1)) = [\tilde{c}(1), f(1)] = [\tilde{c}(0)\lambda, f(1)] = [\tilde{c}(0), \lambda f(1)]$ imply $f(0) = \lambda f(1)$ and this completes the proof.

1.4 Picard and Albanese functorialities

Let Y be a second compact connected Riemann surface, let $f : X \to Y$ be a non-constant holomorphic map and let n be its degree.

To f are associated two morphisms of abelian varieties

$$f^* : \mathrm{Alb}(Y) \to \mathrm{Alb}(X) \quad \text{and} \quad f_* : \mathrm{Alb}(X) \to \mathrm{Alb}(Y).$$

The morphism f^* sends the class of a divisor of degree 0 on Y to the class of its inverse image under f; the morphism f_* sends the class of a divisor of degree 0 on X to the class of its image under f. The map $f_* \circ f^*$ coincides with multiplication by n in $\mathrm{Alb}(Y)$. The kernel of f^* is therefore finite.

Via the canonical isomorphisms between Albanese and Jacobian varieties (see 1.2), we can view the previous maps as morphisms of abelian varieties

$$f^* : J(Y) \to J(X) \quad \text{and} \quad f_* : J(X) \to J(Y).$$

The morphism f^* sends the class of a line bundle L of degree 0 on Y to the class of its pullback $X \times_Y L$. The morphism f_* sends the class of a

line bundle L' of degree 0 on X to the class of its norm $N_{X/Y}L'$ (for the definition of this line bundle in the language of invertible sheaves, see [1], 6.5); this description of f_* will not be used in this paper. We shall say that f^* is deduced from f by Picard functoriality and that f_* is deduced from f by Albanese functoriality.

By taking images by f and inverse images by f of singular 1-cycles, one also defines two group homomorphisms

$$f_* : H_1(X, \mathbf{Z}) \to H_1(Y, \mathbf{Z}) \quad \text{and} \quad f^* : H_1(Y, \mathbf{Z}) \to H_1(X, \mathbf{Z}).$$

We claim that the two diagrams

$$\begin{array}{ccc} J(Y) & \longrightarrow & \mathrm{Hom}(H_1(Y, \mathbf{Z}), \mathbf{U}) \\ f^* \downarrow & & \downarrow {}^t f_* \\ J(X) & \longrightarrow & \mathrm{Hom}(H_1(X, \mathbf{Z}), \mathbf{U}) \end{array} \tag{12}$$

and

$$\begin{array}{ccc} J(X) & \longrightarrow & \mathrm{Hom}(H_1(X, \mathbf{Z}), \mathbf{U}) \\ f_* \downarrow & & \downarrow {}^t f^* \\ J(Y) & \longrightarrow & \mathrm{Hom}(H_1(Y, \mathbf{Z}), \mathbf{U}), \end{array} \tag{13}$$

where the horizontal arrows represent the canonical isomorphisms (8), are commutative. The commutativity of (12) follows immediately from the definitions. The commutativity of (13) is seen more easily by considering Albanese varieties. Let D be a divisor of degree 0 on X and ω_D the corresponding meromorphic differential form (see prop. 2). The trace $\omega = Tr_{X/Y}(\omega_D)$ of ω_D is a meromorphic differential form on Y; it satisfies condition (i) of prop. 2 with respect to the image $f(D)$ of the divisor D on Y, and we have $\int_c \omega = \int_{f^{-1}c} \omega_D$ for each singular 1-cycle c on Y, with support disjoint from the support of $f(D)$. This first implies that ω is equal to $\omega_{f(D)}$ and then implies the commutativity of (13) by formula (10).

REMARK.— Let $g : Z \to Y$ be the maximal abelian unramified covering of the Riemann surface Y through which f factorises, and let A denote its Galois group. Let x be a point of X. By monodromy, A is isomorphic to the largest abelian quotient of $\pi_1(Y, f(x))$ to which $\pi_1(X, x)$ maps to 0, i.e., A is isomorphic to the cokernel of $f_* : H_1(X, \mathbf{Z}) \to H_1(Y, \mathbf{Z})$. This latter isomorphism does not depend on x. We deduce from it, by using the commutative diagram (12), a canonical isomorphism $\eta : \Sigma \to \mathrm{Hom}(A, \mathbf{U})$, where Σ denotes the kernel of $f^* : J(Y) \to J(X)$. If χ is an element of

$\mathrm{Hom}(A, \mathbf{U})$, $\eta^{-1}(\chi)$ is described explicitly as follows: it is the isomorphism class of the line bundle $Z \times_A \mathbf{C}$ associated to the covering Z and to the action $(a, \lambda) \mapsto \chi(a)\lambda$ of A on $\mathbf{C}$.

1.5 The case of modular curves

Let Γ be a subgroup of $SL_2(\mathbf{Z})$ of finite index. Let X denote the Riemann surface $\Gamma\backslash\overline{\mathcal{H}}$ and $p : \overline{\mathcal{H}} \to X$ the canonical surjection. For each point $\tau \in \overline{\mathcal{H}}$, there is a group homomorphism

$$\Gamma \longrightarrow \pi_1(X, p(\tau)) \tag{14}$$

characterised by the following property: if γ is an element of Γ and c a continuous path in $\overline{\mathcal{H}}$ connecting τ to $\gamma\tau$, the image of γ by the homomorphism (14) is the (strict) homotopy class of the loop $p \circ c$. The homomorphism (14) is surjective and its kernel is the subgroup of Γ generated by the elements fixing at least one point in $\overline{\mathcal{H}}$, i.e., those whose trace t satisfies $|t| \leq 2$ ([7], p.5). Since $\pi_1(X, p(\tau))^{\mathrm{ab}}$ is canonically isomorphic to $H_1(X, \mathbf{Z})$, we deduce from (14) a surjective homomorphism

$$\Gamma \longrightarrow H_1(X, \mathbf{Z}). \tag{15}$$

This homomorphism does not depend on τ.

Let $J(X)$ denote the Jacobian variety of X. By composing the transpose of the isomorphism (15) with the isomorphism (8) of 1.3, we get a canonical injective group homomorphism

$$\psi_\Gamma : J(X) \longrightarrow \mathrm{Hom}(\Gamma, \mathbf{U}). \tag{16}$$

A homomorphism $\Gamma \to \mathbf{U}$ belongs to the image of ψ_Γ if and only if its kernel contains the elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ such that $|a + d| \leq 2$.

Let Γ' be a second subgroup of $SL_2(\mathbf{Z})$ of finite index and X' the Riemann surface $\Gamma'\backslash\overline{\mathcal{H}}$. We first assume that there exists a matrix $g \in GL_2^+(\mathbf{R})$ such that $g\Gamma' g^{-1} \subseteq \Gamma$. Let g be such a matrix. By passing to the quotients, we deduce from the transformation $\tau \mapsto g\tau$ of $\overline{\mathcal{H}}$ a holomorphic map $w : X' \to X$ and hence, by Picard functoriality, a morphism $w^* : J(X) \to J(X')$ of abelian varieties. Let $v : \Gamma' \to \Gamma$ denote the homomorphism $\gamma \mapsto g\gamma g^{-1}$ from Γ' to Γ.

PROPOSITION 3 .— *The diagram*

$$\begin{array}{ccc} J(X) & \xrightarrow{\psi_\Gamma} & \mathrm{Hom}(\Gamma, \mathbf{U}) \\ w^* \downarrow & & \downarrow {}^t v \\ J(X') & \xrightarrow{\psi_{\Gamma'}} & \mathrm{Hom}(\Gamma', \mathbf{U}) \end{array}$$

is commutative.

This follows from the commutativity of the diagram (12) and that of the diagram

$$\begin{array}{ccc} \Gamma' & \longrightarrow & H_1(X', \mathbf{Z}) \\ v \downarrow & & \downarrow w_* \\ \Gamma & \longrightarrow & H_1(X, \mathbf{Z}). \end{array}$$

We now assume that Γ' is contained in Γ. We denote by $u : X' \to X$ the holomorphic map deduced from the identity on $\overline{\mathcal{H}}$ by passing to the quotients, and by $u_* : J(X') \to J(X)$ the morphism of abelian varieties deduced from u by Albanese functoriality. Since Γ' is of finite index in Γ, we have a transfer homomorphism (see [2], p.202)

$$V : \Gamma^{\mathrm{ab}} \longrightarrow \Gamma'^{\mathrm{ab}}.$$

We recall its definition: if $S \subseteq \Gamma$ is a system of representatives of $\Gamma' \backslash \Gamma$, and if γ is an element of Γ, there exist a permutation σ of S and, for each $s \in S$, an element $a_{s,\gamma}$ of Γ' such that $s\gamma = a_{s,\gamma}\sigma(s)$. Let $\overline{\gamma}$ denote the image of γ in Γ^{ab} and $\overline{a_{s,\gamma}}$ the image of $a_{s,\gamma}$ in Γ'^{ab}. The product $\prod_{s \in S} \overline{a_{s,\gamma}}$ depends only on $\overline{\gamma}$ (and not on the choice of the system of representatives S) and is equal to $V(\overline{\gamma})$.

PROPOSITION 4 .— *The diagram*

$$\begin{array}{ccccc} J(X') & \xrightarrow{\psi_{\Gamma'}} & \mathrm{Hom}(\Gamma', \mathbf{U}) & = & \mathrm{Hom}(\Gamma'^{\mathrm{ab}}, \mathbf{U}) \\ u_* \downarrow & & & & \downarrow {}^t V \\ J(X) & \xrightarrow{\psi_\Gamma} & \mathrm{Hom}(\Gamma, \mathbf{U}) & = & \mathrm{Hom}(\Gamma^{\mathrm{ab}}, \mathbf{U}) \end{array}$$

is commutative.

We shall prove that the diagram

$$\begin{array}{ccc} \Gamma^{ab} & \xrightarrow{\eta} & H_1(X, \mathbf{Z}) \\ V \downarrow & & \downarrow u^* \\ \Gamma'^{ab} & \xrightarrow{\eta'} & H_1(X', \mathbf{Z}), \end{array} \tag{17}$$

where η, η' are deduced from (15) by passing to the quotients, is commutative. Prop. 4 will then follow from the commutativity of the diagram (13) of 1.4. Let γ be an element of Γ and let $\overline{\gamma}$, S, σ, $a_{s,\gamma}$ and $\overline{a_{s,\gamma}}$ be as introduced before prop. 4. Let τ be a point in $\overline{\mathcal{H}}$, c a continuous path in $\overline{\mathcal{H}}$ connecting τ to $\gamma\tau$ and $q : \overline{\mathcal{H}} \to X'$ the canonical surjection. For each $s \in S$, let c_s be a continuous path in $\overline{\mathcal{H}}$ connecting τ to $s\tau$. By definition of η and u^*, we have

$$u^*(\eta(\overline{\gamma})) = \sum_{s \in S} [q \circ (sc)],$$

where sc denotes the path $t \mapsto sc(t)$ in $\overline{\mathcal{H}}$. As σ is a permutation of S, we can write

$$u^*(\eta(\overline{\gamma})) = \sum_{s \in S} ([q \circ c_s] + [q \circ (sc)] - [q \circ (c_{\sigma(s)})]).$$

We have $q \circ c_{\sigma(s)} = q \circ (a_{s,\gamma} c_{\sigma(s)})$ and the path composed of c_s, of sc and of the inverse of the path $a_{s,\gamma} c_{\sigma(s)}$ connects τ to $a_{s,\gamma}\tau$; we have, therefore,

$$[q \circ (c_s)] + [q \circ (sc)] - [q \circ (c_{\sigma(s)})] = \eta'(\overline{a_{s,\gamma}})$$

in $H_1(X', \mathbf{Z})$ for each $s \in S$, and

$$u^*(\eta(\overline{\gamma})) = \sum_{s \in S} \eta'(\overline{a}_{s,\gamma}) = \eta'(V(\overline{\gamma})).$$

This proves the commutativity of (17).

2 The group structure of $\Sigma(N)$

2.1 The holomorphic map $u : X_1(N) \longrightarrow X_0(N)$

As in the introduction, $u : X_1(N) \to X_0(N)$ denotes the holomorphic map deduced from the identity on $\overline{\mathcal{H}}$ by passing to the quotients.

The group $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. Therefore, one deduces from the action of $\Gamma_0(N)$ on $\overline{\mathcal{H}}$ an action of $\Gamma_0(N)$ on $X_1(N)$. The group

$\Gamma_1(N)$ and the matrix -1 act trivially on $X_1(N)$, hence we have an action of the group

$$G = \Gamma_0(N)/\{-1,1\}\Gamma_1(N) \simeq (\mathbf{Z}/N\mathbf{Z})^\times/\{-1,1\}$$

on $X_1(N)$. The holomorphic map $u : X_1(N) \to X_0(N)$ is a Galois ramified covering with Galois group G.

REMARK (Modular interpretation).— The Riemann surface $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ parametrises the isomorphism classes of pairs (E, C), where E is an elliptic curve over $\mathbf{C}$ and C a cyclic subgroup of E of order N: to the class mod $\Gamma_0(N)$ of a point $\tau \in \mathcal{H}$ corresponds the class of the pair (E_τ, C_τ), where $E_\tau = \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and C_τ is the subgroup of E_τ generated by the image of $\frac{1}{N}$. Similarly, $Y_1(N) = \Gamma_1(N)\backslash\mathcal{H}$ parametrises the isomorphism classes of pairs (E, P), where E is an elliptic curve over $\mathbf{C}$ and P a point of E of exact order N: to the class mod $\Gamma_1(N)$ of a point $\tau \in \mathcal{H}$ corresponds the class of the pair (E_τ, P_τ), where $E_\tau = \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and P_τ is the image of $\frac{1}{N}$ in E_τ. The map $Y_1(N) \to Y_0(N)$ induced by u has the following modular interpretation: it sends the class $[E, P]$ to the class $[E, \langle P\rangle]$, where $\langle P\rangle$ is the cyclic subgroup of E generated by P. The action of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ on $X_1(N)$ induces on $Y_1(N)$ the transformation given in modular terms by $[E, P] \mapsto [E, dP]$. (Note that the class $[E, -P]$ is always equal to the class $[E, P]$.) This modular interpretation of the action of G explains why we prefer to identify $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$ by using d instead of a.

2.2 Proof of theorem 1

We have defined in 1.5, formula (16), a canonical injective group homomorphism

$$\psi : J_0(N) \longrightarrow \mathrm{Hom}(\Gamma_0(N), \mathbf{U}). \tag{18}$$

Prop. 3, applied with $\Gamma = \Gamma_0(N)$, $\Gamma' = \Gamma_1(N)$ and $g = 1$ implies that an element $x \in J_0(N)$ belongs to the Shimura subgroup $\Sigma(N)$ if and only if the kernel of $\psi(x)$ contains $\Gamma_1(N)$. By identifying $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$, we therefore deduce from ψ a canonical injective homomorphism

$$\psi' : \Sigma(N) \longrightarrow \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}). \tag{19}$$

A homomorphism $h : \Gamma_0(N) \to \mathbf{U}$ belongs to the image of ψ if and only if its kernel contains the set $S = \{\gamma \in \Gamma_0(N) | |Tr(\gamma)| \leq 2\}$ (see 1.5). This set consists of the matrices of the form $\begin{pmatrix} t-d & b \\ Nc & d \end{pmatrix}$, with b, c, d in $\mathbf{Z}$, $t \in \{-2, -1, 0, 1, 2\}$ and $d(t-d) - Nbc = 1$. Its image S' under the canonical surjection $\Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^\times$ ($\simeq \Gamma_0(N)/\Gamma_1(N)$) consists of the roots in $\mathbf{Z}/N\mathbf{Z}$ of the polynomials $X^2 - tX + 1$, for $t \in \{-2, -1, 0, 1, 2\}$. A homomorphism $g : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{U}$ belongs to the image of ψ' if and only if its kernel contains S'. Since -1 belongs to S' and since the roots of $X^2 - tX + 1$ and $X^2 + tX + 1$ are interchanged by multiplication by -1, thm. 1 follows.

2.3 Group structure of $\Sigma(N)$

Let J denote the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by -1 and the roots in $\mathbf{Z}/N\mathbf{Z}$ of the polynomials X^2+1, X^2+X+1 and $(X-1)^2$. The dual of the finite abelian group $\Sigma(N)$ is canonically isomorphic to $(\mathbf{Z}/N\mathbf{Z})^\times/J$ (thm. 1). We shall describe explicitly the latter group in this section. First, we recall some notations introduced in cor. 1 of thm. 1:

(i) Let m denote the largest integer such that m^2 divides N.

(ii) Let m_2 be equal to 2 if -1 is a square mod N (i.e., if $4 \nmid N$ and each prime factor $p \neq 2$ of N is congruent to 1 mod 4), and let m_2 be equal to 1 otherwise.

(iii) Let m_3 be equal to 3 if $X^2 + X + 1$ has a root mod N (i.e., if $9 \nmid N$ and each prime factor $p \neq 3$ of N is congruent to 1 mod 3), and let m_3 be equal to 1 otherwise.

LEMMA 1 .— *The set of roots of $(X-1)^2$ in $\mathbf{Z}/N\mathbf{Z}$ is the kernel of the canonical surjection $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/(N/m)\mathbf{Z})^\times$; it is contained in J.*

By the definition of m, an element of $\mathbf{Z}/N\mathbf{Z}$ has square 0 if and only if it is congruent to 0 mod N/m. This proves the first assertion. The second assertion follows from the definition of J.

Let J' denote the image of J in $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$. By lemma 1, the canonical map

$$(\mathbf{Z}/N\mathbf{Z})^\times/J \longrightarrow (\mathbf{Z}/(N/m)\mathbf{Z})^\times/J' \tag{20}$$

is bijective.

If p is an odd prime and $r \geq 1$ is an integer, the group $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is canonically isomorphic to $\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r-1}\mathbf{Z})$ (the class of $1+p$ mod $p^r\mathbf{Z}$ corresponds to $(1, 1+p^{r-1}\mathbf{Z})$). Let $N = \prod p^{r_p}$ be the prime power decomposition of N. By the Chinese remainder theorem, we get an isomorphism

$$(\mathbf{Z}/(N/m)\mathbf{Z})^\times \simeq (\mathbf{Z}/2^{r_2-[r_2/2]}\mathbf{Z})^\times \times \prod_{p|N, p\neq 2} (\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r'_p}\mathbf{Z})), \qquad (21)$$

where, for each prime factor $p \neq 2$ of N, r'_p denotes the integer $r_p - [r_p/2] - 1$. If a prime p distinct from 2 and 3 divides N, we have that $p \equiv 1$ mod $2m_2m_3$ by definition of m_2 and m_3, and the group $\mu_{m_2m_3}(\mathbf{F}_p)$ of m_2m_3-th roots of unity in $\mathbf{F}_p$ has order m_2m_3. We shall denote by J'' the subgroup of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ corresponding to $\prod_{p|N, p\notin\{2,3\}} \mu_{m_2m_3}(\mathbf{F}_p)$ via the isomorphism (21).

PROPOSITION 5 .— *Assume that N is different from 1, 2 and 4. The group J'' is a subgroup of index 2 of J'. If -1 is not a square* mod N, *then -1 belongs to $J' - J''$. If -1 is a square* mod N, *then any square root of -1 in $\mathbf{Z}/N\mathbf{Z}$ reduces modulo N/m to an element of $J' - J''$.*

By lemma 1, the group J' is the image under the canonical surjection $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/(N/m)\mathbf{Z})^\times$ of the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by -1 and the roots of X^2+1 and X^2+X+1.

As we have $N \neq 1, 2, 4$ by hypothesis, we have $N/m \geq 3$, and $-1 \neq 1$ in $\mathbf{Z}/(N/m)\mathbf{Z}$. This implies the two last assertions of prop. 5 because every element x of J'' satisfies $x^3 = 1$ when -1 is not a square mod N and satisfies $x^6 = 1$ when -1 is a square mod N.

Let $\mu_2(\mathbf{Z}/N\mathbf{Z})$ and $\mu_3(\mathbf{Z}/N\mathbf{Z})$ denote the groups of square roots and third roots of unity in $\mathbf{Z}/N\mathbf{Z}$ respectively. The proposition is now a consequence of the following two lemmas.

LEMMA 2 .— *Assume that there exists $a \in \mathbf{Z}/N\mathbf{Z}$ such that $a^2 + 1 = 0$. The subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by the roots of X^2+1 is equal to $\mu_2(\mathbf{Z}/N\mathbf{Z}) \cup \mu_2(\mathbf{Z}/N\mathbf{Z})a$; it contains -1. The reduction modulo N/m of $\mu_2(\mathbf{Z}/N\mathbf{Z})$ is the 2-torsion subgroup of J''.*

The roots of X^2+1 in $\mathbf{Z}/N\mathbf{Z}$ are the elements of $\mu_2(\mathbf{Z}/N\mathbf{Z})a$, and $a^2 = -1$ belongs to $\mu_2(\mathbf{Z}/N\mathbf{Z})$. This implies our first assertion. The existence of a square root of -1 mod N implies that N is divisible by neither 3 nor 4. The last assertion follows easily.

LEMMA 3 .— *Assume that* X^2+X+1 *has a root in* $\mathbf{Z}/N\mathbf{Z}$. *The subgroup of* $(\mathbf{Z}/N\mathbf{Z})^\times$ *generated by these roots is then equal to* $\mu_3(\mathbf{Z}/N\mathbf{Z})$ *and its reduction modulo* N/m *is the* 3*-torsion subgroup of* J''.

Our hypothesis implies that N is divisible by neither 2 nor 9; we may write N as N' or $3N'$, with N' prime to 6. When identifying $(\mathbf{Z}/N\mathbf{Z})^\times$ with $\prod_{p|N}(\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r_p-1}\mathbf{Z}))$, the group $\mu_3(\mathbf{Z}/N\mathbf{Z})$ gets identified with $\prod_{p|N'}\mu_3(\mathbf{F}_p)$. The last assertion of the lemma follows. All roots of X^2+X+1 in $\mathbf{Z}/N\mathbf{Z}$ belong to $\mu_3(\mathbf{Z}/N\mathbf{Z})$. The group $\mu_3(\mathbf{Z}/N\mathbf{Z})$ is generated by the elements x such that $x \not\equiv 1 \bmod p$ for each prime divisor p of N'. For such an x, the relation $(x-1)(x^2+x+1) = x^3-1 = 0$ implies that $x^2+x+1 \equiv 0 \bmod N'$; furthermore, if 3 divides N, we have that $x \equiv 1 \bmod 3$ and hence $x^2+x+1 \equiv 1+1+1 \equiv 0 \bmod 3$. This shows that x is a root of X^2+X+1 in $\mathbf{Z}/N\mathbf{Z}$, and hence completes the proof.

The finite abelian group $\Sigma(N)$ is (non-canonically) isomorphic to its dual $(\mathbf{Z}/N\mathbf{Z})^\times/J$ and hence to $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/J'$ (see (20)). From the explicit description of J' given in prop. 5, and from (21), we deduce:

COROLLARY 1 .— *Assume that* -1 *is a square* mod N *and that* $N \neq 1, 2$. *Then* N *is of the form* N' *or* $2N'$, *with* $N' \neq 1$ *and each prime factor of* N' *congruent to* 1 mod $4m_3$. *The group* $\Sigma(N)$ *is isomorphic to the quotient of the group*

$$\prod_{p|N'}((\mathbf{Z}/\tfrac{p-1}{2m_3}\mathbf{Z}) \times (\mathbf{Z}/p^{r'_p}\mathbf{Z}))$$

by the unique subgroup of order 2 *which has a non-zero projection on each factor* $\mathbf{Z}/\frac{p-1}{2m_3}\mathbf{Z}$.

COROLLARY 2 .— *Assume that* -1 *is not a square* mod N. *Then the group* $\Sigma(N)$ *is isomorphic to* $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/(\{-1,1\}\mu_{m_3}(\mathbf{Z}/(N/m)\mathbf{Z}))$.

3 The order and the exponent of $\Sigma(N)$

In this section, the symbols $m, k, m_1, m_2, m_3, e_0, r_p$ and r'_p have the same meaning as in cor. 1 and cor. 2 of thm. 1.

3.1 The order of $\Sigma(N)$

If $N \leq 4$, the group $(\mathbf{Z}/N\mathbf{Z})^\times/\{-1,1\}$ has order 1 and hence $\Sigma(N)$ has order 1 (thm. 1).

Assume now that $N \geq 5$. In 2.3, we have defined an isomorphism between the dual of the finite abelian group $\Sigma(N)$ and the quotient of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ by a certain subgroup J'. Since m^2 divides N, the order of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ is $\phi(N)/m$, where ϕ denotes the Euler function. We have shown in prop. 5 that J' has a subgroup of index 2 which is of order $m_2^k m_3^k$. In conclusion, we have (for $N \geq 5$)

$$\operatorname{Card} \Sigma(N) = \phi(N)/(2mm_2^k m_3^k).$$

This proves cor. 1 of thm. 1.

3.2 The exponent of $\Sigma(N)$

Let e be the exponent of $\Sigma(N)$. If $N \leq 4$, then $\Sigma(N)$ has order 1 and we have $e = 1$. From now on, we assume that $N \geq 5$. We shall prove cor. 2 of thm. 1 by distinguishing between two cases:

a) *The case where* -1 *is a square* mod N *(i.e.,* $m_2 = 2$*)*

In this case, N is of the form N' or $2N'$, with $N' \neq 1$ and each prime factor of N' congruent to 1 mod $4m_3$, and $\Sigma(N)$ is isomorphic to the quotient of the group

$$A = \prod_{p|N'} ((\mathbf{Z}/\tfrac{p-1}{2m_3}\mathbf{Z}) \times (\mathbf{Z}/p^{r'_p}\mathbf{Z}))$$

by the unique subgroup of order 2 which has a non-zero projection on each factor $\mathbf{Z}/\frac{p-1}{2m_3}\mathbf{Z}$ (2.3, cor. 1 of prop. 5). The exponent of $\Sigma(N)$ is the same as that of A if N' has at least two prime divisors (i.e., if $m_1 = 1$), and is equal to that of A divided by 2 if N' has only one prime divisor (i.e., if $m_1 = 2$). As the exponent e_A of A is given by

$$e_A = \operatorname*{lcm}_{p|N'}\left(\frac{p-1}{2m_3}p^{r'_p}\right) = \frac{1}{2m_3}\operatorname*{lcm}_{p|N'}((p-1)p^{r'_p}) = \frac{e_0}{2m_3},$$

we have

$$e = e_A/m_1 = e_0/2m_1m_3 = e_0/m_1m_2m_3.$$

b) *The case where* -1 *is not a square* mod N *(i.e.,* $m_2 = 1$*)*

In this case, the group $\Sigma(N)$ is isomorphic to the quotient group $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/(\{-1,1\}\mu_{m_3}(\mathbf{Z}/(N/m)\mathbf{Z}))$ (2.3, cor. 2 of prop. 5). Its exponent e is equal to the exponent e' of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/\{-1,1\}$ divided by m_3.

We first assume that $r_2 \leq 2$. Then $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ is isomorphic to $\prod_{p|N,p\neq 2}(\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r'_p}\mathbf{Z}))$ and the exponent of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ is

$$\operatorname*{lcm}_{p|N,p\neq 2}((p-1)p^{r'_p}) = \operatorname*{lcm}_{p|N}((p-1)p^{r'_p}) = e_0.$$

The integer N has at least one odd prime divisor because we have assumed that $N \geq 5$; we have $e' = e_0$ if N has at least two such divisors (i.e., if $m_1 = 1$) and $e' = e_0/2$ if it has only one such divisor (i.e., if $m_1 = 2$). In conclusion, we have

$$e = e'/m_3 = e_0/m_1m_3 = e_0/m_1m_2m_3.$$

We now assume that $r_2 \geq 3$ (hence $m_1 = 1$). We have then an isomorphism (see 2.3, (21))

$$(\mathbf{Z}/(N/m)\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{r'_2}\mathbf{Z} \times \prod_{p|N,p\neq 2}(\mathbf{F}_p^\times \times \mathbf{Z}/p^{r'_p}\mathbf{Z})$$

such that the projection of -1 on the factor $\mathbf{Z}/2\mathbf{Z}$ is of order 2. The group $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/\{-1,1\}$ is hence isomorphic to $\mathbf{Z}/2^{r'_2}\mathbf{Z} \times \prod_{p|N,p\neq 2}(\mathbf{F}_p^\times \times \mathbf{Z}/p^{r'_p}\mathbf{Z})$ and its exponent e' is $\operatorname*{lcm}_{p|N}((p-1)p^{r'_p}) = e_0$. In conclusion, we have

$$e = e'/m_3 = e_0/m_3 = e_0/m_1m_2m_3.$$

3.3 Cases where the exponent of $\Sigma(N)$ is 1 or 2

Let $N \geq 1$ be an integer such that the exponent e of $\Sigma(N)$ is 1 or 2.

For each odd prime divisor p of N, the exponent r_p of p in the prime power decomposition of N is at most 2: otherwise, p would divide e (cor. 2 of thm. 1). Furthermore, $p-1$ divides $m_1m_2m_3e$ (*loc. cit.*) and *a fortiori* 24, hence p belongs to the set $\{3,5,7,13\}$.

The integer N cannot be divisible by 2.7, 2.13, 5.7, 5.13 or $3^2.7$ because, in these cases, we have $m_3 = 1$ and $3|e$ (*loc. cit.*). It cannot be divisible by

3.5, 3.13, 7.13, $2^3.5$ or 2^7 because, in these cases, we have $m_1 = m_2 = 1$ and $4|e$ (*loc. cit.*). From this, we deduce:

(a) If N is divisible by 13, it is equal to 13 or 13^2. In both cases, we have, in fact, $e = 1$.

(b) If N is divisible by 7, it is equal to $7, 7^2, 3.7$ or 3.7^2. We have, in fact, $e = 1$ in the first two cases and $e = 2$ in the last two.

(c) If N is divisible by 5, it is equal to $5, 5^2, 2.5, 2.5^2, 2^2.5$ or $2^2.5^2$. We have, in fact, $e = 1$ in the first four cases and $e = 2$ in the last two.

(d) If N is divisible by 3 and not by 7, it is of the form $2^a 3$ or $2^a 3^2$, with $0 \leq a \leq 6$. We have, in fact, $e = 1$ if $a \leq 2$ and $e = 2$ if $3 \leq a \leq 6$.

(e) If N is a power of 2, it is equal to 2^a, with $0 \leq a \leq 6$. We have, in fact, $e = 1$ if $a \leq 4$ and $e = 2$ if $a = 5$ or $a = 6$.

The integers N for which $e = 1$, i.e., for which the group $\Sigma(N)$ has order 1, are therefore $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25, 36, 49, 50$ and 169. This proves cor. 3 of thm. 1.

The integers N for which $e = 2$ are $20, 21, 24, 32, 48, 64, 72, 96, 100, 144, 147, 192, 288$ and 576.

3.4 Behaviour when N approaches infinity

Let S be a set of positive integers such that the exponents of the groups $\Sigma(N)$, for $N \in S$, are bounded. Cor. 2 of thm. 1 shows that the prime divisors of the integers $N \in S$ are bounded, and that for each prime number p, the exponent of p in N, $N \in S$, is bounded. This implies that S is finite.

In other words, when N approaches infinity, so does the exponent of $\Sigma(N)$. This proves cor. 4 of thm. 1.

4 Action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\Sigma(N)$

4.1 The remark of section 1.4 revisited in algebraic geometry

Let K be a field of characteristic 0 and let $\overline{K}$ be an algebraic closure of K. If S is a K-scheme, we denote the $\overline{K}$-scheme $S \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, \overline{K}$ by $S_{\overline{K}}$.

Let X, Y be two absolutely irreducible proper smooth curves over K, and let $f : X \to Y$ be a non-constant morphism (over K). Let $g : Z \to Y$

be the maximal unramified covering of Y through which f factorises, such that $g_{\overline{K}} : Z_{\overline{K}} \to Y_{\overline{K}}$ is an abelian covering; let A denote the Galois group of the covering $g_{\overline{K}}$. For $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $a \in A$, there exists a unique $\sigma(a) \in A$ such that the diagram

$$\begin{array}{ccc} Z_{\overline{K}} & \xrightarrow{1_Z \times \mathrm{Spec}\,\sigma} & Z_{\overline{K}} \\ {\scriptstyle \sigma(a)}\downarrow & & \downarrow {\scriptstyle a} \\ Z_{\overline{K}} & \xrightarrow{1_Z \times \mathrm{Spec}\,\sigma} & Z_{\overline{K}} \end{array} \tag{22}$$

is commutative. This defines an action of $\mathrm{Gal}(\overline{K}/K)$ on A. We deduce an action $(\sigma, \chi) \mapsto {}^{\sigma}\chi$ of $\mathrm{Gal}(\overline{K}/K)$ on the character group $\hat{A} = \mathrm{Hom}(A, \overline{K}^{\times})$ characterised by the formula $({}^{\sigma}\chi)(a) = \sigma(\chi(\sigma^{-1}(a)))$.

Let $J(X)$ and $J(Y)$ be the Jacobian varieties of X and Y, viewed as the connected components of 0 in the Picard varieties. The group $J(X)(\overline{K})$ parametrises the isomorphism classes of line bundles of degree 0 on $X_{\overline{K}}$. We denote by $f^* : J(Y)(\overline{K}) \to J(X)(\overline{K})$ the homomorphism deduced from f by Picard functoriality.

For each $\chi \in \hat{A}$, there is a line bundle L_χ on $Y_{\overline{K}}$ associated to the Galois covering $Z_{\overline{K}} \to Y_{\overline{K}}$; its underlying scheme is $(Z_{\overline{K}} \times_{\mathrm{Spec}\,\overline{K}} \mathbf{A}^1_{\overline{K}})/A$, where A acts simultaneously on $Z_{\overline{K}}$ and on the affine line $\mathbf{A}^1_{\overline{K}}$, the action on $\mathbf{A}^1_{\overline{K}}$ being given by $a \mapsto \chi(a^{-1})$. The pullback of L_χ on $Z_{\overline{K}}$, and *a fortiori* on $X_{\overline{K}}$, is the trivial line bundle, hence L_χ is of degree 0 and its isomorphism class $[L_\chi]$ belongs to the kernel of f^*.

PROPOSITION 6 .— *The map $\chi \mapsto [L_\chi]$ is a group isomorphism from $\hat{A}$ to the kernel of $f^* : J(Y)(\overline{K}) \to J(X)(\overline{K})$, compatible with the actions of* $\mathrm{Gal}(\overline{K}/K)$.

To prove that the map $\chi \mapsto [L_\chi]$ is a group isomorphism, we can assume that K is equal to $\overline{K}$, then reduce to the case where $K = \mathbf{C}$ by the Lefschetz principle, and finally use the GAGA principle to derive the result from the analogous result for compact connected Riemann surfaces (see 1.4, remark).

We shall now prove the compatibility with the actions of Galois. Let σ be an element of $\mathrm{Gal}(\overline{K}/K)$ and let L be a line bundle of degree 0 on $Y_{\overline{K}}$. The $\overline{K}$-scheme ${}^{\sigma}L$ deduced from L by the base change $\mathrm{Spec}\,\sigma$ is a line bundle of degree 0 on $Y_{\overline{K}}$: this is because the $\overline{K}$-scheme deduced from $Y_{\overline{K}}$ by this base change is $Y_{\overline{K}}$. The action of $\mathrm{Gal}(\overline{K}/K)$ on $J(Y)(\overline{K})$ is none other than $(\sigma, [L]) \mapsto [{}^{\sigma}L]$. Now let us consider the case where L is the line bundle $L_\chi = (Z_{\overline{K}} \times_{\mathrm{Spec}\,\overline{K}} \mathbf{A}^1_{\overline{K}})/A$ associated to a character $\chi \in \hat{A}$. Then

${}^{\sigma}L$ is the quotient $(Z_{\overline{K}} \times_{\mathrm{Spec}\,\overline{K}} \mathbf{A}^1_{\overline{K}})/A$, where A acts on $Z_{\overline{K}}$ by $a \mapsto \sigma(a)$ (see diagram (22)) and acts on $\mathbf{A}^1_{\overline{K}}$ by $a \mapsto \sigma(\chi(a^{-1}))$. This is the same as taking the quotient $(Z_{\overline{K}} \times_{\mathrm{Spec}\,\overline{K}} \mathbf{A}^1_{\overline{K}})/A$, where the action of A on $Z_{\overline{K}}$ is the original action and where A acts on $\mathbf{A}^1_{\overline{K}}$ by $a \mapsto {}^{\sigma}\chi(a^{-1})$. Hence, we have $[{}^{\sigma}(L_\chi)] = [L_{{}^{\sigma}\chi}]$. This completes the proof.

4.2 Galois action on the Shimura subgroup

The Riemann surfaces $X_1(N)$ and $X_0(N)$ are the sets of complex points of algebraic modular curves naturally defined over $\mathbf{Q}$, denoted by $X_1(N)_{\mathbf{Q}}$ and $X_0(N)_{\mathbf{Q}}$: these may be defined as the smooth compactifications of the coarse moduli schemes associated to the modular problems described in the remark of 2.1 (modular problems which make sense over $\mathbf{Q}$). The holomorphic map $u : X_1(N) \to X_0(N)$ considered in 2.1 comes from a morphism $u_{\mathbf{Q}} : X_1(N)_{\mathbf{Q}} \to X_0(N)_{\mathbf{Q}}$ and each automorphism $g \in G$ (with $G = \Gamma_0(N)/\{-1,1\}\Gamma_1(N) \simeq (\mathbf{Z}/N\mathbf{Z})^\times/\{-1,1\}$) of the covering u comes from an automorphism of $X_1(N)_{\mathbf{Q}}$: this follows from the modular description of u and G (2.1, remark).

We have defined in 2.2 a canonical injective homomorphism

$$\psi' : \Sigma(N) \longrightarrow \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}).$$

Let A denote the Galois group of the maximal abelian unramified covering of $X_0(N)$ through which u factorises. It is a quotient of G, and hence of $(\mathbf{Z}/N\mathbf{Z})^\times$. The homomorphism ψ' is none other than the homomorphism obtained by composing the isomorphism $\Sigma(N) \to \mathrm{Hom}(A, \mathbf{U})$ defined in the remark of 1.4 and the canonical injection $\mathrm{Hom}(A, \mathbf{U}) \to \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U})$. This follows from the commutativity of the natural diagram

$$\begin{array}{ccc} \Gamma_0(N) & \longrightarrow & H_1(X_0(N), \mathbf{Z}) \\ \downarrow & & \downarrow \\ (\mathbf{Z}/N\mathbf{Z})^\times & \longrightarrow & A \end{array} .$$

Since $J_0(N)$ is the set of complex points of the Jacobian variety $J_0(N)_{\mathbf{Q}}$ of $X_0(N)_{\mathbf{Q}}$, the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, where $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, acts on the group of torsion points of $J_0(N)$ and, in particular, on $\Sigma(N)$.

Let e be the exponent of the group $\Sigma(N)$ and let μ_e be the group of e-th roots of unity in $\mathbf{C}$. We can interprete ψ' as an injective homomorphism

$\Sigma(N) \to \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mu_e)$. Prop. 6 implies that this homomorphism is compatible with the actions of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (the action on $(\mathbf{Z}/N\mathbf{Z})^\times$ is trivial). Hence, each point of $\Sigma(N)$ is defined over $\mathbf{Q}(\mu_e)$, and $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q})$ acts on $\Sigma(N)$ via the cyclotomic character $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q}) \to (\mathbf{Z}/e\mathbf{Z})^\times$. Let x be an element of $\Sigma(N)$ and let e' be its order. The field of definition of x is the subfield of $\mathbf{Q}(\mu_e)$ fixed by the kernel of the composition of homomorphisms $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q}) \to (\mathbf{Z}/e\mathbf{Z})^\times \to (\mathbf{Z}/e'\mathbf{Z})^\times$, i.e., the cyclotomic field $\mathbf{Q}(\mu_{e'})$. In particular, $\mathbf{Q}(\mu_e)$ is the smallest extension of $\mathbf{Q}$ over which all points of $\Sigma(N)$ are defined. This completes the proof of thm. 2.

4.3 Points of $\Sigma(N)$ rational over $\mathbf{Q}$

Let x be a point of $\Sigma(N)$ and let e' be its order. We have shown in 4.2 that the field of definition of x is $\mathbf{Q}(\mu_{e'})$. In particular, x is rational over $\mathbf{Q}$ if and only if e' is equal to 1 or 2, i.e., if and only if we have $2x = 0$. This proves the first assertion of cor. 1 of thm. 2. To prove the last assertion, we shall, as in the statement of the corollary, denote by P the set of odd primes dividing N and by ϵ the number defined by

$$\epsilon = \begin{cases} -1 & \text{if } 4 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 8; \\ -1 & \text{if } 4|N, 8 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 4; \\ 1 & \text{if } 32|N; \\ 0 & \text{otherwise.} \end{cases}$$

By definition, the 2-rank of an abelian group A is the dimension of $A/2A$ over $\mathbf{Z}/2\mathbf{Z}$.

LEMMA 4 .— *Let A be a finite abelian group and let $a \in A$ be an element of order 2. The 2-rank of $A/\{0, a\}$ is equal to that of A if a belongs to $2A$, and is equal to that of A minus 1 otherwise.*

The lemma is obvious.

To complete the proof of cor. 1 of thm. 2, we have to show that the 2-rank of $\Sigma(N)$ is $\mathrm{Card}(P) + \epsilon$. If N is equal to 1, 2 or 4, the 2-rank of $\Sigma(N)$, $\mathrm{Card}(P)$ and ϵ are all equal to 0. We assume now that N is distinct from 1, 2 and 4, and distinguish between two cases:

a) *The case where* -1 *is a square* mod N.

The integer N is of the form N' or $2N'$, with $N' \neq 1$ and each prime factor of N' congruent to 1 mod 4. The quotient of the group

$$A = \prod_{p|N'} (\mathbf{Z}/\tfrac{p-1}{2}\mathbf{Z})$$

by the unique subgroup of order 2 which has a non-zero projection on each factor has the same 2-rank as $\Sigma(N)$ (2.3, cor. 1 of prop. 5). The 2-rank of A is Card(P). By lemma 4, the 2-rank of $\Sigma(N)$ is Card(P) or Card$(P)-1$, depending on whether each prime factor of N' is congruent to 1 mod 8 or not, i.e., whether $\epsilon = 0$ or $\epsilon = -1$.

b) *The case where* -1 *is not a square* mod N.

Let r_2 be the exponent of 2 in the prime power decomposition of N. The quotient of the group

$$A = (\mathbf{Z}/2^{r_2-[r_2/2]}\mathbf{Z})^\times \times \prod_{p|N,p\neq 2} \mathbf{F}_p^\times$$

by the subgroup $\{-1,1\}$ (which is embedded diagonally in A) has the same 2-rank as $\Sigma(N)$ (2.3, cor. 2 of prop. 5, and isomorphism (21)).

Assume first that $r_2 \leq 2$. Then A is isomorphic to $\prod_{p|N,p\neq 2} \mathbf{F}_p^\times$, and its 2-rank is Card$(P)$. By lemma 4, the 2-rank of $\Sigma(N)$ is Card(P) or Card$(P)-1$, depending on whether the set P' of prime divisors of N congruent to 3 mod 4 is empty or not. If $r_2 = 0$ or $r_2 = 1$, P' is not empty because -1 is not a square mod N; we have $\epsilon = -1$ in this case by definition of ϵ. If $r_2 = 2$, we have $\epsilon = 0$ when $P' = \emptyset$ and $\epsilon = -1$ when $P' \neq \emptyset$, by definition of ϵ. This proves the announced formula for the 2-rank of $\Sigma(N)$ when $r_2 \leq 2$.

Assume now that $r_2 \geq 3$. Then $(\mathbf{Z}/2^{r_2-[r_2/2]}\mathbf{Z})^\times$ is the product of a cyclic group of order 2 onto which $\{-1,1\}$ maps surjectively and a cyclic group of order $2^{r_2'}$, where $r_2' = r_2 - [r_2/2] - 2$. The group $A/\{-1,1\}$ is therefore isomorphic to $\mathbf{Z}/2^{r_2'}\mathbf{Z} \times \prod_{p|N,p\neq 2} \mathbf{F}_p^\times$. Its 2-rank, equal to that of $\Sigma(N)$, is Card(P) or Card$(P)+1$, depending on whether r_2' is equal to 0 (i.e., $r_2 = 3$ or $r_2 = 4$) or is at least 1 (i.e., $r_2 \geq 5$). In the first case, we have $\epsilon = 0$ and in the second case, $\epsilon = 1$, by definition of ϵ.

4.4 Cases where all points of $\Sigma(N)$ are rational over Q

By cor. 1 of thm. 2, all points of $\Sigma(N)$ are rational over $\mathbf{Q}$ if and only if the exponent of the group $\Sigma(N)$ is 1 or 2. The list of integers for which this is the case has been obtained in 3.3. In the 14 cases where the exponent of $\Sigma(N)$ is 2, the 2-rank of $\Sigma(N)$ can be computed by using cor. 1 of thm. 2 and the following table

N	20	21	24	32	48	64	72	96	100	144	147	192	288	576
Card(P)	1	2	1	0	1	0	1	1	1	1	2	1	1	1
ϵ	0	−1	0	1	0	1	0	1	0	0	−1	1	1	1

In all these cases, the 2-rank of $\Sigma(N)$ is equal to 1, except for $N = 96$, 192, 288 and 576 where it is equal to 2. Cor. 2 of thm. 2 follows.

5 Shimura subgroups and Atkin-Lehner involutions

To each divisor N_1 of N such that $\gcd(N_1, N/N_1) = 1$ is associated an Atkin-Lehner involution w_{N_1} of $X_0(N)$.

Analytic definition: The involution w_{N_1} is deduced, by passing to the quotients, from the transformation $\tau \mapsto g\tau$ of $\overline{\mathcal{H}}$, where $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is any matrix in $M_2(\mathbf{Z})$ such that $N_1|A$, $N_1|D$, $N|C$ and $AD - BC = N_1$. (Such a matrix g normalises $\Gamma_0(N)$.)

Modular description: The involution w_{N_1} stabilises $Y_0(N)$ and its restriction to $Y_0(N)$ has the following modular interpretation (with the conventions of 2.1, remark): if E is an elliptic curve over $\mathbf{C}$ and C a cyclic subgroup of E of order N, we have $w_{N_1}([E, C]) = [E/C_{N_1}, (E_{N_1} + C)/C_{N_1}]$, where C_{N_1} and E_{N_1} are the kernels of multiplication by N_1 in C and E respectively.

Let ${w_{N_1}}^*$ and $(w_{N_1})_*$ be the involutions of $J_0(N)$ deduced from w_{N_1} by Picard and Albanese functorialities. Since the holomorphic map w_{N_1} is of degree 1, we have $(w_{N_1})_* \circ {w_{N_1}}^* = \mathrm{Id}_{J_0(N)}$, and this implies $(w_{N_1})_* = {w_{N_1}}^*$ because ${w_{N_1}}^*$ is an involution.

By prop. 3 of 1.5, and 2.2, thm. 3 is a consequence of the following lemma:

LEMMA 5 .— *Let* $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *be as in the analytic definition of* w_{N_1} *given above. The automorphism* $\gamma \mapsto g\gamma g^{-1}$ *of* $\Gamma_0(N)$ *stabilises* $\Gamma_1(N)$. *The automorphism of* $(\mathbf{Z}/N\mathbf{Z})^\times$ $(\simeq \Gamma_0(N)/\Gamma_1(N))$ *which is deduced by passing to the quotients coincides with* $t \mapsto t^{-1}$ *modulo* N_1 *and with the identity modulo* N/N_1.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $\Gamma_0(N)$ and let $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be the matrix $g\gamma g^{-1}$. We have $d' = (-aBC + bAC - cBD + dAD)/N_1$. From the properties satisfied by g and from the fact that N divides c, we deduce that $-aBC$, bAC, $-cBD$, dAD are respectively congruent to $aN_1, 0, 0, 0$ modulo N_1^2 and to $0, 0, 0, dN_1$ modulo N. Therefore, we have $d' \equiv a \equiv d^{-1} \bmod N_1$ and $d' \equiv d \bmod N/N_1$. This proves the lemma.

6 Shimura subgroups and degeneracy maps

6.1 Degeneracy maps

Let M be a divisor of N. For each divisor D of N/M, we have a holomorphic degeneracy map $v_D : X_0(N) \to X_0(M)$. It is the map deduced from the transformation $\tau \mapsto D\tau$ of $\overline{\mathcal{H}}$ by passing to the quotients. The map v_D induces a map from $Y_0(N)$ to $Y_0(M)$ which has the following modular interpretation (with the conventions of 2.1, remark): if E is an elliptic curve over $\mathbf{C}$ and C a cyclic subgroup of E of order N, we have

$$v_D([E, C]) = [E/C_D, C_{MD}/C_D],$$

where C_D and C_{MD} denote the unique subgroups of C of orders D and MD respectively. Let $v_D{}^* : J_0(M) \to J_0(N)$ and $(v_D)_* : J_0(N) \to J_0(M)$ denote the morphisms of abelian varieties deduced from v_D by Picard and Albanese functorialities.

6.2 Proof of thm. 4

By prop. 3 of 1.5, and 2.2, thm. 4 concerning the behaviour of the Shimura subgroups under the degeneracy maps $v_D{}^*$ is a consequence of the following lemma:

LEMMA 6 .— *Let g be the matrix $\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}$ and let $v : \Gamma_0(N) \to \Gamma_0(M)$ be the homomorphism $\gamma \mapsto g\gamma g^{-1}$. We have $v(\Gamma_1(N)) \subseteq \Gamma_1(M)$ and v induces, by passing to the quotients, the canonical surjection $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/M\mathbf{Z})^\times$.*

Lemma 6 follows from the identity

$$\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & bD \\ c/D & d \end{pmatrix}.$$

6.3 A compatibility property of transfer homomorphisms

In this section, G denotes a group and H denotes a subgroup of G. We denote by $\iota_{G,H} : H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ the homomorphism deduced from the canonical injection $H \to G$. If the index $[G : H]$ is finite, $V_{H,G} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ denotes the transfer homomorphism.

LEMMA 7 .— *Let G' be a subgroup of G such that $G = HG'$ (i.e., such that G' maps surjectively to $H\backslash G$) and let H' be a subgroup of $H \cap G'$ of finite index in G'. Then $[G : H]$ is finite, the quotient $r = [G' : H']/[G : H]$ is equal to $[H \cap G' : H']$ and the diagram*

$$\begin{array}{ccc} G'^{\mathrm{ab}} & \xrightarrow{V_{H',G'}} & H'^{\mathrm{ab}} \\ {\scriptstyle \iota_{G,G'}}\downarrow & & \downarrow{\scriptstyle \iota_{H,H'}} \\ G^{\mathrm{ab}} & \xrightarrow{V^r_{H,G}} & H^{\mathrm{ab}}, \end{array}$$

where $V^r_{H,G}$ denotes the homomorphism $x \mapsto (V_{H,G}(x))^r$, is commutative.

In the proof, let us write the groups additively and consider the diagram

$$\begin{array}{ccccc} G'^{\mathrm{ab}} & \xrightarrow{V_{H\cap G',G'}} & (H \cap G')^{\mathrm{ab}} & \xrightarrow{V_{H',H\cap G'}} & H'^{\mathrm{ab}} \\ {\scriptstyle \iota_{G,G'}}\downarrow & & {\scriptstyle \iota_{H,H\cap G'}}\downarrow & & {\scriptstyle \iota_{H,H'}}\downarrow \\ G^{\mathrm{ab}} & \xrightarrow{V_{H,G}} & H^{\mathrm{ab}} & \xrightarrow{r.1_{H^{\mathrm{ab}}}} & H^{\mathrm{ab}}. \end{array} \tag{23}$$

The canonical map $H \cap G'\backslash G' \to H\backslash G$ is bijective by hypothesis, hence H is of finite index in G, we have $[G' : H'] = [G : H][H \cap G' : H']$ and a system

of representatives in G' of $H \cap G' \backslash G'$ is also a system of representatives in G of $H \backslash G$. The first square of diagram (23) is therefore commutative, by definition of the transfer homomorphisms (1.5). This definition also implies that $\iota_{H\cap G',H'} \circ V_{H',H\cap G'}$ coincides with multiplication by $r = [H \cap G' : H']$ in $(H \cap G')^{\mathrm{ab}}$, and the commutativity of the second square of diagram (23) follows. Since the transfer homomorphisms satisfy the transitivity property $V_{H',H\cap G'} \circ V_{H\cap G',G'} = V_{H',G'}$ ([2], thm. 14.2.1), the commutativity of diagram (23) establishes the lemma.

6.4 The transfer homomorphism $\Gamma_0(M)^{\mathrm{ab}} \to \Gamma_0(N)^{\mathrm{ab}}$

Let M be a divisor of N, $\iota_{M,N} : \Gamma_0(N)^{\mathrm{ab}} \to \Gamma_0(M)^{\mathrm{ab}}$ the homomorphism deduced from the injection $\Gamma_0(N) \to \Gamma_0(M)$, $V_{N,M} : \Gamma_0(M)^{\mathrm{ab}} \to \Gamma_0(N)^{\mathrm{ab}}$ the transfer homomorphism, and $\pi_N : \Gamma_0(N)^{\mathrm{ab}} \to (\mathbf{Z}/N\mathbf{Z})^\times$ the surjection deduced from our identification of $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$.

In the next proposition, we use the following notation: for an integer n, n^* denotes n when n is odd and $n/2$ when n is even. We also write $N = N_1 N_2$, with N_2 the largest divisor of N prime to M.

PROPOSITION 7 .— *Let* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an element of* $\Gamma_0(M)$ *and* $\overline{\gamma}$ *its image in* $\Gamma_0(M)^{\mathrm{ab}}$. *The element* $\pi_N(V_{N,M}(\overline{\gamma}))$ *of* $(\mathbf{Z}/N\mathbf{Z})^\times$ *is congruent to* $d^{[\Gamma_0(M):\Gamma_0(N)]}$ *modulo* N_1^* *and to* 1 *modulo* N_2^*.

Let p be a prime divisor of N. Let us write $M = p^m M'$, $N = p^n N'$, with M' and N' prime to p. The map $\Gamma_0(p^n)\backslash SL_2(\mathbf{Z}) \to \mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$ which sends a coset $\Gamma_0(p^n)\begin{pmatrix} u & v \\ w & t \end{pmatrix}$ to the point of $\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$ with homogeneous coordinates (w, t) is bijective. Therefore the canonical map $\Gamma_0(M) \to \Gamma_0(p^n)\backslash\Gamma_0(p^m)$ is surjective. By applying lemma 7, we get a commutative diagram

$$\begin{array}{ccccc} \Gamma_0(M)^{\mathrm{ab}} & \xrightarrow{V_{N,M}} & \Gamma_0(N)^{\mathrm{ab}} & \xrightarrow{\pi_N} & (\mathbf{Z}/N\mathbf{Z})^\times \\ \iota_{p^m,M}\downarrow & & \iota_{p^n,N}\downarrow & & \downarrow \\ \Gamma_0(p^m)^{\mathrm{ab}} & \xrightarrow{V^r_{p^n,p^m}} & \Gamma_0(p^n)^{\mathrm{ab}} & \xrightarrow{\pi_{p^n}} & (\mathbf{Z}/p^n\mathbf{Z})^\times, \end{array} \tag{24}$$

where r is equal to $[\Gamma_0(M) : \Gamma_0(N)]/[\Gamma_0(p^m) : \Gamma_0(p^n)]$ and the last vertical map is the canonical surjection. This shows that, in order to prove the "p-primary part" of the congruences of prop. 7, it is sufficient to prove

prop. 7 when N is a power of p. From now on, we make this assumption. We consider two cases:

a) *The case* $m \geq 1$

In this case, we have $N_1 = N = p^n$, $N_2 = 1$, $M = p^m$ and the matrices $s_l = \begin{pmatrix} 1 & 0 \\ lM & 1 \end{pmatrix}$, with $1 \leq l \leq N/M$, form a system of representatives of $\Gamma_0(N)\backslash\Gamma_0(M)$. For each integer l, $1 \leq l \leq N/M$, there exists a unique integer k such that $1 \leq k \leq N/M$ and $alM + c \equiv kM(blM + d) \bmod N$; the identity

$$\begin{pmatrix} 1 & 0 \\ lM & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - bkM & b \\ alM + c - kM(blM + d) & blM + d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ kM & 1 \end{pmatrix}$$

shows that we have $s_l\gamma = a_{l,\gamma}s_k$ with $a_{l,\gamma}$ in $\Gamma_0(N)$, and that $\pi_N(\overline{a_{l,\gamma}})$ is the class of $blM + d \bmod N$. By definition of the transfer homomorphism (see 1.5), $\pi_N(V_{N,M}(\overline{\gamma}))$ is equal to $\prod_{1\leq l\leq N/M} \pi_N(\overline{a_{l,\gamma}})$, i.e., to the class mod N of $\prod_{1\leq l\leq N/M}(blM + d)$. From this, we deduce

$$\pi_N(V_{N,M}(\overline{\gamma})) = d^{N/M}\Big(\prod_{h\in H} h\Big)^{M'/M}, \tag{25}$$

where M' is given by $M' = \gcd(bM, N)$ and H denotes the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ consisting of the elements congruent to 1 mod M'.

LEMMA 8 .— *Let A be a finite abelian group. The product of the elements of A is equal to the unit element, except in the case where A has a unique element ϵ of order 2; in that case, the product is equal to ϵ.*

The lemma is immediately proved by writing A as a product of cyclic groups.

We now apply the lemma to the subgroup H of $(\mathbf{Z}/N\mathbf{Z})^\times$. The only cases where H has a unique element of order 2 are those where we have $p = 2$, and either $(M', N) = (2, 4)$ or $4 \leq M' < N$. In these cases, $\prod_{h\in H} h$ is the class of $1 + (N/2) \bmod N$; in all the other cases, $\prod_{h\in H} h$ is the class of $1 \bmod N$. From (25), we therefore deduce the congruence

$$\pi_N(V_{N,M}(\overline{\gamma})) \equiv d^{N/M} \bmod N^*. \tag{26}$$

Since we have $N/M = p^{n-m} = [\Gamma_0(M) : \Gamma_0(N)]$, prop. 7 follows.

b) *The case* $m = 0$

In this case, we have $N_1 = M = 1$, $N_2 = N = p^n$. Since prop. 7 is obvious when $N = 1$, we may assume $n \geq 1$. The group $\Gamma_0(M)$ is equal to $SL_2(\mathbf{Z})$. It is isomorphic to the group given by the presentation $\langle s, u; s^4, u^6, s^2u^{-3}\rangle$ ([6], p.52): an isomorphism between this latter group and $SL_2(\mathbf{Z})$ is obtained by sending s to $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and u to TS, where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (*loc. cit.*). The group $SL_2(\mathbf{Z})^{\mathrm{ab}}$ is hence isomorphic to the group defined by the presentation $\langle s, u; s^4, u^6, s^2u^{-3}, sus^{-1}u^{-1}\rangle$, i.e., (by taking $v = u^2$) to the group defined by the presentation $\langle s, v; s^4, v^3, svs^{-1}v^{-1}\rangle$. It is a cyclic group of order 12. Let $\overline{S}$ and $\overline{T}$ denote the canonical images of S and T in $SL_2(\mathbf{Z})^{\mathrm{ab}}$. The subgroup of order 4 of $SL_2(\mathbf{Z})^{\mathrm{ab}}$ is generated by $\overline{S}$ and the subgroup of order 3 by $(\overline{T}\,\overline{S})^2 = \overline{S}^2(\overline{T}\,\overline{S})^{-1} = \overline{S}\,\overline{T}^{-1}$. This implies that $\overline{T}$ generates $SL_2(\mathbf{Z})^{\mathrm{ab}}$. In order to prove prop. 7, it suffices to treat the case where the matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The matrices $s_l = \begin{pmatrix} 1 & 0 \\ lp & 1 \end{pmatrix}$, for $1 \leq l \leq N/p$, and $s'_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$, for $1 \leq j \leq N$, form a system of representatives of $\Gamma_0(N)\backslash SL_2(\mathbf{Z})$. For each integer l, $1 \leq l \leq N/p$, there exists a unique integer k such that $1 \leq k \leq N/p$ and $l \equiv k(1 + lp) \bmod N/p$, and the identity

$$\begin{pmatrix} 1 & 0 \\ lp & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 - kp & 1 \\ lp - kp(1 + lp) & 1 + lp \end{pmatrix}\begin{pmatrix} 1 & 0 \\ kp & 1 \end{pmatrix}$$

shows that $s_lT = a_ls_k$, with a_l in $\Gamma_0(N)$ and $\pi_N(\overline{a_l}) = 1 + lp \bmod N$. Furthermore, we have

$$s'_jT = s'_{j+1} \qquad \text{for } 1 \leq j < N$$

$$s'_NT = \begin{pmatrix} 1 & 0 \\ -N & 1 \end{pmatrix} s'_1.$$

By definition of the transfer homomorphism, $\pi_N(V_{N,1}(\overline{T}))$ is then the class mod N of $\prod_{1 \leq l \leq N/p} (1 + lp)$. By lemma 8, this class is equal to 1 mod N, except in the case $N = 4$, where it is equal to 3 mod N. Prop. 7 follows.

6.5 Proof of thm. 5

Let M be a divisor of N, and D a divisor of N/M. As in 6.4, we write $N = N_1N_2$, with N_2 the largest divisor of N prime to M. The index $[\Gamma_0(M) : \Gamma_0(N)]$ is equal to $\frac{N}{M} \prod_{p|N_2} (1+\frac{1}{p})$, hence is a multiple of N_1/M. Since N_1 and M have the same prime divisors, this implies that, if d is an integer prime to M, the class $d^{[\Gamma_0(M):\Gamma_0(N)]}$ mod N_1 depends only on d mod M. We can therefore define a homomorphism $\delta' : (\mathbf{Z}/M\mathbf{Z})^\times \to (\mathbf{Z}/N\mathbf{Z})^\times$ by the following relations:

$$\begin{cases} \delta'(d + M\mathbf{Z}) \equiv d^{[\Gamma_0(M):\Gamma_0(N)]} & \mod N_1 \\ \delta'(d + M\mathbf{Z}) \equiv 1 & \mod N_2. \end{cases}$$

By prop. 4 of 1.5, and 2.2, thm. 5 concerning the behaviour of the Shimura subgroup of $J_0(N)$ under the morphism $(v_D)_* : J_0(N) \to J_0(M)$ (which was defined in 6.1) is equivalent to the following statement: the diagram

$$\begin{array}{ccccc} \Gamma_0(M)^{\mathrm{ab}} & \longrightarrow & \Gamma_0(M)/\Gamma_1(M) \simeq & (\mathbf{Z}/M\mathbf{Z})^\times & \\ V \downarrow & & & \downarrow \delta' & \qquad (27) \\ \Gamma_0(N)^{\mathrm{ab}} & \longrightarrow & \Gamma_0(N)/\Gamma_1(N) \simeq & (\mathbf{Z}/N\mathbf{Z})^\times, & \end{array}$$

where V is the transfer homomorphism and the horizontal arrows represent the canonical surjections, is commutative modulo J, where J is the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ defined in 2.3.

Prop. 7 tells us that (27) is commutative when $4 \nmid N$, and that (27) is commutative modulo the subgroup of order 2 of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by the class d of $1 + (N/2)$ mod N, when $4|N$. In the latter case, we have $(d-1)^2 = 0$ in $\mathbf{Z}/N\mathbf{Z}$, hence d belongs to J. This completes the proof of thm. 5.

7 Action of the Hecke algebra on the Shimura subgroup

Let p be a prime number. The two degeneracy maps

$$\begin{array}{ccccc} & & X_0(Np) & & \\ & v_p \swarrow & & \searrow v_1 & \\ X_0(N) & & & & X_0(N) \end{array}$$

define a correspondence T_p between $X_0(N)$ and itself: we have $T_p = v_1 \circ v_p^{-1}$, where the symbol v_p^{-1} denotes the inverse correspondence of v_p and $\circ$ denotes the composition of correspondences.

If $[\tau]$ denotes the image in $X_0(N)$ of a point $\tau \in \overline{\mathcal{H}}$, then T_p is given by

$$T_p([\tau]) = \begin{cases} [p\tau] + \sum_{0 \le i \le p-1} \left[\frac{\tau+i}{p}\right] & \text{if } p \nmid N \\ \\ \sum_{0 \le i \le p-1} \left[\frac{\tau+i}{p}\right] & \text{if } p \mid N. \end{cases}$$

The restriction of T_p to $Y_0(N)$ has the following modular interpretation: if E is an elliptic curve defined over $\mathbf{C}$ and C a cyclic subgroup of order N of E, then

$$T_p([E, C]) = \sum_{C'} [E/C', (C + C')/C'],$$

where the sum is indexed by the subgroups C' of E of order p, with the restriction that $C \cap C' = \{0\}$ if p divides N.

We can define endomorphisms T_p^* and $(T_p)_*$ of $J_0(N)$ by

$$\begin{aligned} T_p^* &= (v_p)_* \circ v_1^* \\ (T_p)_* &= (v_1)_* \circ v_p^*. \end{aligned} \tag{28}$$

(When we think of a correspondence as an object generalising a map, T_p^* and $(T_p)_*$ can be thought of as associated to T_p via Picard and Albanese functorialities respectively; however, the definition of each of them involves both functorialities, as is seen in the formulae.)

Theorems 4 and 5 imply that both the endomorphisms T_p^* and $(T_p)_*$ stabilise the Shimura subgroup $\Sigma(N)$ of $J_0(N)$, and that they coincide on $\Sigma(N)$ with multiplication by $[\Gamma_0(N) : \Gamma_0(Np)]$, i.e., by $p + 1$ if p does not divide N, and by p if p divides N. This proves thm. 6.

It is possible to define, for each integer $n \ge 1$, a Hecke correspondence T_n on $X_0(N)$ and, hence, endomorphisms T_n^* and $(T_n)_*$ of $J_0(N)$. The endomorphisms T_n^* satisfy recurrence relations which can be summarised by the formal identity between Dirichlet series

$$\sum T_n^* n^{-s} = \prod_{p \mid N} (1 - T_p^* p^{-s})^{-1} \prod_{p \nmid N} (1 - T_p^* p^{-s} + p^{1-2s})^{-1},$$

and we have an analogous identity for $(T_n)_*$. Therefore, remark 2 in the introduction follows from the identity

$$\sum_{n=1}^{\infty} a_N(n)n^{-s} = \prod_{p|N}(1-p^{1-s})^{-1} \prod_{p\nmid N}(1-p^{-s})(1-p^{1-s})^{-1},$$

where $a_N(n)$ denotes the sum of the divisors d of n satisfying the condition $\gcd(N, \frac{n}{d}) = 1$.

References

[1] A. GROTHENDIECK, *Éléments de Géométrie algébrique*, chapitre II, Publications mathématiques de l'I.H.E.S., Vol. 8, 1961.

[2] M. HALL Jr., *The theory of groups*, The Macmillan Cy., New York, 1959.

[3] B. MAZUR, *Modular curves and the Eisenstein ideal*, Publications mathématiques de l'I.H.E.S., Vol. 47, 1978, pp. 33–186.

[4] M. RAYNAUD, *Familles de fibrés vectoriels sur une surface de Riemann* [d'après C. S. Seshadri, M. S. Narasimhan et D. Mumford], Séminaire Bourbaki 1966/1967, exposé 316.

[5] K. A. RIBET, *On the component groups and the Shimura subgroup of* $J_0(N)$, séminaire de théorie des nombres de Bordeaux, 1987–1988, exposé 6.

[6] J.-P. SERRE, *Arbres, amalgames*, SL_2, Astérisque, Vol. 46, 1977.

[7] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, copublished by Iwonami Shoten and Princeton University Press, 1971.

LING San
Mathematics Department
University of California
Berkeley CA 94720
U.S.A.

OESTERLÉ Joseph
Département de mathématiques
Université de Paris VI
4, place Jussieu
75005 – PARIS
FRANCE

Congruence primes for cusp forms of weight $k \geq 2$

FRED DIAMOND

§1. Introduction

This paper generalizes to higher weights a result of Ribet [R1] on congruences between weight two newforms of different levels. If $f = \sum a_n q^n$ and $g = \sum b_n q^n$ are newforms with the $a_n, b_n \in K$, and $\mathfrak{p}$ is a prime of K over the rational prime p, we say $f \equiv g \mod \mathfrak{p}$ if $a_n \equiv b_n$ for all n prime to the levels of f and g. If f has weight k, character χ and level N, then for a prime ℓ not dividing Np, denote by R_ℓ the set of newforms of weight k, character χ, but of level $d\ell$ with d dividing N (thus "new at ℓ").

THEOREM (RIBET). *For f as above, with $k = 2$, trivial χ, sufficiently large K and $p \nmid \frac{1}{2}\phi(N)N\ell$, there exist $g \in R_\ell$ with $g \equiv f \mod \mathfrak{p}$ if and only if*

$$a_\ell^2 \equiv (\ell + 1)^2 \mod \mathfrak{p}.$$

In [D], it is observed that Ribet's proof requires neither trivial character nor p prime to N. Consequently an analogue [D, Th. 6] is proven for Λ-adic forms ([H2], [W]) which p-adically interpolate classical forms. This provides a result for p-stabilized newforms of any weight $k \geq 2$ [D, Cor. 6.9]. However, inherent in the definition of a p-stabilized newform is that it is ordinary at p. In §2 below, we dispense with this hypothesis and prove:

THEOREM 1. *For f as above, with $k \geq 2$, arbitrary χ, sufficiently large K and $p \nmid \frac{1}{2}\phi(N)N\ell(k-2)!$, there exist $g \in R_\ell$ with $g \equiv f \mod \mathfrak{p}$ if and only if*

$$a_\ell^2 \equiv \chi(\ell)\ell^{k-2}(\ell + 1)^2 \mod \mathfrak{p}.$$

This is proved by applying Ribet's method directly to the parabolic cohomology groups associated to forms of higher weight. Decomposing the space of cusp forms into subspaces which are old and new at ℓ yields a cohomology congruence module

S.M.F.
Astérisque 196-197 (1991)

which can be computed using the ingredients of a result of Ihara [I, Lemma 3.2]. For $k = 2$, Ihara's result may be viewed (via the exact sequence of Lyndon) as the vanishing of the parabolic cohomology group, with coefficients in $\mathbf{F}_p$, of a principal congruence subgroup of level N in $PSL_2(\mathbf{Z}[\ell^{-1}])$. We generalize this to cohomology with weight k coefficients in the proof of Lemma 3.2 below by noting that the restriction of a parabolic cocycle to the principal congruence subgroup of level Np vanishes, as does the kernel of this restriction homomorphism if $p \nmid N(k-2)!$ (Lemma 3.1).

Theorem 1 may be regarded in terms of raising the level of the modular representation $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathcal{O}_K/\mathfrak{p})$ associated to f. It has already been proved in some cases of higher weight in work of Jordan and Livné [J-L]. Their method requires that a prime q divide N exactly, and the result is needed to lower the level of the representation if it is unramified at q (from N to N/q). This also is a generalization of a weight two result of Ribet [R2] relating the Artin conductor of the representation to the level of some form from which it arises, as conjectured by Serre [S]. Theorem 1 is shown to be similarly useful in lowering the level of a modular representation (when q^r divides N, but not the Artin conductor) in recent work of Carayol [C].

This research was completed while visiting Ohio State University. I would like to thank Avner Ash for many suggestions, especially regarding the proof of Lemma 3.1, whose ingredients can be found in [A-S]. I would also like to thank Richard Taylor for helpful correspondence.

§2. Congruences

We fix a rational prime p and a finite extension K of $\mathbf{Q}_p$. Let $\mathcal{O}_K$ be the integral closure of $\mathbf{Z}_p$ in K and denote by $\mathfrak{p}$ its maximal ideal. We also fix embeddings of K into the algebraic closure $\bar{\mathbf{Q}}_p$ of $\mathbf{Q}_p$, and of $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_p$ and $\mathbf{C}$.

Now consider a level N, a weight $k \geq 2$ and a prime ℓ not dividing Np. Let $Z = S_k(\Gamma_1(N) \cap \Gamma_0(\ell); K)$, the cusp forms on $\Gamma_1(N) \cap \Gamma_0(\ell)$ of weight k with q-expansions having coefficients in K. Let $\mathcal{H}_Z$ be the $\mathcal{O}_K$-algebra of endomorphisms of Z generated by the Hecke operators T_n for $n \geq 1$ (e.g. [H2, §1]). We note that this algebra includes the endomorphisms S_m for m prime to N defined by $f \mid S_m = m^{k-2} f \mid \sigma_m$ where $\sigma_m \in \Gamma_0(N\ell)$ is congruent to $\begin{pmatrix} m^{-1} & 0 \\ 0 & m \end{pmatrix}$ mod N.

We have a decomposition of Z into its subspaces which are old and new at ℓ, $Z = X \oplus Y$ [R1, §2]. Here X is the direct sum of two copies of $S_k(\Gamma_1(N); K)$, and Y may be characterized as the kernel of $T_\ell^2 - S_\ell$. The newforms in X are those

in Z of level dividing N, and those in Y have level divisible by ℓ. We will always assume $X \neq 0$ (in particular, if $N \leq 2$ then k is even and sufficiently large). This decomposition is stable under the action of $\mathcal{H}_Z$. We let $\mathcal{H}_X$ be the image of $\mathcal{H}_Z$ in the endomorphism ring of X and similarly define $\mathcal{H}_Y$. Then to prove the existence of non-trivial congruences between forms in X and forms in Y, we must show that $\mathcal{H}_{X,Y} = \mathcal{H}_X \oplus \mathcal{H}_Y / \mathcal{H}_Z$ is non-trivial. We do so (under suitable conditions) by using the cohomology to construct an $\mathcal{H}_{X,Y}$-module.

We now apply Ribet's analysis [R1, §3] of such a cohomology congruence module to the parabolic cohomology corresponding to cusp forms of weight k. For $n = k-2$, we define $L_n(\mathbb{Z}) = \mathbb{Z}^{n+1}$ with the action of $SL_2(\mathbb{Z})$ determined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}^n = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}^n,$$

where $\begin{pmatrix} x \\ y \end{pmatrix}^n = {}^t(x^n, x^{n-1}y, \ldots, y^n)$.

For any abelian group R, $SL_2(\mathbb{Z})$ then acts on $L_n(R) = L_n(\mathbb{Z}) \otimes R$. Then let $W(\mathcal{O}_K)$ be the image of $\mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(\mathcal{O}_K))$ in $\mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(K))$ and let $W(R) = W(\mathcal{O}_K) \otimes_{\mathcal{O}_K} R$ for any $\mathcal{O}_K$-module R. Similarly define $V(R)$ using the parabolic cohomology of $\overline{\Gamma_1(N) \cap \Gamma_0(\ell)}$. (For a subgroup G of $SL_2(\mathbb{Z})$, $\bar{G}$ will denote its image in $PSL_2(\mathbb{Z})$.) Following Hida, we can define a pairing on $W(\mathcal{O}_K)$ which is perfect if $p \nmid N(k-2)!$ [H1, Th. 3.2], as is the pairing defined analogously on $V(\mathcal{O}_K)$. (Note that the constraint on p, together with the assumption $X \neq 0$, ensures that there are no elliptic elements of order p.)

The inclusions of $\Gamma_1(N) \cap \Gamma_0(\ell)$ in $\Gamma_1(N)$ and in $\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ naturally induce a homomorphism $W(R)^2 \to V(R)$. Let $A(K)$ be the image of $W(K)^2$ in $V(K)$, and $B(K)$ its orthogonal complement under the pairing (on $V(K)$). Then $V(K) = A(K) \oplus B(K)$, and under the natural action of the Hecke operators of level $N\ell$, $A(K)$, $B(K)$ and $V(\mathcal{O}_K)$ are respectively faithful $\mathcal{H}_X$, $\mathcal{H}_Y$ and $\mathcal{H}_Z$-modules (see [D, Prop. 3.1]). Therefore

$$\Omega = [A(K) + V(\mathcal{O}_K)] \cap [B(K) + V(\mathcal{O}_K)] \Big/ V(\mathcal{O}_K)$$

is an $\mathcal{H}_{X,Y}$-module.

As a generalization of Ihara's result [I, Lemma 3.2], we will prove in §3 the injectivity (if $p \nmid N(k-2)!$) of the induced map

$$\alpha : W(K/\mathcal{O}_K)^2 \to V(K/\mathcal{O}_K).$$

As an immediate consequence $\Omega \cong \ker(\beta \circ \alpha)$, where $\beta : V(K/\mathcal{O}_K) \to W(K/\mathcal{O}_K)^2$ is the adjoint of α with respect to the above pairings. This isomorphism is $\mathcal{H}_Z$-linear where for m prime to ℓ, T_m acts as the matrix $\begin{pmatrix} T'_m & 0 \\ 0 & T'_m \end{pmatrix}$ on $W(K/\mathcal{O}_K)^2$ (using primes to denote Hecke operators of level N), and T_ℓ as $\begin{pmatrix} T'_\ell & \ell^{k-1} \\ -\ell^{2-k}S'_\ell & 0 \end{pmatrix}$.

A straightforward computation then yields

$$\beta \circ \alpha = \begin{pmatrix} \ell+1 & T'^*_\ell \\ T'_\ell & \ell^{k-2}(\ell+1) \end{pmatrix}$$

(where T'^*_ℓ is adjoint to T'_l and satisfies $\ell^{k-2}T'_\ell = S'_\ell T'^*_\ell$). Since $S_\ell = \begin{pmatrix} S'_\ell & 0 \\ 0 & S'_\ell \end{pmatrix}$ on $W(K/\mathcal{O}_K)^2$, we have

$$T_\ell^2 - S_\ell = \begin{pmatrix} -S'_\ell & T'_\ell \\ 0 & -\ell^{2-k}S'_\ell \end{pmatrix} \circ \beta \circ \alpha.$$

Since S'_ℓ is an automorphism, we have $\ker(\beta \circ \alpha) = \ker(T_\ell^2 - S_\ell)$. Using Ribet's argument ([R1, p. 510] or [D, Prop. 3.4]), we deduce that $\mathrm{Ann}_{\mathcal{H}_X} \Omega \subseteq (T_\ell^2 - S_\ell)\mathcal{I}_X$ where $\mathcal{I}_X$ is the integral closure of $\mathcal{H}_X$ in $\mathcal{H}_X \otimes_{\mathcal{O}_K} K$. Now since Ω is an $\mathcal{H}_{X,Y}$-module, this implies

$$(*) \qquad (T_\ell^2 - S_\ell)\mathcal{H}_X \subseteq \pi_X(\ker \pi_Y) \subseteq (T_\ell^2 - S_\ell)\mathcal{I}_X,$$

where π_X and π_Y denote the appropriate projection maps of $\mathcal{H}_Z$.

We can replace Z by $Z^{(\chi)} = S_k(\Gamma_0(N\ell), \chi; K)$, where χ is a Dirichlet character defined mod N with values in K and consider the decomposition $Z^{(\chi)} = X^{(\chi)} \oplus Y^{(\chi)}$. If $p \nmid \frac{1}{2}\phi(N)$, then $\mathcal{H}_{Z^{(\chi)}}$ is a direct summand of $\mathcal{H}_Z$, and we can replace X and Y by $X^{(\chi)}$ and $Y^{(\chi)}$ in $(*)$. Now suppose $f = \sum a_n q^n$ is a newform of level N, weight k, character χ and coefficients in K. Suppose further that $x^2 - a_\ell x + \ell^{k-1}\chi(\ell)$ has roots $\alpha, \beta \in K$. Then $f_\alpha = f - \beta f(\ell z)$ is an eigenform of T_ℓ, and applying π_{Kf_α} to $(*)$ we get

$$\pi_{Kf_\alpha}(\ker \pi_{Y^{(\chi)}}) = (\alpha^2 - \chi(\ell)\ell^{k-2})\mathcal{O}_K.$$

Using the duality between the Hecke algebra and the lattice in Z of forms with integral coefficients to compute the congruence module [D, §2], we find

$$C_{Kf_\alpha, Y^{(\chi)}} \cong (\alpha^2 - \chi(\ell)\ell^{k-2})^{-1}\mathcal{O}_K \,/\, \mathcal{O}_K.$$

Noting that

$$(\alpha^2 - \chi(\ell)\ell^{k-2})(\beta^2 - \chi(\ell)\ell^{k-2})\mathcal{O}_K = (a_\ell^2 - \chi(\ell)\ell^{k-2}(\ell+1)^2)\mathcal{O}_K,$$

we see that if $p \nmid \frac{1}{2}\phi(N)N(k-2)!$, and $a_\ell^2 \equiv \chi(\ell)\ell^{k-2}(\ell+1)^2 \mod \mathfrak{p}$, then there exists $g \in R_\ell$ congruent to f modulo the maximal ideal of the ring of integers of $\bar{\mathbf{Q}}_p$. Conversely, if such a g exists, we deduce from properties of the associated Galois representations that $a_\ell^2 \equiv \chi(\ell)\ell^{k-2}(\ell+1)^2 \mod \mathfrak{p}$ [R1, p. 506]. This proves Theorem 1.

We can sharpen this result by decomposing $Y^{(\chi)} = Y^+ \oplus Y^-$, computing the appropriate congruence modules and applying a method of Wiles using Fitting ideals. We thus obtain Theorem 2; for further details, see [D, §4].

THEOREM 2. *For f as above, K sufficiently large and $p \nmid N\ell(k-2)!$, there exist integers d_i and distinct newforms $g_i \in Y^{(\chi)}$ with*

$$g_i \equiv f \mod \mathfrak{p}^{d_i} \quad \text{and} \quad \sum d_i \geq v_\mathfrak{p}(a_\ell^2 - \chi(\ell)\ell^{k-2}(\ell+1)^2) - 2v_\mathfrak{p}(2\phi(N)).$$

§3. Parabolic cohomology

In this section we prove the injectivity of α (Lemma 3.2). First recall that for a group G, a subset Q of G, and a G-module A, $\mathrm{H}^1_Q(G,A)$ is the subgroup of $\mathrm{H}^1(G,A)$ obtained from the cocycles u satisfying $u(\gamma) \in (\gamma - 1)A$ for all $\gamma \in Q$. For a congruence subgroup of $PSL_2(\mathbb{Z})$, we write $\mathrm{H}^1_P(G,A)$ for $\mathrm{H}^1_Q(G,A)$ where Q is the set of parabolic elements of G. We begin by proving the vanishing of a finite cohomology group necessary to the proof of Lemma 3.2. In many cases this is a consequence of [K-P-S, Th. 1.5.3].

LEMMA 3.1. *Let Q be a p-sylow subgroup of $G = SL_2(\mathbf{F}_p)$, and $\mathbf{F}_q$ a finite field of characteristic p. Then $\mathrm{H}^1_Q(G, L_n(\mathbf{F}_q)) = 0$ for $0 \leq n \leq p-1$.*

PROOF: We let Q act trivially on $\mathbf{F}_q$ and consider the induced module $\mathrm{Ind}_Q^G(\mathbf{F}_q)$, the set of functions from G/Q to $\mathbf{F}_q$. Identifying G/Q with the punctured plane $\mathbf{F}_p{}^2 \setminus \{(0,0)\}$, and $L_n(\mathbf{F}_q)$ with the space of homogeneous polynomials of degree n in $\mathbf{F}_q[x,y]$, we have an injection of G-modules $\phi : L_n(\mathbf{F}_q) \to \mathrm{Ind}_Q^G(\mathbf{F}_q)$ [A-S, p. 855], which induces

$$\phi_* : \mathrm{H}^1_Q(G, L_n(\mathbf{F}_q)) \to \mathrm{H}^1_Q(G, \mathrm{Ind}_Q^G(\mathbf{F}_q)).$$

Since Shapiro's isomorphism,

$$\mathrm{H}^1(G, \mathrm{Ind}_Q^G(\mathbf{F}_q)) \cong \mathrm{H}^1(Q, \mathbf{F}_q),$$

sends $\mathrm{H}^1_Q(G, \mathrm{Ind}_Q^G(\mathbf{F}_q))$ to $\mathrm{H}^1_Q(Q, \mathbf{F}_q) = 0$, we conclude that $\mathrm{H}^1_Q(G, \mathrm{Ind}_Q^G(\mathbf{F}_q)) = 0$.

We now need only prove ϕ_* is injective. By the long exact sequence of the cohomology, this will follow from the surjectivity of

$$(\mathrm{Ind}_Q^G(\mathbf{F}_q))^G \to (A_n(\mathbf{F}_q))^G,$$

where $A_n(\mathbf{F}_q)$ denotes the cokernel of ϕ. Since all functions from $\mathbf{F}_p{}^2$ to $\mathbf{F}_q$ are defined by polynomials, we can decompose (as G-modules)

$$\mathrm{Ind}_Q^G(\mathbf{F}_q) = \bigoplus_{j=0}^{p-2} M_j(\mathbf{F}_q),$$

where $M_j(\mathbf{F}_q)$ denotes those functions defined by homogeneous polynomials of degree $d \equiv j \mod (p-1)$. First note that $M_0(\mathbf{F}_q) = L_0(\mathbf{F}_q) \oplus L_{p-1}(\mathbf{F}_q)$, so the desired surjectivity holds for $n = 0$ or $p-1$. If $1 \leq n \leq p-2$, then we have an exact sequence of G-modules (see [A-S, Lemma 3.2])

$$0 \to L_n(\mathbf{F}_q) \xrightarrow{\phi} M_n(\mathbf{F}_q) \xrightarrow{\psi} L_{p-1-n}(\mathbf{F}_q) \to 0$$

where ψ is defined by

$$\psi(x^r y^{n+p-1-r}) = \begin{cases} \binom{r}{n} x^{r-n} y^{p-1-r}, & \text{if } n \leq r \leq p-1 \\ 0, & \text{otherwise.} \end{cases}$$

Surjectivity for such n then follows from the vanishing of $(L_{p-1-n}(\mathbf{F}_q))^G$.

LEMMA 3.2. *If $p \nmid N(k-2)!$, then α is injective.*

PROOF: We first reduce the problem to one involving the cohomology of principal congruence subgroups [R1, p. 511] by considering the commutative diagram,

$$\begin{array}{ccc} W(K/\mathcal{O}_K)^2 & \xrightarrow{\alpha} & V(K/\mathcal{O}_K) \\ \downarrow{\scriptstyle \gamma} & & \downarrow \\ \mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(K/\mathcal{O}_K))^2 & & \mathrm{H}^1_P(\overline{\Gamma_1(N) \cap \Gamma_0(\ell)}, L_n(K/\mathcal{O}_K)) \\ \downarrow{\scriptstyle \delta} & & \downarrow \\ \mathrm{H}^1_P(\overline{\Gamma(N)}, L_n(K/\mathcal{O}_K))^2 & \xrightarrow{\varepsilon} & \mathrm{H}^1_P(\overline{\Gamma(N) \cap \Gamma_o(\ell)}, L_n(K/\mathcal{O}_K)). \end{array}$$

We show α is injective by proving that γ, δ and ε are injective.

The map γ arises from the long exact sequence of the cohomology,

$$\cdots \to \mathrm{H}^1(\overline{\Gamma_1(N)}, L_n(\mathcal{O}_K)) \to \mathrm{H}^1(\overline{\Gamma_1(N)}, L_n(K)) \to \mathrm{H}^1(\overline{\Gamma_1(N)}, L_n(K/\mathcal{O}_K)) \to \cdots$$

If π generates a parabolic subgroup of $\overline{\Gamma_1(N)}$, then it is conjugate in $PSL_2(\mathbb{Z})$ to $\pm\left(\begin{smallmatrix}1 & d\\ 0 & 1\end{smallmatrix}\right)$ for some d dividing N. Since $p \nmid N(k-2)!$, we have

$$(\pi - 1)L_n(K) \cap L_n(\mathcal{O}_K) = (\pi - 1)L_n(\mathcal{O}_K),$$

and the exactness of

$$\mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(\mathcal{O}_K)) \to \mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(K)) \to \mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(K/\mathcal{O}_K)).$$

Recalling the definition of $W(K/\mathcal{O}_K)$, we see γ is injective.

Next consider the inflation-restriction exact sequence

$$\mathrm{H}^1(\mathbb{Z}/N\mathbb{Z}, L_n(K/\mathcal{O}_K)^{\overline{\Gamma(N)}}) \to \mathrm{H}^1(\overline{\Gamma_1(N)}, L_n(K/\mathcal{O}_K)) \to \mathrm{H}^1(\overline{\Gamma(N)}, L_n(K/\mathcal{O}_K)).$$

Note that $\mathbb{Z}/N\mathbb{Z}$ has order prime to p and $L_n(K/\mathcal{O}_K)$ is a p-group, so the restriction, and consequently δ, are injective.

The problem now is to prove that ε is injective. For $n = 0$, Ribet [R1, p. 513] appeals to the long exact sequence of Lyndon. We may do so for $n \geq 0$ to obtain

$$\mathrm{H}^1(\Gamma_N, L_n(K/\mathcal{O}_K)) \xrightarrow{\theta} \mathrm{H}^1(\overline{\Gamma(N)}, L_n(K/\mathcal{O}_K))^2 \to \mathrm{H}^1(\overline{\Gamma(N) \cap \Gamma_o(\ell)}, L_n(K/\mathcal{O}_K)),$$

where Γ_N is the principal congruence subgroup of level N in $PSL_2(\mathbb{Z}[\ell^{-1}])$. Now suppose $u \in Z^1(\Gamma_N, L_n(K/\mathcal{O}_K))$ with $\theta(\bar{u}) \in \mathrm{H}^1_P(\overline{\Gamma(N)}, L_n(K/\mathcal{O}_K))^2$. Let S be the set of elements of Γ_N conjugate in $PSL_2(\mathbb{Z}[\ell^{-1}])$ to $\pm\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$. Then if $\pi \in S$, $\pi^{\ell^M} \in \overline{\Gamma(N)}$ for sufficiently large M [R1, p. 513], and

$$(1 + \pi + \pi^2 + \cdots + \pi^{\ell^M - 1})u(\pi) = u(\pi^{\ell^M}) \in (\pi^{\ell^M} - 1)L_n(K/\mathcal{O}_K).$$

Since $(1 + \pi + \pi^2 + \cdots + \pi^{\ell^M - 1})$ is an automorphism of $L_n(K/\mathcal{O}_K)$, we conclude that $\bar{u} \in \mathrm{H}^1_S(\Gamma_N, L_n(K/\mathcal{O}_K))$. So if this group vanishes, then ε is injective.

Multiplication by a uniformizer Π in K leads to a long exact sequence

$$\cdots \to \mathrm{H}^1(\Gamma_N, L_n(\mathbb{F}_q)) \to \mathrm{H}^1(\Gamma_N, L_n(K/\mathcal{O}_K)) \xrightarrow{\Pi} \mathrm{H}^1(\Gamma_N, L_n(K/\mathcal{O}_K)) \to \cdots.$$

If π is conjugate in $PSL_2(\mathbb{Z}[\ell^{-1}])$ to $\pm\left(\begin{smallmatrix}1 & d\\ 0 & 1\end{smallmatrix}\right)$ with $d \in \mathbb{Z}[\ell^{-1}]$ prime to p, then we have $(\pi - 1)L_n(K/\mathcal{O}_K) \cap L_n(\mathfrak{p}^{-1}\mathcal{O}_K/\mathcal{O}_K) = (\pi - 1)L_n(\mathfrak{p}^{-1}\mathcal{O}_K/\mathcal{O}_K)$. Since any element of S is the power of such a π, we in fact have the exactness of

$$\mathrm{H}^1_S(\Gamma_N, L_n(\mathbb{F}_q)) \to \mathrm{H}^1_S(\Gamma_N, L_n(K/\mathcal{O}_K)) \xrightarrow{\Pi} \mathrm{H}^1_S(\Gamma_N, L_n(K/\mathcal{O}_K)).$$

So it suffices to prove $\mathrm{H}^1_S(\Gamma_N, L_n(\mathbf{F}_q)) = 0$. For if so, multiplication by Π is injective on $\mathrm{H}^1_S(\Gamma_N, L_n(K/\mathcal{O}_K))$, whose elements are p-torsion.

For this key step we use the inflation-restriction exact sequence,

$$\mathrm{H}^1(G, L_n(\mathbf{F}_q)) \to \mathrm{H}^1(\Gamma_N, L_n(\mathbf{F}_q)) \to \mathrm{H}^1(\Gamma_{Np}, L_n(\mathbf{F}_q)),$$

where $G = PSL_2(\mathbf{F}_p)$ if $N = 1$ or 2, and $SL_2(\mathbf{F}_p)$ if $N > 2$. Again Γ_{Np} is the principal congruence subgroup of level Np in $PSL_2(\mathbf{Z}[\ell^{-1}])$. As for the parabolic cohomology, this gives the exactness of

$$\mathrm{H}^1_Q(G, L_n(\mathbf{F}_q)) \to \mathrm{H}^1_S(\Gamma_N, L_n(\mathbf{F}_q)) \to \mathrm{H}^1_{S\cap\Gamma_{Np}}(\Gamma_{Np}, L_n(\mathbf{F}_q)),$$

where Q is a p-sylow subgroup of G. The first term vanishes as a consequence of Lemma 3.1. The third term vanishes since Γ_{Np} is generated by elements of $S \cap \Gamma_{Np}$ [R1, p. 513] and acts trivially on $L_n(\mathbf{F}_q)$. Hence the middle term vanishes, and the proof is complete.

References.

[A-S] A. Ash and G. Stevens, *Modular forms in characteristic ℓ and special values of their L-functions*, Duke Math. J. **53** (1986), 849–868.

[C] H. Carayol, *Sur les représentations Galoisiennes modulo ℓ attachées aux formes modulaires*, preprint.

[D] F. Diamond, *On congruence modules associated to Λ-adic forms*, Comp. Math. **71** (1989), 49–83.

[H1] H. Hida, *Congruences of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), 225–261.

[H2] H. Hida, *Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. **85** (1986), 545–613.

[I] Y. Ihara, *On modular curves over finite fields*, Proceedings of the International Colloquium on Discrete Subgroups of Lie Groups and Applications to Moduli, Bombay, January 1973, 161–202.

[J-L] B. Jordan and R. Livné, *Conjecture "Epsilon" for weight $k > 2$*, Bull. Amer. Math. Soc. (N.S.) **21**, 51–56.

[K-P-S] M. Kuga, W. Parry and C.-H. Sah, *Group cohomology and Hecke operators*, in "Manifolds and Lie Groups," Progress in Mathematics **14** (1980), 223–266, Birkhauser, Boston.

[R1] K. Ribet, *Congruence relations between modular forms*, Proc. I.C.M. (1983), 503–514.

[R2] K. Ribet, *On modular representations of* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, preprint.

[S] J-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.

[W] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.

Fred Diamond
Dept. of Mathematics
Boston University
Boston, MA 02215

Two-dimensional representations in the arithmetic of modular curves

B. Mazur K. A. Ribet

In the theory of automorphic representations of a reductive algebraic group G over a number field K, it is broadly — but not always — true that irreducible representations occurring in $L^2(G_{\mathbf{A}}/G_K)$ occur with multiplicity one. In a *classical special case* ($G = \mathbf{GL}(2)$, $K = \mathbf{Q}$, and where we restrict attention to automorphic representations which are holomorphic, cuspidal, and of weight 2), the Galois-theoretic counterpart of the above "multiplicity one phenomenon" is the assertion that given a newform of the above type, of level N, the (two-dimensional p-adic) $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation associated to it occurs *with multiplicity one* in the p-adic Tate module of $J_1(N)$.

For some important arithmetic applications, however, one is led to search for criteria guaranteeing certain analogues of the above "multiplicity one phenomenon" valid for the mod p Galois representations associated to newforms. The "mod p multiplicity" questions are somewhat more delicate than their p-adic counterparts. Indeed, to our knowledge, the main cases where the mod p Galois representation questions have been treated seriously so far are for cuspidal newforms of weight two which are either unramified at p [20, 30] or ordinary and nonspecial at p [25, 43].

The present article concerns itself with a "missing p-ordinary case," one for which the newform is "special" at p.[1] We assume, more precisely, that the level of the newform is divisible by p but not by p^2, and also that the Nebentypus character of the form is trivial. (Our method might also treat the more general case in which the character is unramified at p, but possibly non-trivial.) For the case where the character is ramified at p, see [12].

[1] We also require that the associated mod p Galois representation be absolutely irreducible, avoiding the important, but much more difficult, case of *Eisenstein primes* [20, 24].

This case arises in the second author's article [30] on Serre's conjectures. Assume that p is an odd prime, and suppose that ρ is an irreducible mod p representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which arises from the space of weight-2 modular forms on $\Gamma_o(M)$. (We then say that ρ is *modular of level* M.) Assume that $\ell \neq p$ is a prime factor of M for which ρ is unramified at ℓ. Then Serre's conjectures [37] predict that ρ is modular of level M_o, where M_o is the prime-to-ℓ part of M. This statement was proved by the first author [22] in case ℓ "exactly divides M" (i.e., $M_o = M/\ell$) and the congruence $\ell \equiv 1 \bmod p$ is *not* satisfied. (See [30], Theorem 6.1.) It was proved by the second author if ℓ exactly divides M and the newform giving ρ is unramified at p, i.e., p is prime to M ([30], Theorem 8.2). The methods of [30] show, more generally, that ρ is modular of level M_o whenever ℓ exactly divides M and ρ occurs with multiplicity one in the Jacobian $J_o(M)$. This motivated our interest in the mod p multiplicity one question for Galois representations.

The mod p multiplicity-one question for Galois representations has an intriguing, and relatively complicated, answer for twisted forms of $\mathbf{GL}(2)$ [32]. It would be quite interesting to have even a conjectural picture telling us what to expect for multiplicities of mod p Galois representations in a more general context.

We would like to thank Bas Edixhoven for enlightening conversations on subjects related to this article and for detailed comments on our preliminary versions. We also thank the IHES for providing the congenial setting in which much of this work was done.

Contents

1 Introduction and statement of the main theorem

1.1 The representations V_φ

Let M be a positive integer. Let $\Gamma_o(M)$ be (as usual) the subgroup of $\mathbf{SL}(2,\mathbf{Z})$ which consists of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbf{Z})$ with $c \equiv 0 \pmod{M}$. Let $X_o(M)$ be the associated modular curve over $\mathbf{Q}$. Finally, let T_n for $n \geq 1$ denote the standard Hecke correspondences on $X_o(M)$. (See, for example, [24], Chapter 2, §5 for a description of the Hecke operators T_q for q prime. When q divides M, our operator T_q is the "Atkin operator" denoted U_q in [24].)

These operators induce endomorphisms on the space $S_2(\Gamma_o(M))$ of weight-2 cusp forms on the group $\Gamma_o(M)$ and on the Jacobian

$$J = J_o(M) = \mathrm{Pic}^o(X_o(M))$$

of $X_o(M)$. We write simply T_n for each of these endomorphisms. (The endomorphism T_n of $J_o(M)$ is denoted T_n^* in [18].) The subrings of $\mathrm{End}(J_o(M))$ and of $\mathrm{End}(S_2(\Gamma_o(M)))$ which these operators generate are the "same." More precisely, the faithful operation of $\mathrm{End}(J_o(M))$ on $S_2(\Gamma_o(M))$ (coming from the fact that this latter space is the cotangent space of the abelian variety dual to $J_o(M)$) maps the endomorphism labeled T_n of $J_o(M)$ to the endomorphism of $S_2(\Gamma_o(M))$ labeled T_n. We let $\mathbf{T}_M$ be the subring of $\mathrm{End}(J_o(M))$

generated by the T_n, viewing this ring, when convenient, as operating on $S_2(\Gamma_o(M))$.

Let $\varphi : \mathbf{T}_M \to \overline{\mathbf{F}}_p$ be a ring homomorphism. The kernel of φ is a maximal ideal $\mathfrak{m} = \mathfrak{m}_\varphi$ of $\mathbf{T}_M$. As usual, we denote by $J[\mathfrak{m}]$ the "kernel of $\mathfrak{m}$ on J," i.e., the intersection of the kernels of all elements of $\mathfrak{m}$ acting on $J(\overline{\mathbf{Q}})$. This subgroup of the finite group $J[p]$ has natural commuting actions of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and of the residue field $k_\mathfrak{m} = T_M/\mathfrak{m}$. Further, the field $k_\mathfrak{m}$ is embedded in $\overline{\mathbf{F}}_p$ by φ. Let

$$V_\varphi := J[\mathfrak{m}] \otimes_{k_\mathfrak{m}} \overline{\mathbf{F}}_p.$$

Then V_φ is a finite-dimensional (continuous) representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$. The vector space V_φ is easily seen to be non-zero.

The representations $J[\mathfrak{m}]$ and V_φ may be compared with the canonical two-dimensional representation $\rho_\mathfrak{m}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which is associated to $\mathfrak{m}$ ([11], Th. 6.7 or [30], Prop. 5.1). Recall that this is the semisimple representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $k_\mathfrak{m}$, unique up to isomorphism, which is unramified outside the set of primes dividing pM and which satisfies

$$\mathrm{trace}(\rho_m(\sigma_r)) \equiv T_r \bmod \mathfrak{m}, \qquad \det(\rho_\mathfrak{m}(\sigma_r)) \equiv r \bmod \mathfrak{m}$$

for all primes r not dividing pM. (Here σ_r is a Frobenius element for r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) We define ρ_φ to be the representation $\rho_\mathfrak{m} \otimes_{k_\mathfrak{m}} \overline{\mathbf{F}}_p$, i.e., the representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ deduced from $\rho_\mathfrak{m}$ by the base change $k_\mathfrak{m} \to \overline{\mathbf{F}}_p$ induced by φ.

These two-dimensional representations are said to be *modular of level* M. More generally, suppose that $\mathbf{F}$ is an algebraic extension of $\mathbf{F}_p$. We say that a semisimple representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F})$ is modular of level M if there is an embedding $\iota : \mathbf{F} \hookrightarrow \overline{\mathbf{F}}_p$ so that ρ, when viewed over $\overline{\mathbf{F}}_p$ via ι, is isomorphic to some ρ_φ. It is equivalent to ask that the representation $\rho \otimes_\mathbf{F} \overline{\mathbf{F}}_p$ be of the form ρ_φ for *each* embedding $\iota : \mathbf{F} \hookrightarrow \overline{\mathbf{F}}_p$.

Assume that the two-dimensional representation $\rho_\mathfrak{m}$ *is irreducible.* Then by the Eichler-Shimura relations, the Cebotarev Density Theorem, and the Brauer-Nesbitt Theorem, one sees that the semisimplification of $J[\mathfrak{m}]$ as a $k_\mathfrak{m}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module is a direct sum of some number of copies of $\rho_\mathfrak{m}$ ([20], Chapter II,§14 or [30], Th. 5.2). Also, the representation ρ_φ is automatically an irreducible representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$, provided that $p \neq 2$.[2]

[2]According to a recent theorem of Boston, Lenstra and the second author [6], $J[\mathfrak{m}]$ is semisimple whenever ρ_φ is irreducible over $\overline{\mathbf{F}}_p$.

1.2 Questions of multiplicity

Definition 1 The *multiplicity* of $\rho_{\mathfrak{m}}$ in the representation $J[\mathfrak{m}]$ is the multiplicity of $\rho_{\mathfrak{m}}$ in the semisimplification of $J[\mathfrak{m}]$. We denote this integer by $\mu_{\mathfrak{m}}$ or μ_{φ}. We have $\mu_{\varphi} = \dim V_{\varphi}/2$.

The multiplicity $\mu_{\mathfrak{m}}$ is "typically" equal to 1. To cite the simplest possible example, take $M = 11$. Then $J_o(11)$ is an elliptic curve, $\mathbf{T} = \mathbf{Z}$, and the ideals $\mathfrak{m}$ are the prime ideals (p) of $\mathbf{Z}$. The kernel $J_o(11)[p]$ is then an $\mathbf{F}_p$-vector space of dimension two. In [20], the first author showed more generally that $\mu_{\mathfrak{m}} = 1$ when M is a *prime*, except perhaps in a small number of special situations when $p = 2$. (In these special situations, no example has been found where $\mu_{\mathfrak{m}} \neq 1$.) In [30] (Th. 5.2b), the second author employed the techniques of [20] to prove a theorem valid when M is not necessarily prime, but p does not divide $2M$.

MAIN THEOREM *Let $M = pN$, where N is prime to p. Let $\mathfrak{m}$ be a maximal ideal of the Hecke ring $\mathbf{T}_M$ with $\mathbf{T}/\mathfrak{m}$ of characteristic p. Suppose that $\rho_{\mathfrak{m}}$ is an absolutely irreducible representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Assume further that $\rho_{\mathfrak{m}}$ is not modular of level N. Then $\mu_{\mathfrak{m}} = 1$.*

The absolute irreducibility of $\rho_{\mathfrak{m}}$, is equivalent to the irreducibility of $\rho_{\mathfrak{m}}$ as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{T}/\mathfrak{m}$ whenever p is odd. This follows from the fact that $\rho_{\mathfrak{m}}(c)$, where c is a complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then has the distinct eigenvalues $+1$, -1 in $\mathbf{T}/\mathfrak{m}$.

The condition that $\rho_{\mathfrak{m}}$ is not modular of level N may be examined from varied perspectives. Serre conjectured in 1985 that $\rho_{\mathfrak{m}}$ is *finite* at p ([37], p. 189) if and only if $\rho_{\mathfrak{m}}$ is modular of level N ([36], Conjecture C_2, cf. [37]). This conjecture was proved by the first author soon afterwards: see [22], or [30], Theorem 6.1.

The condition may also be expressed in terms of newforms of weight 2. To say that $\rho_{\mathfrak{m}}$ is modular of level pN means, concretely, that it is a mod p representation attached to a weight-2 newform f, having trivial character, whose level divides pN. To say that it is not modular of level N then means that every f giving rise to $\rho_{\mathfrak{m}}$ has level divisible by p. In the language of representation theory, f is "special" at p in the sense that the component at p of the adelic representation of $\mathbf{GL}(2)$ associated to f is a special representation of $\mathbf{GL}(2, \mathbf{Q}_p)$. (See [25] for results in the case of weight-two p-ordinary modular forms which are not special at p.)

Suppose, more generally, that $\mathfrak{m} \subset \mathbf{T}_M$ is a maximal ideal, and assume that ρ_m is absolutely irreducible. What is the multiplicity of ρ_m in $J_o(M)[\mathfrak{m}]$?

In cases where the residue characteristic p of $\mathfrak{m}$ divides the integer M, we have little information other than that provided by the Main Theorem. For example, we have not been able to determine the multiplicity in all cases when $M = pN$ is as in the Main Theorem, but $\rho_{\mathfrak{m}}$ is modular of level N. We have been able to show, at least, that there are some cases where the multiplicity exceeds 1; those which we have discovered have M divisible by p^3 and $\rho_{\mathfrak{m}}$ modular of level M/p^2 (see §13 below).

The reader may wish to consult also [32], which gives a systematic construction of multiplicity-two examples for Jacobians of Shimura curves.

1.3 mod p Galois representations ρ and homomorphisms φ

The discussion of this section records some thoughts on placing the Main Theorem in a somewhat larger context. It will not be used in the rest of the article. For simplicity, we suppose throughout this discussion that p is a prime number different from 2 and 3.

We shall be concerned with mod p Galois representations arising from weight-two eigenforms with Nebentypus, whose associated Dirichlet characters have conductor prime to p. In other words, we shall consider cusp forms of weight two on groups of the form $\Gamma_1(N) \cap \Gamma_o(p^\nu)$, where N an integer prime to p and where $\Gamma_1(N)$ is, as usual, the subgroup of $\mathbf{SL}(2, \mathbf{Z})$ which is represented by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ which satisfy the congruences $a \equiv d \equiv 1$ and $c \equiv 0 \pmod{N}$.

There is a standard operation of $(\mathbf{Z}/N\mathbf{Z})^*$ on the space of such forms. For each $a \in (\mathbf{Z}/N\mathbf{Z})^*$, the corresponding automorphism of the space of cusp forms is the "diamond bracket operator" $\langle a \rangle$. This operator arises from an automorphism, again denoted $\langle a \rangle$, of the modular curve over $\mathbf{Q}$ which is associated with the subgroup $\Gamma_1(N) \cap \Gamma_o(p^\nu)$ of $\mathbf{SL}(2, \mathbf{Z})$. (See, for example, [18] for a discussion of $\langle a \rangle$ in varied guises.) In the context of $\Gamma_1(N) \cap \Gamma_o(p^\nu)$, we include the operators $\langle a \rangle$, for $a \in (\mathbf{Z}/N\mathbf{Z})^*$, along with the Hecke operators T_n, in defining $\mathbf{T}_{p^\nu N}$. A semisimple representation $\rho_\varphi \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_p)$ is again associated to each ring homomorphism $\varphi : \mathbf{T}_{p^\nu N} \to \overline{\mathbf{F}}_p$. This representation satisfies

$$\mathrm{trace}(\rho_\varphi(\sigma_r)) = \varphi(T_r), \qquad \det(\rho_\varphi(\sigma_r)) = \varphi(\langle r \rangle) r$$

for all prime numbers r which are prime to pN.

Similarly, for each $M \geq 1$, we have a diamond bracket operation of $(\mathbf{Z}/M\mathbf{Z})^*$ on the space of cusp forms of weight two on $\Gamma_1(M)$.

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_p)$ be a continuous, irreducible representation with odd determinant. Serre ([37],§3) has associated to such a representation three invariants: $N = N(\rho)$, $k = k(\rho)$, and $\epsilon = \epsilon(\rho)$. Here N is a positive integer prime to p (which we shall call *the tame level* of ρ), k is an integer ≥ 2 (the *weight* of ρ), and ϵ is a homomorphism from $(\mathbf{Z}/N\mathbf{Z})^*$ to $\overline{\mathbf{F}}_p^*$ (the *character* of ρ).

Given such a homomorphism $\epsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$, we have its multiplicative (or "Teichmüller") lifting $\epsilon_o : (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{Q}}_p^*$, the unique character of finite order prime to p which lifts ϵ.

Serre conjectures ([37] 3.2.3, 3.2.4) that there exists a classical (parabolic) newform over $\overline{\mathbf{Q}}_p$, on $\Gamma_o(N)$, with weight k and character ϵ_o, such that the mod p Galois representation associated to it (by the construction of Shimura when $k = 2$ and Deligne for $k > 2$) is equivalent to ρ. (As Serre has noted [38], his conjectures must be modified slightly in the cases $p = 2$ and $p = 3$. These cases have been excluded in our discussion.)

Suppose, now, that ρ is given with invariants (N, k, ϵ) and that Serre's conjecture holds for ρ, i.e., that there is a newform with invariants (N, k, ϵ_o) whose associated mod p Galois representation is equivalent to ρ. Suppose further that

$$k \equiv 2 \bmod p-1.$$

The determinant of ρ is then the product $\chi\epsilon$, where χ is the mod p cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This suggests that ρ arises from an eigenform of weight two on $\Gamma_1(N) \cap \Gamma_o(p^\nu)$ for some integer $\nu \geq 0$. If this is the case for a given ν, we shall refer to p^ν as a *wild level* for ρ.

PROPOSITION 1 *There is a newform with invariants $(p^\nu N, \epsilon_o, 2)$ whose associated mod p Galois representation is equivalent to ρ, for some $\nu \leq 2$.*

Proof. Using Theorem 3.5(d) of [4], we can find an integer j such that the twist of ρ by the j^{th} power of the mod p cyclotomic character arises from an eigenvector g in the space of weight-two cusp forms on $\Gamma_1(pN)$ over $\overline{\mathbf{F}}_p$. This eigenform may be chosen so that the diamond bracket operation of $(\mathbf{Z}/pN\mathbf{Z})^*$ on g is given as follows: the group $(\mathbf{Z}/N\mathbf{Z})^*$ operates via the character ϵ, and the group $(\mathbf{Z}/p\mathbf{Z})^*$ operates as the $(2j)^{\text{th}}$ power of the identity character $(\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{F}_p^*$. Equivalently, $(\mathbf{Z}/N\mathbf{Z})^*$ operates via (the mod p reduction of the character) ϵ_o, while $(\mathbf{Z}/p\mathbf{Z})^*$ operates via ω^{2j}, where ω is the unique Dirichlet character $(\mathbf{Z}/p\mathbf{Z})^* \to \overline{\mathbf{Q}}_p^*$ which lifts the identity character. After twisting g by ω^{-j}, we obtain a weight-two eigenform on the group $\Gamma_1(p^2N)$,

with character ϵ, whose associated Galois representation is ρ. (For a convenient discussion of the behavior of characters and levels of eigenforms under twisting, see [3], §3.) This eigenform is a modular form over $\overline{\mathbf{F}}_p$.

It follows by a well known lemma ([11], lemme 6.11) that ρ arises from a weight-two eigenform on $\Gamma_1(L)$, for some level L dividing p^2N. Further, the associated Dirichlet character of $(\mathbf{Z}/L\mathbf{Z})^*$ is a lift of the character ϵ. By [8], Prop. 3 (which applies because we have supposed $p \geq 5$), we may assume that this lift is ϵ_o. Also, we may suppose that the eigenform is a newform, possibly after replacing L by a divisor of L. (A short summary of the theory of newforms is presented in [28], §1.) The Proposition now follows from the fact that L is necessarily divisible by N ([8], §1.1 or [19], Proposition 0.1). □

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_p)$ be an irreducible representation as above, i.e., one of tame level N for which Serre's conjecture holds. Suppose that p^ν is a wild level for ρ.

Definition 2 A homomorphism $\varphi : \mathbf{T}_{p^\nu N} \to \overline{\mathbf{F}}_p$ is *associated* to ρ if the representations ρ and ρ_φ are isomorphic. The homomorphism $\varphi : \mathbf{T}_M \to \overline{\mathbf{F}}_p$ is *(p-)ordinary* if $\varphi(T_p) \neq 0$. It is *(p)-singular* if $\varphi(T_p) = 0$.

For each homomorphism φ associated to ρ, a multiplicity μ_φ is defined as above. The methods presented below should show that we have $\mu_\varphi = 1$ in the case where $\nu = 1$ and where p^ν is a minimal wild level for ρ, i.e., where ρ is not modular of level N. Similarly, the argument of [20], Chapter II, Proposition 14.2 (cf. [30], Proposition 5.1b) should prove that $\mu = 1$ whenever $\nu = 0$. (In both cases, one needs only to check that arguments given for forms on $\Gamma_o(N)$ work equally well for $\Gamma_1(N)$.) This suggests that the multiplicity μ_φ should be 1 in the remaining case where p^ν is a minimal wild level for ρ, i.e., that for which $\nu = 2$ and ρ does not arise from weight-2 forms on $\Gamma_1(N) \cap \Gamma_o(p)$. It would be very interesting to investigate this question.

We next discuss the extent to which φ is determined by ρ.

PROPOSITION 2 *There is at most one p-singular homomorphism φ associated to ρ.*

Proof. Let φ be a p-singular homomorphism φ associated to ρ. By definition, the image of T_p under φ is 0. The images of the diamond bracket operators $\langle a \rangle$, for $a \in (\mathbf{Z}/N\mathbf{Z})^*$, are the character values $\epsilon(a)$, where $\epsilon = \epsilon(\rho)$. Similarly, for each prime number r not dividing pN, $\varphi(T_r) = \mathrm{trace}(\rho_\varphi(\sigma_r))$. It remains

to show that the quantity $\varphi(T_r)$ is uniquely determined when r is a prime dividing N.

Let V be a two-dimensional $\overline{\mathbf{F}}_p$-vector space which is furnished with a continuous $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-action equivalent to ρ. For each prime $r \neq p$, let $I_r \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be an inertia group for r. We shall prove the formula

$$\varphi(T_r) = \mathrm{trace}(\sigma_r \mid V^{I_r}), \tag{1}$$

where V^{I_r} is the space of I_r-invariants on V.

For this, we recall that the formal power series $\sum_{n\geq 1} \varphi(T_n)q^n$ is a weight-two cusp form on $\Gamma_1(N)\cap\Gamma_o(p^\nu)$, with coefficients in $\overline{\mathbf{F}}_p$ (cf. [30], §5). This means that there is a cusp form on this group, with coefficients in the "integer ring" $\mathcal{O}$ of $\mathbf{Q}_p$, whose q-expansion reduces to $\sum_{n\geq 1} \varphi(T_n)q^n$ modulo the maximal ideal $\mathfrak{p}$ of $\mathcal{O}$. The form $\sum_{n\geq 1} \varphi(T_n)q^n$ is an eigenform for the Hecke operators T_n, with eigenvalues $\varphi(T_n)$.

By a well known lemma ([11], 6.11), one may find an eigenform $f = \sum a_n q^n$ with coefficients in $\mathcal{O}$ whose eigenvalues λ_n lift the $\varphi(T_n)$. There is then a newform g of level dividing $p^\nu N$ whose n^{th} coefficient coincides with λ_n for n prime to pN. The level of g is in fact divisible by N. Indeed, let W be the $\mathfrak{p}$-adic representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ associated to f. According to results of Deligne, Langlands and Carayol (see [7]), the level of g is the conductor of W. Further, this conductor is divisible by the conductor $N = N(\rho)$ which Serre associates to V ([8], §1.1 or [19]).

Thus the conductors of V and W coincide locally at each prime $r \neq p$. Concretely, this equality means that the $\overline{\mathbf{F}}_p$-dimension of V^{I_r} agrees with the $\overline{\mathbf{Q}}_p$-dimension of the space W^{I_r} ([8], *loc. cit.*). By viewing V as the mod $\mathfrak{p}$ reduction of a lattice in W, we then obtain the congruence

$$\mathrm{trace}(\sigma_r \mid V^{I_r}) \equiv \mathrm{trace}(\sigma_r \mid W^{I_r}) \bmod \mathfrak{p}.$$

However, by the results of Deligne, Langlands and Carayol mentioned above, we have the equality

$$\mathrm{trace}(\sigma_r \mid W^{I_r}) = \lambda_r.$$

Since λ_r reduces to $\varphi(T_r)$ mod $\mathfrak{p}$, we find the desired congruence (1). □

Analogously, we find:

PROPOSITION 3 *There is at most one p-ordinary homomorphism φ associated to ρ.*

Proof. In view of the proof we have given for Proposition 2, the proposition will follow after we show that there is at most one possibility for $\varphi(T_p)$, given that $\varphi(T_p)$ is non-zero and that φ is associated to ρ.

PROPOSITION 4 ([23]) *Let φ be associated to ρ and suppose that $\varphi(T_p) \neq 0$. Then V, viewed as a representation of a decomposition group for p, D_p, in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, has a 1-dimensional unramified quotient on which σ_p acts by multiplication by $\varphi(T_p)$.*

This proposition follows from Theorem 9 of [23] (which, incidentally, requires the hypothesis $p > 3$ which we imposed above). It clearly implies that there is at most one non-zero possibility for $\varphi(T_p)$, since V cannot have two distinct unramified quotients. Indeed, the full representation V cannot be unramified at p, since the determinant of V is given by the character $\epsilon\chi$, which is *ramified* at p. (Note that $p \neq 2$ by assumption.) □

2 Admissible models and admissible morphisms

Let p be a prime number. Let K be a finite field extension of $\mathbf{Q}_p$, $\mathcal{O} \subset K$ its ring of integers, and k its residue field. Let $\mathcal{O}^{\mathrm{h}}$ be the completion of a strict henselization of $\mathcal{O}$, and denote by $\overline{k}$ the (algebraically closed) residue field of $\mathcal{O}^{\mathrm{h}}$. The *normalized valuation* on $\mathcal{O}^{\mathrm{h}}$ is the one which gives a uniformizer of $\mathcal{O}$ the value 1.

Let n be a positive integer. A complete local $\mathcal{O}^{\mathrm{h}}$-algebra R will be said to be of *type* n if there is an element $\zeta \in \mathcal{O}^{\mathrm{h}}$ of normalized valuation n, such that R is isomorphic (as complete local $\mathcal{O}^{\mathrm{h}}$-algebra) to $\mathcal{O}^{\mathrm{h}}[[X,Y]]/(XY-\zeta)$, where $\mathcal{O}^{\mathrm{h}}[[X,Y]]$ is the power series ring in the two variables X and Y over $\mathcal{O}^{\mathrm{h}}$. If R is of type n, then R is a rational singularity, and, in fact, an isolated normal singularity of type A_n in the sense of [1] (see also: [16] and [10] Chap. VI 6.9). If R is of type 1, then R is regular, and the images of X and Y provide a *regular sequence* for R. If R is of type $n > 1$, then R is not regular. Nevertheless, the scheme $\mathrm{Spec}\, R$ has a canonical (minimal) desingularization obtained by a series of blow-ups; the inverse image of the closed point of $\mathrm{Spec}\, R$ in this canonical desingularization is a chain of $n-1$ curves of genus zero. For a readable and graphic account of this blow-up procedure, at least in the analogous situation of complex surfaces, see Pinkham's survey article [26].

Say that a local $\mathcal{O}^{\mathrm{h}}$-algebra R is *admissible* if it is of type n for some positive integer n.

Let $\mathcal{X}$ be a proper flat $\mathcal{O}$-scheme. Then we will call $\mathcal{X}$ *admissible* if the closed fiber is reduced, every irreducible component of the closed fiber is a smooth curve, and the completions of the strict henselizations of the local rings of the scheme $\mathcal{X}$ at all closed points x at which the structure morphism $\mathcal{X} \to \operatorname{Spec} \mathcal{O}$ is non-smooth are admissible local $\mathcal{O}^{\mathrm{h}}$-algebras. A proper flat admissible $\mathcal{O}$-scheme has the property that its closed fiber is reduced, and is a union of smooth curves which possesses only ordinary double points as singularities. In particular, such a scheme $\mathcal{X}$ has only a finite number of non-regular points, and possesses a canonical minimal desingularization $\tilde{\mathcal{X}}$ obtained by punctual blow-ups.

Let $X_{/K}$ be a smooth, proper (not necessarily irreducible) curve. An *admissible model* for $X_{/K}$ over $\mathcal{O}$ is a proper flat model $X_{/\mathcal{O}}$ for $X_{/K}$ over $\operatorname{Spec} \mathcal{O}$ such that the scheme $X_{/\mathcal{O}}$ is admissible. If $X_{/\mathcal{O}}$ is admissible, then the canonical desingularization $\tilde{X}_{/\mathcal{O}}$ is also admissible.

Example 1 Let N be an integer relatively prime to p, and let $X_o(Np)_{/\mathbf{Q}_p}$ be Shimura's canonical model of the modular curve $X_o(Np)$ over $\mathbf{Q}_p$. Then the canonical model $X_o(Np)_{/\mathbf{Z}_p}$ as described in [10, 14] is *admissible* in the above sense. The special fiber of $X_o(Np)_{/\mathbf{Z}_p}$ is isomorphic to two copies of $X_o(N)_{/\mathbf{F}_p}$ intersecting transversally at each of the supersingular points, these supersingular points being of type A_n for some $n \geq 1$.

For a proof of this assertion, the reader can consult [10], Chapter VI, Theorem 6.9, where in fact a more general result (which will also be useful to us) is proved. Namely, let N be an integer prime to p, let H be a subgroup of $\mathbf{GL}(2, \mathbf{Z}/N\mathbf{Z})$, and let $H^{\sim}$ be the inverse image of H in $\mathbf{GL}(2, \hat{\mathbf{Z}})$. In [10], the coarse moduli scheme $M_{H^{\sim} \cap \Gamma_o(p)}$ over $\mathbf{Z}[\frac{1}{N}]$ is studied. Let $\mathcal{O} = \mathbf{Z}_p$ and let $X_o(p; H^{\sim})_{/\mathbf{Z}_p}$ be the pullback of $M_{H^{\sim} \cap \Gamma_o(p)}$ to $\mathbf{Z}_p$. (It should perhaps be noted that the scheme $X_o(p; H^{\sim})_{/\mathbf{Z}_p}$ is not necessarily irreducible, but this is not much of a bother.) The indicated theorem of [10] guarantees that $X_o(p; H^{\sim})_{/\mathbf{Z}_p}$ is admissible.

Consider a finite morphism

$$f : X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$$

between admissible $\mathcal{O}$-schemes which is surjective on generic fibers. It follows that f is finite and faithfully flat on generic fibers. The restriction of f to fibers over $\overline{k}$ has the property that it is again finite and surjective (but not necessarily flat).

If s_2 is any singular point of the fiber of X_2 over $\overline{k}$, denote by A_2 and B_2 the two irreducible components of $X_{2/\overline{k}}$ containing s_2. Let s_1 be a point of $X_{1/\overline{k}}$ in $f^{-1}(s_2)$.

Definition 3 The mapping f is said to be *equi-ramified* at s_1 if:

(a) *The point s_1 is singular in $X_{1/\overline{k}}$.* The two components of $X_{1/\overline{k}}$ containing s_1 then have the property that one of them (say, A_1) is mapped by f onto A_2 and the other (call it B_1) is mapped onto B_2.

(b) *The ramification indices at s_1 of the two mappings*

$$A_1 \to A_2 \qquad B_1 \to B_2$$

induced by f are equal.

If f, as above, is equi-ramified at s_1, we let the *ramification index* $e_f(s_1)$ of f at s_1 be the common ramification index of the two mappings $A_1 \to A_2$ and $B_1 \to B_2$.

Definition 4 The mapping f is said to be *admissible* if it is a finite morphism of admissible models, as above, which is equi-ramified at every point s_1 of $X_{1/\overline{k}}$ such that $f(s_1)$ is a singular point in $X_{2/\overline{k}}$.

We thank Bas Edixhoven for providing us with a proof of the following Proposition.

PROPOSITION 5 *Let*

$$f : X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$$

be a finite morphism between admissible models. Then f is an admissible morphism. If the schemes $X_{1/\mathcal{O}}$ and $X_{2/\mathcal{O}}$ are regular, then f is finite and flat; moreover, for s_1 any closed point of $X_{1/\overline{k}}$ such that $s_2 = f(s_1)$ is a singular point of $X_{2/\overline{k}}$, the ramification index $e_f(s_1)$ is 1 (i.e., f is unramified at s_1).

Proof. Without loss of generality, we may assume that $\overline{k} = k$. Let s_1 be a closed point of $X_{1/k}$ such that $s_2 = f(s_1)$ is a double point. For $i = 1, 2$, let R_i denote the completed local rings of the schemes $X_{i/\mathcal{O}}$ at s_i. Then the rings R_i are of the form

$$R_1 = A[[x, y]](xy - z^a), \qquad R_2 = A[[u, v]]/(uv - z^b),$$

where A is a complete discrete valuation ring, z is a uniformizer of A, and a, b are positive integers. The morphism f induces a morphism $\varphi\colon R_2 \to R_1$ of A-algebras which makes R_1 a finite R_2-algebra. Let Z_x, Z_y denote the irreducible components of $\operatorname{Spec} R_1/zR_1$ defined as the reduced subschemes with support $x = 0$ and $y = 0$, respectively. Interchanging x and y, if necessary, we may suppose that f maps Z_x and Z_y to the branches of $\operatorname{Spec} R_2/zR_2$ cut out by $u = 0$ and $v = 0$, respectively. In particular, $\varphi(u)$ is a unit at the generic point of Z_y and $\varphi(v)$ is a unit at the generic point of Z_x.

Form the complete regular local ring $R = A[[s,t]]/(st - z)$. Map the ring R_1 to R by sending x to s^a and y to t^a and send R_2 to R by composing φ with this homomorphism $R_1 \to R$. The homomorphisms of R_i to R are injections. The ring R is a unique factorization domain, and the factorization of z is given by $z = st$ (s and t being irreducible elements). Since $uv = z^b$ ($= s^b \cdot t^b$ in R), and since $\varphi(u)$ is a unit at the generic point of Z_y, the unique factorization of the image $\tilde{u}$ of u in R is given by $\tilde{u} = \tilde{\alpha} \cdot s^c$ where $\tilde{\alpha}$ is a unit of R, and c is a positive integer. For the same reason, the unique factorization of the image $\tilde{v}$ of v in R is given by $\tilde{v} = \tilde{\beta} \cdot t^d$ for $\tilde{\beta}$ a unit of R and d a positive integer. It follows that $\tilde{\alpha}\tilde{\beta} = 1$ and $c = d = b$. Now let $\mathcal{O}_s$, $\mathcal{O}_t$ denote the discrete valuation rings which are the localizations at the generic points of the irreducible components $s = 0$ and $t = 0$, respectively, in $\operatorname{Spec} R$. Let $\mathcal{O}_x$, $\mathcal{O}_y$, $\mathcal{O}_u$, $\mathcal{O}_v$ be the analogously defined discrete valuation rings for x, y, u and v. Their residue fields are respectively $k((t))$, $k((s))$ and $k((y))$, $k((x))$, $k((v))$, $k((u))$, where k is A/zA, the residue field of A. All six of these discrete valuation rings have $z \in A$ as uniformizer. Therefore, the extensions

$$\mathcal{O}_u \subset \mathcal{O}_x \subset \mathcal{O}_s, \qquad \mathcal{O}_v \subset \mathcal{O}_y \subset \mathcal{O}_t$$

have degrees equal to the degrees of the corresponding residue field extensions

$$k((u)) \subset k((x)) \subset k((s)), \qquad k((v)) \subset k((y)) \subset k((t)).$$

In view of the two equalities

$$[k((s)) : k((u))] = [k((s)) : k((x))] \cdot [k((x)) : k((u))],$$

$$[k((t)) : k((v))] = [k((t)) : k((y))] \cdot [k((y)) : k((v))],$$

we have $b = a \cdot n$, where n is the (common) degree

$$n = [k((x)) : k((u))] = [k((y)) : k((v))].$$

Hence $\tilde{\alpha} \cdot \tilde{x}^n = \tilde{u}$ and $\tilde{\alpha}^{-1} \cdot \tilde{y}^n = \tilde{v}$, giving that

$$\varphi(u) = \alpha \cdot x^n \text{ and } \varphi(v) = \alpha^{-1} y^n,$$

for α a suitable unit in R_1. In particular, f is admissible, the ramification index $e_f(s_1)$ is equal to n, and we have established the first assertion of the Proposition.

Suppose now that the schemes $X_{i/\mathcal{O}}$ are regular. Then $a = b = 1$, and so $n = e_f(s_1)$ is also equal to 1. Since f is a finite morphism between regular (equidimensional) schemes of the same dimension, it follows that f is finite and flat; for a proof of this, see [14], *Notes added in proof*, pp. 507–508. □

PROPOSITION 6 *Let M and N be positive integers such that M divides N and N is relatively prime to p. Then the natural mapping*

$$X_o(Np)_{/\mathbf{Z}_p} \to X_o(Mp)_{/\mathbf{Z}_p},$$

composed, before and after, with any automorphisms of the domain and range $\mathbf{Z}_p$-schemes, is an admissible morphism of admissible schemes.

Proof. We will prove (and make use of) a more general assertion. Let H_1 and H_2 be subgroups of $\mathbf{GL}(2, \mathbf{Z}/N\mathbf{Z})$ with $H_1 \subseteq H_2$, and let $H_1\tilde{}$ and $H_2\tilde{}$ be their inverse images in $\mathbf{GL}(2, \hat{\mathbf{Z}})$. Let $X_o(p; H_1\tilde{})_{/\mathbf{Z}_p}$ and $X_o(p; H_2\tilde{})_{/\mathbf{Z}_p}$ be the corresponding modular curves, as in Example 1 above. Consider the natural projection

$$X_o(p; H_1\tilde{})_{/\mathbf{Z}_p} \to X_o(p; H_2\tilde{})_{/\mathbf{Z}_p},$$

and let h be a composition of this map with automorphisms of the source and target $\mathbf{Z}_p$-schemes. Then we have

PROPOSITION 7 *The mapping h is admissible.*

Proof. By the discussion in Example 1 above, the domain and range of h are admissible schemes over $\mathbf{Z}_p$. The morphism h being finite, Proposition 5 implies the statement of our Proposition. □

3 The graph S

Let $X_{/\mathcal{O}}$ be admissible, and denote by $Z_{/k} \to X_{/k}$ the normalization of the special fiber. Thus $Z_{/k}$ is a disjoint union of smooth projective curves over k. By the *graph of our model*, we mean the usual graph S (or $S(\bar{k})$ to emphasize its dependence on the choice of an algebraic closure, $\bar{k}$) of its special fiber. In other words, the set of *vertices of* $S(\bar{k})$ is the set of irreducible components

of $X_{/\overline{k}}$ (or equivalently, of $Z_{/\overline{k}}$) and the set of *edges* of $S(\overline{k})$ is $\mathrm{Sing}(X_{/\overline{k}})$, the set of singular points of $X_{/\overline{k}}$. The incidence relations are the evident ones, i.e., inverse-inclusion, and the graph $S(\overline{k})$ is endowed with a natural action of $\mathrm{Gal}(\overline{k}/k)$.

By $H_1(S, W)$ we mean the singular (first) homology group of the graph S, with coefficients in an abelian group W. We may view $H_1(S, W)$ explicitly as follows (cf. [13], IX 12.3.5). The *oriented edges* of the graph $S(\overline{k})$ are in 1-1 correspondence with points $\mathbf{s}$ on $Z_{/\overline{k}}$ which lie over singular points $s \in \mathrm{Sing}(X_{/\overline{k}})$. Since each s is an ordinary double point, there are two oriented edges lying over each singular point s. A 1-chain with values in W is a formal sum $\sum w_{\mathbf{s}} \cdot \mathbf{s}$ where the summation is taken over oriented edges, the coefficients are drawn from W, and we have $w_{\mathbf{s}} = -w_{\mathbf{s}'}$ whenever $\mathbf{s}$ and $\mathbf{s}'$ are the two oriented edges lying over a given $s \in \mathrm{Sing}(X_{/\overline{k}})$. For each $\mathbf{s}$, let $A(\mathbf{s})$ be the irreducible component of $Z_{/\overline{k}}$ containing $\mathbf{s}$, and set

$$\partial(\sum w_{\mathbf{s}} \cdot \mathbf{s}) := \sum w_{\mathbf{s}} \cdot A(\mathbf{s}),$$

where the right-hand sum is considered as formal sum, with coefficients in W, on the set of components of $Z_{/\overline{k}}$. The group $H_1(S, W)$ is then the subgroup of the group of 1-chains consisting of those 1-chains $\sum w_{\mathbf{s}} \cdot \mathbf{s}$ which are annihilated by ∂. This condition means that for each irreducible component A we have $\sum w_{\mathbf{s}} = 0$, where the summation is taken over all oriented edges $\mathbf{s}$ which correspond to points lying on A.

We shall view $H_1(S, \overline{k}) = H_1(S(\overline{k}), \mathbf{F}_p) \otimes \overline{k}$ as a $\mathrm{Gal}(\overline{k}/k)$-module via the *diagonal* action.

Let $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ be an admissible mapping. Let $Z_{i/k} \to X_{i/k}$ be the normalizations of the special fibers of the domain and range of f and let $S_i(\overline{k})$ denote the associated graphs ($i = 1$ and 2). The mapping f induces a map on special fibers $Z_1 \to Z_2$ over k and a $\mathrm{Gal}(\overline{k}/k)$-equivariant mapping of graphs $S_1 \to S_2$. This latter mapping is surjective on vertices and edges; it collapses an edge of S_1 if and only if the corresponding singular point x_1 of $X_{1/\overline{k}}$ maps to a smooth point of $X_{2/\overline{k}}$. For each abelian group W, we define

$$f_* : H_1(S_1, W) \to H_1(S_2, W)$$

to be the map on homology which is induced by this equivariant mapping. Further, we define

$$f^* : H_1(S_2, W) \to H_1(S_1, W)$$

by defining f^* on oriented edges as follows: $f^*(\mathbf{s}_2) = \sum e_f(s_1) \cdot \mathbf{s}_1$, where the summation is taken over all oriented edges $\mathbf{s}_1$ of the special fiber of X_1 which

map, via f, to the oriented edge $\mathbf{s}_2$ of the special fiber of X_2. Here, $e_f(s_1)$ is the ramification index of the unoriented edge s_1 (i.e., the unoriented edge "underlying" $\mathbf{s}_1$). It is straightforward to check that f^* so defined brings 1-cycles to 1-cycles, i.e., induces a mapping $f^*\colon H_1(S_2, W) \to H_1(S_1, W)$, and that $f^* f_*$ is given by multiplication by $\deg(f)$.

In what follows, we will concentrate on the $\mathrm{Gal}(\overline{k}/k)$-equivariant mappings $f_*\colon H_1(S_1, \overline{k}) \to H_1(S_2, \overline{k})$ and $f^*\colon H_1(S_2, \overline{k}) \to H_1(S_1, \overline{k})$ on homology.

PROPOSITION 8 *The homotopy type of the graph S is functorially dependent only upon $X_{/K}$ and not upon the choice of admissible model $X_{/\mathcal{O}}$.*

Proof. The essential fact used in the demonstration of this proposition is that any two (admissible) models $X_{/\mathcal{O}}$ and $X'_{/\mathcal{O}}$ of the same curve $X_{/K}$ are commensurable via blow-ups at points on the special fiber [15, 39]. This being the case, one must show that the homotopy type of S is independent of such blow-ups, which is straightforward. □

4 $\mathrm{Pic}^o(X_{/\mathcal{O}})$

Let $X_{/\mathcal{O}}$ be admissible, and let $\tilde{X}_{/\mathcal{O}} \to X_{/\mathcal{O}}$ be its canonical desingularization. Let Pic^o be the functor which is studied by Raynaud in [27]. Since X has rational singularities, the induced morphism of functors

$$\mathrm{Pic}^o(X_{/\mathcal{O}}) \to \mathrm{Pic}^o(\tilde{X}_{/\mathcal{O}})$$

is an isomorphism. Indeed, this can be seen by a computation of the mapping on tangent spaces induced by the above morphism using the Leray spectral sequence for the mapping $\varphi : \tilde{X} \to X$, and relative coherent cohomology over $\mathcal{O}$. More precisely, since φ is the "blowing down" morphism of a rational singularity, one calculates:

LEMMA 1 *We have*

$$R^q\varphi_*\mathcal{O}_{\tilde{X}} = \begin{cases} 0 & \text{for } q > 0, \\ \mathcal{O}_X & \text{for } q = 0. \end{cases}$$ □

Since the functor $\mathrm{Pic}^o(\tilde{X}_{/\mathcal{O}})$ is representable by a smooth group scheme over $\mathcal{O}$, so is $\mathrm{Pic}^o(X_{/\mathcal{O}})$. We refer to the group scheme representing $\mathrm{Pic}^o(X_{/\mathcal{O}})$ simply as $\mathrm{Pic}^o(X_{/\mathcal{O}})$.

Let $A_{/\mathcal{O}}$ denote the Néron model over the base $\mathcal{O}$ of the abelian variety $A = \mathrm{Pic}^o(X_{/K})$. (The recent publication [5] may be consulted as a source book on Néron models. It contains, in particular, a detailed discussion of Néron models of Jacobians of curves.) By Raynaud's theorem (for statements, compare: [24] Chap. 2 Prop. 1, [9] Theorem 2.5, [13] IX 12.1 and [27]), which applies to $\tilde{X}_{/\mathcal{O}}$ since $\tilde{X}_{/\mathcal{O}}$ is a regular surface with reduced special fiber, the natural homomorphism of group schemes over $\mathcal{O}$, $\mathrm{Pic}^o(X_{/\mathcal{O}}) \to A_{/\mathcal{O}}$ identifies $\mathrm{Pic}^o(X_{/\mathcal{O}})$ with the open subgroup scheme $A^o_{/\mathcal{O}}$ (the connected component containing the identity) of $A_{/\mathcal{O}}$. We have natural morphisms

$$\begin{aligned} f_* &: \mathrm{Pic}^o(X_{1/K}) \to \mathrm{Pic}^o(X_{2/K}) \\ f^* &: \mathrm{Pic}^o(X_{2/K}) \to \mathrm{Pic}^o(X_{1/K}) \end{aligned} \tag{2}$$

since f is finite and flat on generic fibers. From (2), and functoriality of the Néron model we obtain direct and inverse image mappings

$$\begin{aligned} f_* &: A_{1/\mathcal{O}} \to A_{2/\mathcal{O}} \\ f^* &: A_{2/\mathcal{O}} \to A_{1/\mathcal{O}} \end{aligned} \tag{3}$$

which by restriction to connected components and the identification described above yield:

$$\begin{aligned} f_* &: \mathrm{Pic}^o(X_{1/\mathcal{O}}) \to \mathrm{Pic}^o(X_{2/\mathcal{O}}) \\ f^* &: \mathrm{Pic}^o(X_{2/\mathcal{O}}) \to \mathrm{Pic}^o(X_{1/\mathcal{O}}). \end{aligned} \tag{4}$$

By restriction to the closed fiber, we have morphisms

$$\begin{aligned} f_* &: \mathrm{Pic}^o(X_{1/k}) \to \mathrm{Pic}^o(X_{2/k}) \\ f^* &: \mathrm{Pic}^o(X_{2/k}) \to \mathrm{Pic}^o(X_{1/k}), \end{aligned} \tag{5}$$

In (2)–(5), the composition f^*f_* of direct and inverse image mappings is given by multiplication by $\deg(f)$. Moreover, the inverse image mapping in (5) is the natural pullback morphism.

5 Semi-stable filtrations

Let $X_{/\mathcal{O}}$ be admissible. We shall recall and compare the standard filtrations on (a) the special fiber $A_{/k}$ and (b) the p-divisible group associated to the generic fiber $A_{/K}$.

(a) As for the special fiber $A_{/k}$, we have the three-stage filtration:

$$0 \subset (A_{/k})^{\mathrm{t}} \subset (A_{/k})^{o} \subset A_{/k}, \tag{6}$$

where the superscripts ^{o} and $^{\mathrm{t}}$ refer to "connected component containing the identity" and "toric part," respectively.

Denote by $T_{/k}$ the toric part $(A_{/k})^{\mathrm{t}}$ and let $J_{/k}$ be the abelian variety $(A_{/k})^o/T_{/k}$. We have already remarked in §4 above that $\mathrm{Pic}^o(X_{/k})$ is isomorphic to $(A_{/k})^o$ by Raynaud's theorem. The natural normalization mapping $Z_{/k} \to X_{/k}$ induces a mapping $\varphi\colon \mathrm{Pic}^o(X_{/k}) \to \mathrm{Pic}^o(Z_{/k})$, which is a surjective mapping of group schemes over k. The kernel of φ can be identified with the subfunctor of $\mathrm{Pic}^o(X_{/k})$ whose $\overline{k}$-valued points are given by isomorphism classes of line bundles on $X_{/\overline{k}}$ which are trivial on each irreducible component of $X_{/\overline{k}}$. Since $\mathrm{Pic}^o(Z_{/k})$ is an abelian variety and since, from the above description, $\ker\varphi$ is seen to be a torus whose character group may be naturally identified with $H_1(S(\overline{k}), \mathbf{Z})$ (cf. [13], IX, 12.3.7), we have:

PROPOSITION **9** *The abelian variety* $\mathrm{Pic}^o(Z_{/k})$ *may be identified (via* φ*) with* $J_{/k}$*, the* abelian variety part *of* $\mathrm{Pic}^o(X_{/k})$ *while* $T_{/k}$*, the* toric part *of* $\mathrm{Pic}^o(X_{/k})$*, may be identified with* $\ker\varphi$*, whose character group is canonically isomorphic to* $H_1(S(\overline{k}), \mathbf{Z})$. □

It follows from this that the Néron model $A_{/\mathcal{O}}$ is semi-stable.

(b) As for the semi-stable filtration on p-divisible groups over K, let $A_{p/K}$ denote the p-divisible group (over K) attached to the abelian variety $A_{/K}$. We have the filtration of p-divisible groups over K:

$$0 \subset A_p^{\mathrm{t}} \subset A_p^{\mathrm{f}} \subset A_p \tag{7}$$

in which A_p^{t} denotes the maximal p-divisible subgroup of A_p over K which extends to the p-divisible group associated to a torus over $\mathcal{O}$, and where A_p^{f} is the maximal p-divisible subgroup of $A_{p/K}$ which extends to a p-divisible group over $\mathcal{O}$ (cf. [13] IX §5 and especially Raynaud's result quoted there (Thm. 5.8)). By a result of Tate [42], if there is an extension of a p-divisible group over K to $\mathcal{O}$, then that extension is unique (up to canonical isomorphism). Let, then, $A^{\mathrm{f}}_{p/\mathcal{O}}$ and $A^{\mathrm{t}}_{p/\mathcal{O}}$ denote the unique extensions of A_p^{f} and A_p^{t}, respectively, to $\mathcal{O}$.

By ([13] IX 5.2) the filtration (7) is self-dual in the sense that in the natural (Cartier) self-duality on the $\mathrm{Gal}(\overline{K}/K)$-module $\mathsf{Ta}(A_p(\overline{K}))$, the submodules $\mathsf{Ta}(A_p^{\mathrm{t}}(\overline{K}))$ and $\mathsf{Ta}(A_p^{\mathrm{f}}(\overline{K}))$ are the annihilator subspaces of each other, where Ta denotes "Tate module."

PROPOSITION 10 *There are canonical morphisms*

(i) $A^{\mathrm{f}}_{p/\mathcal{O}} \to A_{/\mathcal{O}}$

(ii) $A^{\mathrm{t}}_{p/\mathcal{O}} \to A^{\mathrm{f}}_{p/\mathcal{O}}$,

where (i) is a morphism in the evident sense (i.e., a direct limit of compatible morphisms on the kernels of multiplication by p^n *in the p-divisible group over* $\mathcal{O}$*, as n goes to infinity) extending the natural morphisms on the generic fiber, and where (ii) is an embedding of p-divisible groups over* $\mathcal{O}$ *extending the natural embedding on the generic fiber.*

Proof. The existence of the morphism (i) is a direct consequence of Raynaud ([13] IX 5.8). To see that (ii) is an embedding, note that the dual of $A^{\mathrm{t}}_{p/\mathcal{O}}$ is etale, and is consequently a (faithfully flat) quotient of the "etale quotient group" of $A^{\mathrm{f}}_{p/\mathcal{O}}$. The result then follows easily by dualizing. □

Starting with the morphism (i) of Proposition 10, we first pass to the special fiber, and then note that the resulting morphism factors through $(A_{/k})^o$ and hence through its associated p-divisible group. We obtain therefore a morphism

(iii) $$A^{\mathrm{f}}_{p/k} \to (A_{/k})^o_p.$$

of p-divisible groups over k.

PROPOSITION 11 *The above morphism is an isomorphism, and it identifies the p-divisible subgroup* $A^{\mathrm{t}}_{p/k}$ *of* $A^{\mathrm{f}}_{p/k}$ *with* $(A_{/k})^{\mathrm{t}}_p \subset (A_{/k})^o_p$.

Proof. This is the content of the isomorphisms (7.3.1)–(7.3.4) of [13]. □

Returning to the filtration (7) of p-divisible group schemes over K, and letting the "suffix" $[p^n]$ denote kernel of multiplication by p^n, we have the filtration

$$0 \subset A^{\mathrm{t}}_p[p^n] \subset A^{\mathrm{f}}_p[p^n] \subset A_p[p^n] \tag{8}$$

of finite (etale) group schemes over K. The Weil pairing $[\ ,\ ]$ defines a perfect (alternating) self-duality

$$A_p[p^n] \times A_p[p^n] \to \mu_{p^n}$$

with values in the scheme-theoretic kernel μ_{p^n} of multiplication by p^n in the multiplicative group $\mathbf{G}_{\mathrm{m}}$. The filtration (8) is auto-dual with respect to this pairing, in the sense that $A^{\mathrm{t}}_p[p^n]$ and $A^{\mathrm{f}}_p[p^n]$ are each other's annihilators. This follows from a simple argument using ([13] IX 5.2.2 or Prop. 5.6).

COROLLARY *Let W denote the module defined by the exact sequence*

$$0 \to A_p^{\mathrm{f}}[p](\overline{K}) \to A_p[p](\overline{K}) \to W \to 0.$$

Choose an algebraic closure $\overline{K}/K$ compatible with the choice of algebraic closure $\overline{k}/k$ of the residue field, giving a surjection

$$\iota : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{k}/k).$$

Use ι to endow the $\mathbf{F}_p[\mathrm{Gal}(\overline{k}/k)]$-module $H_1(S(\overline{k}), \mathbf{F}_p)$ with an action of the Galois group $\mathrm{Gal}(\overline{K}/K)$. Once $\overline{K}$ and ι are fixed, there is a canonical isomorphism of $\mathbf{F}_p[\mathrm{Gal}(\overline{K}/K)]$-modules,

$$W \approx H_1(S(\overline{k}), \mathbf{F}_p).$$

In particular, the action of $\mathrm{Gal}(\overline{K}/K)$ on W is unramified.

Proof. This is a straightforward calculation using the duality statement above combined with Proposition 9. (Cf. [13], IX, §11.6.) □

6 Rosenlicht differentials

Let $X_{/\mathcal{O}}$ be admissible, and let $Z_{/k} \to X_{/k}$ be the normalization mapping of its special fiber. If $s \in X(\overline{k})$ is a singular point, denote by $s_1, s_2 \in Z(\overline{k})$ the two points in its pre-image. If k' is a subfield of $\overline{k}$, a *Rosenlicht differential* on an open subscheme U of $X_{/k'}$ is a rational differential 1-form ω on V, the pre-image of U in $Z_{/k'}$, such that ω is regular on the complement in V of the pre-image of the singular locus of U and such that ω has, at worst, simple poles on the pre-image points $s_1, s_2 \in V(\overline{k})$ of each singular point s in $U(\overline{k}) \subset X(\overline{k})$ and such that ω has residues of opposite sign at these pre-image points:

$$\mathrm{res}_{s_1} \omega = -\mathrm{res}_{s_2} \omega. \tag{9}$$

The assignment

$$U \mapsto \text{ Rosenlicht differentials on } U$$

defines a coherent sheaf on X/k, which we denote simply Ω or $\Omega_{X_{/k}}$.

Remark. The reader might compare the above definition with ([33] bottom of page 177 and Theorem 8) and also ([35] Chapter IV, §3, n°9), where the notion of *regular differential* is defined on singular curves. Specifically, if

X is a complete singular (reduced) algebraic curve, a *regular differential* on X is defined to be a regular differential ω (in the ordinary sense) on the normalization X' of X, which has the property that

$$\sum_{s' \to s} \operatorname{res}_{s'}(g \cdot \omega) = 0.$$

Here, s is any $\overline{k}$-valued point of X, s' ranges over all points of X' lying over s, and g is an arbitrary rational function on X' which is regular at all points lying over s.

A global Rosenlicht differential ω on $X_{/\overline{k}}$ defines a simplicial 1-cycle with coefficients in $\overline{k}$ on the graph $S(\overline{k})$ in an evident manner. Indeed, let

$$c_\omega := \sum \operatorname{res}_{\mathbf{s}} \omega \cdot \mathbf{s},$$

where the sum runs over all points on $Z_{/\overline{k}}$ lying over some singular point of $X_{/\overline{k}}$. In view of (9), the sum c_ω is a 1-chain in the sense of §3. Moreover, this 1-chain is visibly a 1-cycle (i.e., satisfies $\partial(c_\omega) = 0$) because the sum of the residues of ω over all points in any irreducible component vanishes. Passing to the homology class of the cycle c_ω, we obtain a map

$$h : H^0(X_{/\overline{k}}, \Omega) \to H_1(S(\overline{k}), \overline{k}).$$

This map is $\operatorname{Gal}(\overline{k}/k)$-equivariant because of the formula

$$\sigma(\operatorname{res}_{\mathbf{s}} \omega) = \operatorname{res}_{\sigma \mathbf{s}}(\sigma\omega), \tag{10}$$

valid for $\sigma \in \operatorname{Gal}(\overline{k}/k)$, $\omega \in H^0(X_{/\overline{k}}, \Omega)$, and $\mathbf{s}$ a $\overline{k}$-valued point on Z.

PROPOSITION **12** *The map $h: \omega \mapsto c_\omega$ is a surjection*

$$H^0(X_{/\overline{k}}, \Omega) \to H_1(S(\overline{k}), \overline{k})$$

whose kernel may be identified with $H^0(Z_{/\overline{k}}, \Omega^1)$. We have, in other words, a $\operatorname{Gal}(\overline{k}/k)$-equivariant exact sequence:

$$0 \to H^0(Z_{/\overline{k}}, \Omega^1) \to H^0(X_{/\overline{k}}, \Omega) \xrightarrow{h} H_1(S(\overline{k}), \overline{k}) \to 0.$$

Proof. Left-exactness of the sequence in the statement of the Proposition is immediate. The surjectivity of h follows from a general fact: given any finite set $\mathcal{S}$ of points on a smooth projective curve over $\overline{k}$, and any mapping $r: \mathcal{S} \to \overline{k}$ such that the sum $\sum_{s \in \mathcal{S}} r(s)$ vanishes, there is a 1-differential ω on the curve with at worst simple poles on $\mathcal{S}$ as singularities and such that for each $s \in \mathcal{S}$ we have $\operatorname{res}_s(\omega) = r(s)$. □

COROLLARY *Let k' be an extension of k in $\overline{k}$, and let $G' = \mathrm{Gal}(\overline{k}/k')$. Then we have an exact sequence*

$$0 \to H^0(Z_{/k'}, \Omega^1) \to H^0(X_{/k'}, \Omega) \to H_1(S(\overline{k}), \overline{k})^{G'} \to 0. \tag{11}$$

Proof. Taking G'-invariants in the exact sequence of Proposition 12, we obtain (11). Indeed, it is well known that the 1-dimensional cohomology of G' with values in the $\overline{k}$-vector space $H^0(Z_{/\overline{k}}, \Omega^1)$ vanishes (Hilbert's Theorem 90). □

Now let $f: X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ be an admissible mapping. Then we have a series of induced "direct" and "inverse" image mappings f_*, f^* which fit into a diagram

$$\begin{array}{ccccccccc} 0 & \to & H^0(Z_{1/\overline{k}}, \Omega^1) & \to & H^0(X_{1/\overline{k}}, \Omega) & \to & H_1(S_1(\overline{k}), \overline{k}) & \to & 0 \\ & & f^* \uparrow\downarrow f_* & & f^* \uparrow\downarrow f_* & & f^* \uparrow\downarrow f_* & & \\ 0 & \to & H^0(Z_{2/\overline{k}}, \Omega^1) & \to & H^0(X_{2/\overline{k}}, \Omega) & \to & H_1(S_2(\overline{k}), \overline{k}) & \to & 0. \end{array} \tag{12}$$

The definition of f^* and f_* on regular differentials on $Z_{1/\overline{k}}$ and $Z_{2/\overline{k}}$ is given in the standard local manner, the definition of f_* being the usual trace construction on differentials using flatness of the morphism $Z_{1/\overline{k}} \to Z_{2/\overline{k}}$. To check that the trace mapping (which is defined *a priori* on rational differential 1-forms) extends to regular and to Rosenlicht differentials, we may use the characterization of Rosenlicht differentials which is given in the above Remark, together with the local calculation

$$\sum_{s' \mapsto s} \mathrm{res}_{s'}(\omega) = \mathrm{res}_s(\mathrm{Trace}_{Z_1/Z_2}(\omega))$$

for ω any rational differential 1-form on $Z_{1/\overline{k}}$ and for s' ranging through all points of $Z_{1/\overline{k}}$ lying over a point s of $Z_{2/\overline{k}}$. (Compare: [35], Chapter II, n°12, Lemma 4; or [2] Chapter VIII (3.7) and (4.4).)

The definition of f^* and f_* on the homology of the graphs is as given in §3.

PROPOSITION **13** *The above diagram (12) is commutative.*

Proof. Commutativity of the square(s) on the left is immediate. As for those on the right, it is a direct calculation, where in the case of commutativity involving f_* one uses the fact that $\mathrm{res}_s(f_*\omega) = f_*(\sum \mathrm{res}_{s'} \omega)$, where the summation is over all s' in Z_1 mapping to s in Z_2. □

7 Regular differentials on $X_{/\mathcal{O}}$

Let $X_{/\mathcal{O}}$ be admissible, and let $\tilde{X}_{/\mathcal{O}}$ be its canonical desingularization. The smooth loci $Y_{/\mathcal{O}}$ and $\tilde{Y}_{/\mathcal{O}}$ of the $\mathcal{O}$-schemes $X_{/\mathcal{O}}$ and $\tilde{X}_{/\mathcal{O}}$ are open subschemes consisting in the complements of the closed (finite) subschemes of ordinary double points in the special fibers of $X_{/\mathcal{O}}$ and $\tilde{X}_{/\mathcal{O}}$, respectively. Let $\Omega^1_{\tilde{Y}_{/\mathcal{O}}}$ denote the coherent sheaf of (relative) Kähler differentials on the smooth $\mathcal{O}$-scheme $\tilde{Y}_{/\mathcal{O}}$. Since $\tilde{X}$ is regular, the complement of $\tilde{Y}$ in $\tilde{X}$ consists in closed points of depth 2, and therefore the coherent sheaf $\Omega^1_{\tilde{Y}_{/\mathcal{O}}}$ has a unique extension (the direct image) to an invertible coherent sheaf on $\tilde{X}$, which we shall call $\Omega_{\tilde{X}_{/\mathcal{O}}}$.

Definition 5 Let $X_{/\mathcal{O}}$ be admissible. Let $\varphi\colon \tilde{X}_{/\mathcal{O}} \to X_{/\mathcal{O}}$ be the canonical desingularization. By the sheaf $\Omega_{X_{/\mathcal{O}}}$ we mean the direct image $\varphi_*\Omega_{\tilde{X}_{/\mathcal{O}}}$.

The sheaf $\Omega_{\tilde{X}_{/\mathcal{O}}}$ may be seen to be the relative dualizing sheaf of the $\mathcal{O}$-scheme $\tilde{X}$, and, as a consequence of this, together with the fact that $\varphi\colon \tilde{X} \to X$ consists in blowing up rational isolated singularities, one sees that $\Omega_{X_{/\mathcal{O}}}$ is an invertible $\mathcal{O}_X$-module, and is the relative dualizing sheaf of the $\mathcal{O}$-scheme X. Further, we have:

LEMMA 2 *The natural mappings*

$$i : \Omega_{\tilde{X}_{/\mathcal{O}}} \to \varphi^*\Omega_{X_{/\mathcal{O}}}, \qquad j : \varphi_*\Omega_{\tilde{X}_{/\mathcal{O}}} \to \Omega_{X_{/\mathcal{O}}}$$

are isomorphisms. □

Remark. It would be good to have a concise and complete reference for Duality Theory tailored to admissible models and, in particular, to modular curves over rings of integers in number fields. Lacking such a reference, we suggest [10] and [20] II 3 for a discussion of these issues, and especially [15] Chapter IV §4 for a more complete discussion, with some proofs.

Next, if $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping, we have "direct" and "inverse" image mappings f_*, f^* connecting $\Omega^1_{\tilde{Y}_{1/\mathcal{O}}}$ and $\Omega^1_{\tilde{Y}_{2/\mathcal{O}}}$. These extend uniquely to $\Omega^1_{\tilde{X}_{1/\mathcal{O}}}$ and $\Omega^1_{\tilde{X}_{2/\mathcal{O}}}$, since the schemes $\tilde{X}_{i/\mathcal{O}}$ are regular and the subschemes $\tilde{Y}_{i/\mathcal{O}}$ are the complements in $\tilde{X}_{i/\mathcal{O}}$ of points of codimension 2. Using Lemma 2, one constructs "direct" and "inverse" image mappings f_* and f^* connecting $\Omega_{X_{1/\mathcal{O}}}$ and $\Omega_{X_{2/\mathcal{O}}}$.

PROPOSITION **14** *(i) Let $X_{/\mathcal{O}}$ be admissible. There is a natural isomorphism of coherent sheaves over $X_{/k}$:*

$$\Omega_{X_{/\mathcal{O}}} \otimes k \approx \Omega_{X_{/k}}.$$

(ii) If $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping, then the direct and inverse image mappings f_*, f^* are compatible, in an evident sense, with the isomorphisms of (i) above for X_1 and X_2.

Proof. Part (i) is seen by local calculations where we distinguish the case of a neighborhood of a smooth point for the morphism f and that of a neighborhood of an ordinary double point of the fiber of f. Once (i) is established, (ii) follows easily. □

Now suppose that $X_{/\mathcal{O}}$ is admissible, and let $\mathrm{Cot}(A_{/\mathcal{O}})$ denote the cotangent space at the zero-section of the Néron model $A_{/\mathcal{O}}$. If $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping, let

$$f_*\colon \mathrm{Cot}(A_{1/\mathcal{O}}) \to \mathrm{Cot}(A_{2/\mathcal{O}})$$

be the mapping induced by $f^*\colon A_{2/\mathcal{O}} \to A_{1/\mathcal{O}}$, and define f^* on $\mathrm{Cot}(A_{2/\mathcal{O}})$ similarly.

PROPOSITION **15** *There is a natural identification*

$$H^0(X, \Omega_{X_{/\mathcal{O}}}) \approx \mathrm{Cot}(A_{/\mathcal{O}})$$

which is compatible with f^* and f_* whenever $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping.

Proof. This is standard. See the discussion in [21] §2 (e). □

8 Admissible correspondences

Let $X_{i/\mathcal{O}}$ $(i = 0, 1, 2)$ be admissible, and let $\begin{array}{ccc} & X_0 & \\ \swarrow & & \searrow \\ X_1 & & X_2 \end{array}$ be a diagram of admissible mappings $f_i\colon X_0 \to X_i$ $(i = 1, 2)$. Referring to such an *ordered* pair of admissible morphisms (f_1, f_2) by the single letter f, we call f an *admissible correspondence*. We think of f as a generalized admissible mapping $X_1 \rightsquigarrow X_2$. Set $f_* := f_{2*}{f_1}^*$ and $f^* := f_{1*}{f_2}^*$, so that we have direct and

inverse image mappings defined for the same panoply of instances that they have been defined, in the case of admissible mappings. If f is an admissible correspondence corresponding to the ordered pair (f_1, f_2), its *adjoint* is the admissible correspondence f' obtained by reversing the order, i.e., by using (f_2, f_1) in place of (f_1, f_2). Clearly, $f'_* = f^*$ and $f'^* = f_*$.

Let $X_{/\mathcal{O}}$ be admissible. A *commutative* subring

$$R \subset \mathrm{End}(A_{/K})$$

will be called *admissible* if it is generated by the direct and inverse image mappings f_* and g^* coming from admissible correspondences $\begin{array}{ccc} & X_0 & \\ \swarrow & & \searrow \\ X & & X \end{array}$ (with no *a priori* restriction on the admissible models $X_{0/\mathcal{O}}$ which may appear). By replacing correspondences by their adjoints, we may require in the definition that R be generated exclusively by inverse image or direct image mappings.

PROPOSITION **16** *For each $T \in R$, there are associated endomorphisms T_* and T^* on each of the following: $A_{/K}$, $A_{/\mathcal{O}}$, $A_{/k}$, $H^0(X, \Omega)$, $H^0(Z, \Omega^1)$, and $H_1(S, \overline{k})$. For fixed $T \in R$, the families of maps (T_*) and (T^*) are each compatible with the morphisms listed in Propositions 13–15.*

Proof. This is immediate from the statements of those Propositions. □

In the discussion which follows, we will be concerned principally with the maps (T_*). We use the phrase "covariant action" to suggest that T acts as T_* on a given object.

9 Local admissible data

For simplicity, we now suppose that $k = \mathbf{F}_p$. Let $X_{/\mathcal{O}}$ be an admissible model of its generic fiber X. We preserve much of the previous notation. Thus, for example, we let $Z_{/k}$ be the normalization of the special fiber $X_{/k}$ of $X_{/\mathcal{O}}$. In addition, we shall let Φ be the group of components of $A_{/k}$. We view Φ as a finite abelian group furnished with an action of $\mathrm{Gal}(\overline{k}/k)$ ([13], IX, §11).

Let R be a commutative subring of $\mathrm{End}(A_{/K})$ generated by admissible correspondences. Then R operates by functoriality on $A_{/k}$ and thereby (covariantly) on the component group Φ and the abelian variety $\mathrm{Pic}^o Z$. We let $\overline{R}$ be the image of R in $\mathrm{End}(\mathrm{Pic}^o Z)$. We consider the *covariant* action of R on $H^0(X_{/k}, \Omega)$.

Suppose that $\mathfrak{p} \subset R$ is a maximal ideal of residual characteristic p. Let $F = R/\mathfrak{p}$ be the residue field of R. We say that the triple $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is *local admissible data* if the following axioms are satisfied:

I. The image of $\mathfrak{p}$ in $\overline{R}$ is the unit ideal of $\overline{R}$.

II. The F-vector space $H^0(X_{/k}, \Omega)[\mathfrak{p}]$ has dimension ≤ 1.

III. If $p = 2$, then $\mathfrak{p}$ does not belong to the support of the R-module Φ.

Remark. To anticipate the application of our theory, it might help if we dropped these hints: We will be working in the context where $K = \mathbf{Q}_p$, and X is a classical modular curve. Axiom I will follow since $\mathfrak{p}$ will correspond to a p-newform, and since Z "involves" only forms of lower p-level, $\mathfrak{p}$ can have no support in $H^0(Z, \Omega^1)$. Axiom II will follow from a version of the "q-expansion principle." Axiom III results from the fact that the component group Φ is known to be "Eisenstein" in the situation we encounter [31]. Hence a prime $\mathfrak{p}$ of R can belong to the support of Φ only if the associated Galois representation is reducible.

PROPOSITION **17** *Let $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ be local admissible data. Let W be the module introduced in the Corollary to Proposition 11. Then*

$$\dim_F W[\mathfrak{p}] \leq 1.$$

Proof. By the Corollary to Proposition 11, it is equivalent to prove that

$$\dim_F H_1(S(\overline{k}), \mathbf{F}_p)[\mathfrak{p}] \leq 1.$$

By the Corollary to Proposition 12, and by Axiom I, we have for each k' an isomorphism

$$H^0(X_{/k'}, \Omega)[\mathfrak{p}] \approx H_1(S(\overline{k}), \overline{k})^{\mathrm{Gal}(\overline{k}/k')}[\mathfrak{p}].$$

Consider this isomorphism in the case where $k' = k = \mathbf{F}_p$, and let $G = \mathrm{Gal}(\overline{k}/\mathbf{F}_p)$. The proposition follows from the following lemma, in which we have put $Y := H_1(S(\overline{k}), \mathbf{F}_p)$.

LEMMA **3** *We have* $\dim_F Y[\mathfrak{p}] = \dim_F (Y \otimes_{\mathbf{F}_p} \overline{k})^G[\mathfrak{p}]$.

Proof. One first shows that the natural inclusion

$$Y[\mathfrak{p}] \otimes_{\mathbf{F}_p} \overline{k} \subset (Y \otimes_{\mathbf{F}_p} \overline{k})[\mathfrak{p}]$$

is an isomorphism (e.g., by proving this with $\overline{k}$ replaced by any finite subfield k', via a dimension count over $\mathbf{F}_p$, and then passing to $\overline{k}$ by direct limit). Since passage to the submodule of G-invariants commutes with passage to the kernel of $\mathfrak{p}$, we get that the natural inclusion

$$(Y[\mathfrak{p}] \otimes_{\mathbf{F}_p} \overline{k})^G \subset (Y \otimes_{\mathbf{F}_p} \overline{k})^G[\mathfrak{p}]$$

is also an isomorphism. This reduces us to the case where $Y = Y[\mathfrak{p}]$. In this case, the equality to be proved,

$$\dim_{\mathbf{F}_p} Y = \dim_{\mathbf{F}_p} (Y \otimes_{\mathbf{F}_p} \overline{k})^G,$$

is evident. □

10 Global admissible data

We now let $X_{/\mathbf{Q}}$ be a smooth projective curve over $\mathbf{Q}$, and denote by $A_{/\mathbf{Z}}$ the Néron model of its Jacobian over the base $\mathbf{Z}$. Let R be a subring of endomorphisms of $A_{/\mathbf{Q}}$ defined over $\mathbf{Q}$ (equivalently, a subring of $\mathrm{End}(A_{/\mathbf{Z}})$). Let $\mathfrak{p} \subset R$ be a maximal ideal of residual characteristic p. Let F be the residue field of $\mathfrak{p}$, as in §8. Let $X_{/\mathbf{Q}_p}$ denote the base extension of $X_{/\mathbf{Q}}$ to $\mathbf{Q}_p$. Let $\mathcal{O} = \mathbf{Z}_p$ and let $X_{/\mathcal{O}}$ be an admissible model of $X_{/\mathbf{Q}_p}$ over the base $\mathbf{Z}_p$. We shall say that $\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is *globally admissible data* if:

(a) It is *locally admissible*; i.e., $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is locally admissible in the sense of §9, and,

(b) The $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module $A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$ has a Jordan-Hölder filtration all of whose successive quotients are isomorphic to one absolutely irreducible $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module V for which $\dim_F V = 2$.

PROPOSITION **18 ("dimension two")** *Assume that*

$$\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$$

is globally admissible. Then $A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$ *is an* F*-vector space of dimension two.*

Proof. Let U denote the $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module $A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$. Then U is non-zero because R acts faithfully on A. By property (b) above, all minimal $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-submodules of U are isomorphic to V. Choose one such submodule, and identify it with V; this gives us an inclusion $V \subset U$.

Let $\dim_F U = 2N$, so that U possesses an $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-stable Jordan-Hölder filtration of N stages, each of whose "successive quotients" is isomorphic, as $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module, to V. We must prove that $N = 1$.

Fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$; use it to identify $U = A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$ with $A_{/\mathbf{Q}_p}[\mathfrak{p}](\overline{\mathbf{Q}}_p)$. Via this identification, U and its submodule V inherit filtrations (as $F[\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)]$-modules) from the filtration (8), made with $n = 1$:

$$\begin{array}{ccccccc} 0 & \subset & U^{\mathrm{t}} & \subset & U^{\mathrm{f}} & \subset & U, \\ 0 & \subset & V^{\mathrm{t}} & \subset & V^{\mathrm{f}} & \subset & V. \end{array}$$

Axiom I of §9 (coupled with Propositions 9 and 11) proves that $U^{\mathrm{t}} = U^{\mathrm{f}}$ and therefore that $V^{\mathrm{t}} = V^{\mathrm{f}}$. Further, since $U/U^{\mathrm{t}} = U/U^{\mathrm{f}}$ embeds in the module $W[\mathfrak{p}]$ of the previous §, and since, by Proposition 17, $W[\mathfrak{p}]$ is of F-dimension ≤ 1, the codimension c of U^{t} in U is at most 1.

The inertia subgroup I of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts trivially on U/U^{t} and as the mod p cyclotomic character χ on U^{t}. Hence the semisimplification of U as an I-module is the sum of c copies of the trivial representation and $2N - c$ copies of the 1-dimensional representation corresponding to χ. Meanwhile, this semisimplification is the sum of N copies of the semisimplification of V.

Assume now that p is an odd prime. Then χ is non-trivial, and we see that either $N = 1$ or else $U = U^{\mathrm{t}}$. We will eliminate the latter possibility, using the assumption that p is odd.

For this, we note first that the entire p-divisible group $A_p(\overline{\mathbf{Q}}) \otimes_R R_{\mathfrak{p}} = \bigcup A[\mathfrak{p}^i](\overline{\mathbf{Q}}_p)$ lies in the toric part A_p^{t} of the p-divisible group of A. Indeed, suppose that $A[\mathfrak{p}^i]$ lies in $A_p[p^n]$. Then, by Axiom I, to say that $A[\mathfrak{p}^i]$ is contained in $A_p^{\mathrm{t}}[p^n]$ is to say that it is contained in $A_p^{\mathrm{f}}[p^n]$. If not, then $A[\mathfrak{p}^i]$ maps non-trivially to $A_p[p^n]/A_p^{\mathrm{f}}[p^n]$, which is unramified, whereas the assumption $U = U^{\mathrm{t}}$ implies easily that $A[\mathfrak{p}^i]$ has no unramified quotient. (One uses the standard fact that $A[\mathfrak{p}^i]/A[\mathfrak{p}^{i-1}]$ maps injectively to a direct sum of copies of U, cf. [20], II, §14.)

We then conclude by using an argument due to Serre (compare [24], Chap. III §7). Let Γ be the $\mathbf{Q}_p$-adic Tate module associated to $A_p(\overline{\mathbf{Q}}) \otimes_R R_{\mathfrak{p}}$, and let Λ denote its h^{th} exterior power where h is the dimension of Γ. Let $\Lambda(-h)$ be the twist of Λ by the $-h$th power of the p-adic cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then $\Lambda(-h)$ is unramified at p, so that $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\Lambda(-h)$ via a character of finite order. Hence the eigenvalues of Frobenius

elements φ_ℓ on Λ (where $\ell \neq p$ is any prime of good reduction for A) are of the form $\ell^h\zeta$, where ζ is a root of unity. These eigenvalues thus have archimedean absolute values ℓ^h. However, the eigenvalues of φ_ℓ on Γ all have absolute values $\ell^{1/2}$, which is a contradiction.

We now consider the case $p = 2$. Then, by Axiom III, the maximal ideal $\mathfrak{p}$ does not belong to the support of Φ. Using this information, but making no further use of the assumption $p = 2$, we shall establish that U^{t} has dimension ≤ 1. Since its codimension is also bounded from above by 1, we get that U has dimension at most 2, so that $N = 1$ as desired.

Let $\mathcal{X}$ denote temporarily the character group $\mathrm{Hom}_{\overline{\mathbf{F}}_p}(A^{\mathrm{t}}_{/k}, \mathbf{G}_{\mathsf{m}})$ of the maximal torus in the reduction of A. Then $U^{\mathrm{t}} = \mathrm{Hom}(\mathcal{X}/\mathfrak{p}\mathcal{X}, \mu_p(\overline{\mathbf{Q}}_p))$. Hence the F-dimension of U^{t} is that of $\mathcal{X}/\mathfrak{p}\mathcal{X}$. If $\mathcal{Y}$ is the analogue of $\mathcal{X}$ for the reduction of the dual of A (so that $\mathcal{Y}$ and $\mathcal{X}$ are in fact isomorphic), then the monodromy pairing of SGA7I furnishes an exact sequence

$$0 \to \mathcal{Y} \to \mathrm{Hom}(\mathcal{X}, \mathbf{Z}) \to \Phi \to 0.$$

By considering the maps "multiplication by p" on the groups in this sequence, and by using the Snake Lemma, we find a 4-term exact sequence

$$0 \to \Phi[p] \to W \to \mathrm{Hom}(\mathcal{X}/p\mathcal{X}, \mathbf{F}_p) \to \Phi/p\Phi \to 0,$$

since W is canonically $\mathcal{Y}/p\mathcal{Y}$. If we localize at $\mathfrak{p}$, the two terms involving Φ disappear, because of Axiom III. Hence, localizing and then performing the operation "$[\mathfrak{p}]$" gives an isomorphism

$$W[\mathfrak{p}] \approx \mathrm{Hom}(\mathcal{X}/\mathfrak{p}\mathcal{X}, \mathbf{F}_p).$$

In view of Proposition 17, the dimension of the right-hand side is ≤ 1, as claimed. □

11 Modular curves and Hecke operators

Let N be an integer prime to p, and let $M = pN$. Let X be the complete modular curve $X_o(M)_{/\mathbf{Q}}$, which is associated with the subgroup $\Gamma_o(M)$ of $\mathbf{PSL}(2, \mathbf{Z})$. We will be working with this curve and its canonical model over $\mathbf{Z}[1/N]$. As we intimated in the Introduction, however, one could work equally well with the curve $X(N, p)$ attached to the subgroup $\Gamma_1(N) \cap \Gamma_o(p)$ of $\Gamma_o(pN)$. This subgroup is defined by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ which satisfy the

additional congruence $a \equiv d \equiv 1 \pmod{N}$. These two cases could be treated simultaneously by the introduction of a curve which lies between $X(N,p)$ and X in the natural covering $X(N,p) \to X$.

As we recalled in our introductory comments, the curve X is furnished with a standard Hecke correspondence T_n for each integer $n \geq 1$; the correspondence T_ℓ is frequently called U_ℓ when ℓ is a prime number dividing pN. The correspondences T_n induce endomorphisms of the Jacobian $J_o(pN) = \mathrm{Pic}^o(X)$ of X, which are again denoted T_n. (We use the convention which was explained in §3 of [30]. Thus, the endomorphism T_n is the transpose of the endomorphism ξ_n which is defined in Chapter 7 of [41].) Let $w = w_p$ be the Atkin-Lehner involution of X relative to the prime p, and write again w for the involution of $J_o(pN)$ induced by this operator.

Also, recall [21] that there are two *degeneracy maps*

$$\alpha = \delta_1, \beta = \delta_p : X \rightrightarrows X_o(N).$$

These correspond respectively to the modular operations

$$(E, C_N, C_p) \mapsto (E, C_N), \quad (E, C_N, C_p) \mapsto (E/C_p, (C_N + C_p)/C_p),$$

where C_N and C_p denote cyclic subgroups of orders N and p on an elliptic curve E. These degeneracy maps induce maps $\alpha_*, \beta_* : J_o(pN) \rightrightarrows J_o(N)$ and $\alpha^*, \beta^* : J_o(N) \rightrightarrows J_o(pN)$. The maps α^* and β^* each identify $J_o(N)$ with an abelian subvariety of $J_o(pN)$.

Consider now the following three closely related commutative subrings of $\mathrm{End}(J_o(pN))$:

- $S =$ the subring generated by the T_n with n prime to p,
- $\mathbf{T} = \mathbf{T}_{pN} =$ the subring generated by the T_n for all n,
- $R =$ the ring generated by S and w.

We have $\mathbf{T} = S[T_p] = S[U_p]$ and $R = S[w]$. All three rings are finitely generated as $\mathbf{Z}$-modules, since $\mathrm{End}(J_o(pN))$ is of finite rank over $\mathbf{Z}$.

We say that maximal ideals $\mathfrak{p} \subset R$ and $\mathfrak{m} \subset \mathbf{T}$ are *compatible* if their intersections with S coincide. By the "going-up" theorem of Cohen-Seidenberg, there is always at least one maximal ideal $\mathfrak{m}$ or $\mathfrak{p}$ compatible with a given $\mathfrak{p}$ or $\mathfrak{m}$.

Next, let $\overline{S}$ be the "p-old quotient" of S, defined (for instance) as the quotient of S cut out by $J_o(N)$, viewed as an abelian subvariety of $J_o(pN)$. In other words, we identify $J_o(N)$ with its image in $J_o(pN)$ under α^*, and

observe that this image is stable under T_n for all n prime to p. The subring of $\mathrm{End}(J_o(N))$ generated by these T_n is then the quotient $\overline{S}$ of S. (Alternatively, $\overline{S}$ may be defined as the image of S in $\overline{R}$, where $\overline{R}$ is defined as in §9, cf. [30], 3.11.) Note that $\overline{S}$ is a subring of the Hecke algebra $\mathbf{T}_N$, which is the subring of $\mathrm{End}(J_o(N))$ generated by *all* the Hecke operators T_n at level N. Thus $\mathbf{T}_N$ is the ring generated by $\overline{S}$ and the Hecke operator T_p at level N.

We call a maximal ideal $\mathfrak{m}_o$ of S *strongly p-new*, or simply *strongly new*, if it is not the inverse image in S of a maximal ideal of $\overline{S}$. Thus, "strongly p-new" means "not p-old." A maximal ideal $\mathfrak{m} \subset \mathbf{T}$ or $\mathfrak{p} \subset R$ is defined to be strongly (p-)new if its intersection with S is strongly new.

PROPOSITION **19** *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_{pN}$. Assume that $\rho_{\mathfrak{m}}$ is an irreducible representation which is not modular of level N. Then $\mathfrak{m}$ is strongly p-new.*

Proof. Let $\mathfrak{m}_o = \mathfrak{m} \cap S$. Assume that $\mathfrak{m}$ is not strongly p-new, so that $\mathfrak{m}_o$ is the inverse image of a maximal ideal I of $\overline{S}$. The residue field of I is then the quotient $S/\mathfrak{m}_o$, which is a subfield of $\mathbf{T}_{pN}/\mathfrak{m}$. Let J be a maximal ideal of $\mathbf{T}_N$ lying over I, and consider the representation ρ_J. For almost all prime numbers r, we have

$$\begin{aligned} \mathrm{trace}(\rho_m(\sigma_r)) &= T_r \bmod \mathfrak{m}_o = \mathrm{trace}(\rho_J(\sigma_r)), \\ \det(\rho_{\mathfrak{m}}(\sigma_r)) &= r \bmod \mathfrak{m} = \det(\rho_J(\sigma_r)), \end{aligned}$$

the equalities holding in the common subfield $S/\mathfrak{m}_o$ of $\mathbf{T}_{pN}/\mathfrak{m}$ and $\mathbf{T}_N/J$. (Here, σ_r is a Frobenius element for r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) By the Cebotarev density theorem, the representations $\rho_{\mathfrak{m}}$ and ρ_J are isomorphic in the sense that they both arise by base change from the same two-dimensional representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $S/\mathfrak{m}_o$. This contradicts the assumption that $\rho_{\mathfrak{m}}$ is not modular of level N. □

PROPOSITION **20** *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ which is strongly p-new. Then R acts on $J_o(pN)[\mathfrak{m}](\overline{\mathbf{Q}})$ via a surjective homomorphism $R \to \mathbf{T}/\mathfrak{m}$.*

Proof. The endomorphism $T_p + w$ of $J_o(pN)$ maps $J_o(pN)$ into the subvariety $\alpha^*(J_o(N))$ of $J_o(pN)$ (cf. [30], proof of Proposition 3.7). In particular, $T_p + w$ maps $J_o(pN)[\mathfrak{m}]$ into $J_o(N) \cap J_o(pN)[\mathfrak{m}_o]$, where $\mathfrak{m}_o$ is the intersection $S \cap \mathfrak{m}$. The group $J_o(N) \cap J_o(pN)[\mathfrak{m}_o]$ is killed by the image of $\mathfrak{m}_o$ in $\overline{S}$, which is the unit ideal of $\overline{S}$ by hypothesis. Hence $J_o(N) \cap J_o(pN)[\mathfrak{m}_o] = 0$, so

that $T_p = -w$ on $J_o(pN)[\mathfrak{m}]$. All generators of R now act on $J_o(pN)[\mathfrak{m}]$ as elements of $\mathbf{T}$, since $T_\ell \in R$ acts as $T_\ell \in \mathbf{T}$, for $\ell \neq p$. The result now follows; in particular, the action of R on $J_o(pN)[\mathfrak{m}](\overline{\mathbf{Q}})$ is given by a *surjective* homomorphism because each generator of $\mathbf{T}/\mathfrak{m}$ is, up to sign, the image of a generator of R. □

COROLLARY *Assume that* $\mathfrak{m}$ *is strongly p-new. Then we have*

$$J_o(pN)[\mathfrak{m}](\overline{\mathbf{Q}}) \subseteq J_o(pN)[\mathfrak{p}](\overline{\mathbf{Q}}),$$

for some maximal ideal $\mathfrak{p}$ *of* R *which is compatible with* $\mathfrak{m}$ *and whose residue field is isomorphic to that of* $\mathfrak{m}$. □

12 Admissible data coming from modular curves

We continue the discussion of §11, retaining the notation. In addition, we let $X_{/\mathbf{Z}[1/N]}$ denote the canonical model of the modular curve $X = X_{/\mathbf{Q}}$, as in [10], [14], or [24]. Let $\mathcal{O} = \mathbf{Z}_p$, and let $X_{/\mathcal{O}}$ denote the base change of $X_{/\mathbf{Z}[1/N]}$ to $\mathcal{O}$.

PROPOSITION **21** *The model* $X_{/\mathcal{O}}$ *is admissible, and the ring* R *is an admissible subring of* $\mathrm{End}(J_o(pN))$.

Proof. That $X_{/\mathcal{O}}$ is an admissible model follows from the discussion of Example 1 of § 2. The scheme-theoretic definitions given in ([24], Chapter 2, §5) of the correspondences defining the T_ℓ (for ℓ not dividing pN) and the U_ℓ (for ℓ dividing N) show that these correspondences are determined by diagrams

$$\begin{array}{ccc} & X'_{/\mathcal{O}} & \\ \swarrow & & \searrow \\ X_{/\mathcal{O}} & & X_{/\mathcal{O}} \end{array}$$

where the oblique arrows are morphisms of the type given in Proposition 6. It follows from that Proposition that the correspondences T_ℓ (for ℓ not dividing pN) and U_ℓ (for ℓ dividing N) are admissible. The map w_p, in the other hand, extends to an automorphism of $X_{/\mathcal{O}}$, so its admissibility again follows from Proposition 6. □

The scheme-theoretic definition of the correspondence U_p (as in [24], Chapter 2, §5) does not exhibit U_p as an admissible correspondence. However, U_p behaves as the negative of w on the representation spaces which

interest us, cf. Proposition 20 and its corollary. Thus, U_p is "morally" an element of the ring R.

Now let $\mathfrak{p} \subset R$ be a maximal ideal whose residue field F is of characteristic p. As we recalled in the Introduction (in discussing maximal ideals of $\mathbf{T}$), one can attach to $\mathfrak{p}$ a two-dimensional semi-simple Galois representation

$$\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, F).$$

This representation is unramified at primes not dividing pN and enjoys the following property: Let ℓ be a prime number not dividing pN, and let $\varphi_\ell \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be a Frobenius element for the prime ℓ. Then the characteristic polynomial of $\rho_{\mathfrak{p}}(\varphi_\ell)$ is $X^2 - a_\ell X + \ell$, where a_ℓ is the image in $F = R/\mathfrak{p}$ of the Hecke operator $T_\ell \in R$. This representation visibly depends only on the intersection $\mathfrak{p} \cap S$; it coincides with $\rho_{\mathfrak{m}}$ for any $\mathfrak{m} \subset \mathbf{T}$ which is compatible with $\mathfrak{p}$.

We say that $\mathfrak{p}$ is *of absolutely irreducible type* if the associated representation $\rho_{\mathfrak{p}}$ is absolutely irreducible. By working with a complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, one sees when $p > 2$ that $\rho_{\mathfrak{p}}$ is absolutely irreducible if and only if it is irreducible over F.

PROPOSITION **22** *Let p be a prime number and N an integer not divisible by p. Let $X_{/\mathbf{Q}}$, $X_{/\mathcal{O}}$, and R be as above. Let $\mathfrak{p}$ be a maximal ideal in R of residual characteristic p, which is strongly p-new of absolutely irreducible type. Then $\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is globally admissible.*

Proof. Since $\mathfrak{p}$ is strongly p-new one sees immediately that Axiom I (in the definition of "local admissible data," §9) holds for $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$. Indeed, R acts on $H^0(Z, \Omega^1)$ through its quotient $\overline{R}$.

To establish Axiom II, we shall make use of "q-expansion principle" techniques, very similar to those used in ([24], Chap. 2 §10). The work of Deligne-Rapoport [10] implies that $X_{/k}$ is as depicted on page 177 of [20]. In particular, two components of $X_{/\overline{k}}$ are copies of the modular curve $X_o(N)$; we shall refer to these below as the "good components." The remaining components, if any, are projective lines arising from supersingular points of $X_o(N)_{/\overline{k}}$ (which are represented by elliptic curves plus subgroups of order N) with "extra automorphisms." We refer to these components as the "possible $\mathbf{P}^1$'s."

To prove Axiom II, we must bound the dimension of the F-vector space $H^0(X_{/k}, \Omega)[\mathfrak{p}]$. Let k' be a subfield of $\overline{k}$. A Rosenlicht differential ω in the $k' \otimes_k F$-module $H^0(X_{/k'}, \Omega)[\mathfrak{p}]$ is uniquely determined by its restriction to the

good component containing the cusp ∞. Indeed, the restriction of ω to the good component containing ∞ determines it on the other good component as well (the action of w_p permutes the two good components and takes ω to ω times the image of w_p in F). Further, its restriction to the "possible $\mathbf{P}^1$'s" is also determined since we know its residues by virtue of the fact that ω is a Rosenlicht differential. Thus ω is entirely determined by its q-expansion at the cusp ∞, since it is standard that this q-expansion determines ω on the good component containing ∞.

Let F' be a finite field extension of F, and suppose that we are given a Rosenlicht differential ω on $X_{/k}$ with the property that when viewed as Rosenlicht differential over F', it is an eigenvector for the operators in R. Say that λ_n is the eigenvalue of T_n acting on ω (for each integer n prime to p) and that $-\lambda_p = \pm 1$ is the eigenvalue of w_p acting on ω. We need to show that ω is determined by its eigenvalues up to multiplication by a scalar in F'. (Cf. Propositions 9.2 and 9.3 of [20], Chapter II.)

Consider the q-expansion $f = a_1 q^1 + a_2 q^2 + \dots$ of ω. We will show that all a_n are determined by a_1 and the λ's. A familiar argument (cf. [24] Chap. 2 §10) proves that the coefficients a_n for n prime to p are determined by a_1. Indeed, since the coefficient of q in the expansion of $\omega | T_n$ is a_n, we have $a_n = \lambda_n a_1$ for each n prime to p. To control the coefficients a_n with n divisible by p, we shall establish the complementary formula $a_{np} = \lambda_p a_n$ for $n \geq 1$.

Consider the Cartier operator $\mathcal{C}$ ([34], §10) on the space $H^0(X_o(N)_{/\overline{k}}, \Omega^1)$. (Compare the discussion in [24] Chap. 2 §10.) Think of $X_o(N)$ as the good component containing ∞, and write simply ω for the restriction of ω to this component. Let σ denote the Frobenius automorphism of $\overline{k}$. The differential $\sigma(\mathcal{C}\omega)$ has q-expansion $\sum_n a_{np} q^n$, and it will suffice to show that $\sigma(\mathcal{C}\omega)$ is the negative of the restriction to $X_o(N)$ of $w_p\omega$.

At each supersingular point $\mathbf{s}$ of $X_o(N)_{/\overline{k}}$, the residue of $w_p\omega$ is $-\operatorname{res}_{\mathbf{s}^{(p)}} \omega$, since w_p permutes the two good components and induces the Frobenius map $^{(p)}$ (an involution) on the set of singular points of $X_{/\overline{k}}$. On the other hand, we have the formula

$$\sigma(\operatorname{res}_{\mathbf{s}}(\mathcal{C}\omega)) = \operatorname{res}_{\mathbf{s}^{(p)}} \sigma(\mathcal{C}\omega),$$

cf. (10). The left-hand side of this equation, however, represents the residue at $\mathbf{s}$ of ω, in view of equation (33) of [34]. [The exponent $^{(p)}$ was incorrectly placed on the left-hand side of this latter equation in the initial printing of [34]. The equation was reprinted correctly, with the exponent on the right-hand side, in Serre's *Œuvres*.] Hence $w_p\omega + \sigma(\mathcal{C}\omega)$ is a differential of the first

kind on $X_o(N)_{/\bar{k}}$. However, it is clear that this differential is annihilated by the intersection $\mathfrak{m}_o$ of $\mathfrak{m}$ and the subring S of R. By the definition of "strongly p-new," we see that $w_p\omega + \sigma(C\omega) = 0$.

We now come to Axiom III. This follows from Theorem 2 of [31], which proves that the component group Φ is "Eisenstein." Indeed, if the mod p Galois representation associated with a prime $\mathfrak{p}$ is irreducible, $\mathfrak{p}$ cannot intervene in the support of a module which is Eisenstein (cf. [30], Th. 5.2c). (It is perhaps worth pointing out that no information about the residue characteristic of $\mathfrak{p}$ is used.)

We have therefore established that $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is locally admissible. To see that $\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$ constitutes global admissible data we need only check condition (b) of §10. This follows from the argument in the proof of Proposition 14.2 of [20]. To give the bearest hint: the Eichler-Shimura relations, and the Cebotarev Density Theorem guarantee that the characteristic polynomials of the action of elements of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the F-vector space $J_o(pN)_{/\mathbf{Q}}[\mathfrak{p}]$ are the same as on a direct sum of a number of copies of V. The Brauer-Nesbitt theorem then provides the existence of an $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-Jordan-Hölder filtration whose successive quotients are isomorphic to V. [Alternatively, we could now apply the main theorem of [6], which guarantees that $J_o(pN)_{/\mathbf{Q}}[\mathfrak{p}]$ is a *direct sum* of copies of V.] □

We now can prove the Main Theorem which appears in the Introduction. We repeat it here as

THEOREM 1 *Let p be a prime number and N an integer not divisible by p. Let $\mathfrak{m}$ be a maximal ideal in $\mathbf{T}_{pN}$ of residue characteristic p, which is of absolutely irreducible type and such that $\rho_{\mathfrak{m}}$ is not modular of level N. Then $J_o(pN)(\overline{\mathbf{Q}})[\mathfrak{m}]$ is a vector space of dimension two over $\mathbf{T}_{pN}/\mathfrak{m}$, and the representation $\rho_{\mathfrak{m}}$ is equivalent to the natural representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $J_o(pN)(\overline{\mathbf{Q}})[\mathfrak{m}]$.*

Proof. Let $\mathfrak{p}$ be chosen as in the Corollary to Proposition 20. By that Corollary, it suffices to prove that $J_o(pN)(\overline{\mathbf{Q}})[\mathfrak{p}]$ is of dimension two. This result follows from Proposition 18, in view of Propositions 21, 19, and 22. □

13 Higher multiplicities

In this §, we construct kernels $J_o(M)[\mathfrak{m}]$ with multiplicities $\mu_{\mathfrak{m}} > 1$. In our examples, M is divisible by p^3, and the representation $\rho_{\mathfrak{m}}$ is modular of level M/p^2.

Let p be a prime number, and let N be a positive integer prime to p. For each ν, let $\alpha_\nu : X_o(p^{\nu+1}N) \to X_o(p^\nu N)$ be the degeneracy covering with the modular interpretation $(E, C) \mapsto (E, C[p^\nu N])$, where C denotes a cyclic subgroup of order $p^{\nu+1}N$ in an elliptic curve E. Let β_ν be the "other" degeneracy covering $X_o(p^{\nu+1}N) \to X_o(p^\nu N)$; it has the modular interpretation $(E, C) \mapsto (E/C[p], C/C[p])$. The degeneracy coverings α_ν, β_ν have degree p if $\nu \geq 1$, and degree $p+1$ when $\nu = 0$. (In §11, we introduced the degeneracy coverings $\alpha = \alpha_0$ and $\beta = \beta_0$.) They induce maps

$$\alpha_{\nu *}, \beta_{\nu *} : J_o(p^{\nu+1}N) \rightrightarrows J_o(p^\nu N), \qquad \alpha_\nu^*, \beta_\nu^* : J_o(p^\nu N) \rightrightarrows J_o(p^{\nu+1}N)$$

via the two functorialities of the Jacobian. Since neither covering α_ν, β_ν factors through a non-trivial unramified abelian covering $Z \to X_o(p^\nu N)$, the maps α_ν^* and β_ν^* are injective. Correspondingly, their duals $\alpha_{\nu *}$ and $\beta_{\nu *}$ are surjective, with connected kernels.

Let α_ν' and β_ν' denote the transposes of α_ν and β_ν, viewed as correspondences. (We regard α_ν' and β_ν' as generalized maps $X_o(p^\nu N) \rightsquigarrow X_o(p^{\nu+1}N)$.) We have the formulas $\alpha_{\nu *}' = \alpha_\nu^*$, and $\beta_{\nu *}' = \beta_\nu^*$. The Hecke correspondence T_p on $X_o(p^\nu N)$ is defined as the composition $\alpha_\nu \circ \beta_\nu'$. Accordingly, we have the formula $T_p' = \beta_\nu \circ \alpha_\nu'$ for the transpose of T_p. One may check that this Hecke correspondence has the familiar modular description

$$(E, C) \mapsto \sum_D (E/D, (C \oplus D)/D),$$

in which the sum runs over subgroups of E having order p whose intersection with C is trivial. From this description, we obtain for $\nu \geq 1$ the formulas

$$\alpha_\nu \circ T_p = T_p \circ \alpha_\nu, \qquad \beta_\nu \circ T_p = p \cdot \alpha_\nu.$$

The Hecke operator T_p on the left-hand side of each equation is a self correspondence of $X_o(p^{\nu+1}N)$, whereas the T_p on the right-hand side of the first equation is a self-correspondence of $X_o(p^\nu N)$. Finally, consider the Hecke operator T_p and the Atkin-Lehner involution w_p on the modular curve $X_o(pN)$. As we recalled above in our proof of Proposition 20, the sum $T_p + w_p$ is the correspondence $\beta_0' \circ \alpha_0$ of degree $p+1$ (cf. [30], Prop. 3.7).

Fix $\nu \geq 1$. For each $n \geq 1$, write, as usual, T_n for the n^{th} Hecke operator on $J_o(p^\nu N)$, i.e., the pullback to $J_o(p^\nu N) = \mathrm{Pic}^o(X_o(p^\nu N))$ of the Hecke correspondence T_n on $X_o(p^\nu N)$. Similarly, write w_p for the involution of $J_o(p^\nu N)$ induced by the Atkin-Lehner involution of $X_o(p^\nu N)$. Also, write $T_n^\vee$ for the "dual" of T_n, i.e., the pullback of T_n' to $J_o(p^\nu N)$.

Take $\nu = 1$, and let $\mathfrak{m} \subset \mathbf{T}_{pN}$ be a maximal ideal of residue characteristic p for which the associated representation $\rho_{\mathfrak{m}}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is: (1) absolutely irreducible and, (2) not modular of level $N = M/p$. Let $V = J_o(pN)[\mathfrak{m}]$, which is *a priori* a successive extension of some number $\mu_{\mathfrak{m}} \geq 1$ of copies of $\rho_{\mathfrak{m}}$. Our main theorem states that the multiplicity $\mu_{\mathfrak{m}}$ of $\rho_{\mathfrak{m}}$ in V is 1; however, we shall *not* make use of this fact. Since $\rho_{\mathfrak{m}}$ is not modular of level N, we have $\alpha_{0*}(V) = \beta_{0*}(V) = 0$. Because of the formula $T_p + w_p = \alpha_0^* \circ \beta_{0*}$, w_p is the scalar $-T_p$ on V. Similarly, $w_p = -T_p^\vee$ on V. We deduce, first, that $T_p = \pm 1$ on V, and secondly that $T_p^\vee = T_p$ on V. Therefore, $T_p T_p^\vee = T_p^\vee T_p = 1$ on V.

Let $\gamma : J_o(pN)^2 \to J_o(p^2N)$ be the composition of the product $\alpha_1^* \times \beta_1^*$ and the "sum" map on $J_o(p^2N)$. Thus, symbolically,

$$\gamma(x, y) = \alpha_1^*(x) + \beta_1^*(y).$$

LEMMA 4 *The map $\beta_2^* \circ \gamma : J_o(pN)^2 \to J_o(p^3N)$ induces an injection*

$$V \times V \hookrightarrow J_o(p^3N).$$

Proof. Let $\delta : J_o(p^2N) \to J_o(pN)^2$ be the map given by the symbolic formula $t \mapsto (\alpha_{1*}(t), \beta_{1*}(t))$. The composition $\delta \circ \gamma$ is the endomorphism of $J_o(pN)^2$ represented by the matrix $\begin{pmatrix} p & T_p \\ T_p^\vee & p \end{pmatrix}$ (or its transpose, depending on conventions). The restriction of this composition to $V \times V$ is thus the automorphism $\begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}$ of $V \times V$. Accordingly, the restriction of γ to $V \times V$ is injective. The lemma now follows, since $\beta_2^* : J_o(p^2N) \to J_o(p^3N)$ is injective. □

The Hecke ring $\mathbf{T}_{pN}$ acts on V via a tautological character $\mathbf{T}_{pN} \to k$, where k is the residue field of $\mathfrak{m}$. For each $n \geq 1$, let a_n be the image of T_n under this character, i.e., $T_n \bmod \mathfrak{m}$. Let W denote the image of $V \times V$ in $J_o(p^3N)$ under $\beta_2^* \circ \gamma$. For all $n \geq 1$ with $(n, p) = 1$, the Hecke operator $T_n \in \mathbf{T}_{p^3N}$ acts on W by the homothety a_n. In view of the formula $T_p \circ \beta_2^* = p\alpha_2^*$, and the fact that $p = 0$ on W, we see that $T_n = 0$ on W for all n divisible by p. Thus the action of $\mathbf{T}_{p^3N}$ on W is given by the homomorphism $\varphi : \mathbf{T}_{p^3N} \to k$ which is determined by:

$$\varphi(T_n) = \begin{cases} a_n & \text{for } (n, p) = 1, \\ 0 & \text{for } n \text{ divisible by } p. \end{cases}$$

This homomorphism is in fact surjective, since $a_p = \pm 1$.

Let $\mathcal{M}$ be the kernel of φ. Then φ identifies the residue field of $\mathcal{M}$ with the residue field k of $\mathfrak{m}$. Moreover, the k-representations $\rho_{\mathfrak{m}}$ and $\rho_{\mathcal{M}}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ are isomorphic, by the Cebotarev Density Theorem. Now $W \subseteq J_o(p^3N)[\mathcal{M}]$, and the dimension of W over $k = \mathbf{T}_{p^3N}/\mathcal{M}$ is $2\mu_{\mathfrak{m}}$. Hence the multiplicity $\mu_{\mathcal{M}}$ of $\rho_{\mathcal{M}}$ in $J_o(p^3N)[\mathcal{M}]$ satisfies $\mu_{\mathcal{M}} \geq 2\mu_{\mathfrak{m}}$.

Summing up, we get

THEOREM 2 *Let N be a positive integer prime to p, and let $\mathfrak{m} \subseteq \mathbf{T}_{pN}$ be an ideal of residue characteristic p. Assume that the representation $\rho_{\mathfrak{m}}$ is absolutely irreducible and that $\rho_{\mathfrak{m}}$ is not modular of level N. Then there is a homomorphism $\mathbf{T}_{p^3N} \to \mathbf{T}_{pN}/\mathfrak{m}$ taking $T_n \in \mathbf{T}_{p^3N}$ to T_n mod $\mathfrak{m}$ for all n prime to p. If $\mathcal{M}$ is the kernel of this homomorphism, then $\rho_{\mathfrak{m}}$ has multiplicity greater than 1 in the kernel $J_o(p^3N)[\mathcal{M}]$. More precisely, the representations $\rho_{\mathcal{M}}$ and $\rho_{\mathfrak{m}}$ are canonically isomorphic, and $J_o(p^3N)[\mathcal{M}]$ contains a product of two copies of $\rho_{\mathfrak{m}}$.*

To make a concrete example of a maximal ideal $\mathfrak{m}$ as in the Theorem, take $p = 11$ and $N = 1$. The ring $\mathbf{T}_{11}$ is isomorphic to $\mathbf{Z}$, and there is a unique ideal $\mathfrak{m} = (11)$ of residue characteristic p. The associated representation $\rho_{\mathfrak{m}}$ is the two-dimensional representation $J_o(11)[11]$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{F}_{11}$. This representation is known to be absolutely irreducible; indeed, the associated map $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(J_o(11)[11])$ is surjective [40].

References

[1] Artin, M.: On isolated singularities of surfaces. Amer. J. Math. **88**, 129–136 (1966)

[2] Altman, A., Kleiman, S.: Introduction to Grothendieck Duality Theory. Lecture Notes in Mathematics **146**. Berlin-Heidelberg-New York: Springer 1970

[3] Atkin, A.O.L., Li, W-C.: Twists of newforms and pseudo-eigenvalues of W-operators. Invent. Math. **48**, 221–243 (1978)

[4] Ash, A., Stevens, G.: Modular forms in characteristic ℓ and special values of their L-functions. Duke Math. J. **53**, 849–868 (1986)

[5] Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron Models. Berlin-Heidelberg-New York: Springer 1990

[6] Boston, N., Lenstra, H.W. Jr., Ribet, K.: Quotients of group rings arising from two-dimensional representations. To appear

[7] Carayol, H.: Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert. Ann. Sci. ENS **19**, 409–468 (1986)

[8] Carayol, H.: Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires. Duke Math. J. **59**, 785–801 (1989)

[9] Deligne, P., Mumford, D.: The irreducibility of the space of curves of given genus. Publ. Math. IHES **36**, 75–109 (1969)

[10] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. Lecture Notes in Math. **349**, 143–316 (1973)

[11] Deligne, P., Serre, J-P.: Formes modulaires de poids 1. Ann. Sci. Ecole Norm. Sup. **7**, 507–530 (1974)

[12] Gross, B.: A tameness criterion for Galois representations associated to modular forms (mod p). Duke Math. J. **61** (1990). To appear

[13] Grothendieck, A.: Groupes de monodromie en géométrie algébrique (SGA 7 I). Lecture Notes in Mathematics **288**. Berlin-Heidelberg-New York: Springer 1972

[14] Katz, N. M., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Annals of Math. Studies **108**. Princeton: Princeton University Press 1985

[15] Lang, S.: Introduction to Arakelov Theory. Berlin-Heidelberg-New York: Springer 1988

[16] Lipman, J.: Rational singularities, with applications to algebraic surfaces and unique factorization. Publ. Math. IHES **36**, 195–279 (1969)

[17] Ling, S.: Congruence relations between modular forms on $\Gamma_o(p)$ and $\Gamma_o(p^2)$. To appear

[18] Ling, S., Oesterlé, J.: The Shimura subgroup of $J_0(N)$. This volume

[19] Livné, R.: On the conductors of mod ℓ Galois representations coming from modular forms. J. Number Theory **31**, 133–141 (1989)

[20] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. IHES **47**, 33–186 (1977)

[21] Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)

[22] Mazur, B. Letter to J-F. Mestre (16 August 1985)

[23] Mazur, B., Tilouine, J.: Représentations galoisiennes, différentielles de Kähler et «conjectures principales». Publ. Math. IHES. **71**, 65–103 (1990)

[24] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbf{Q}$. Invent. Math. **76**, 179–330 (1984)

[25] Mazur, B., Wiles, A.: On p-adic analytic families of Galois representations. Compositio Math. **59**, 231–264 (1986)

[26] Pinkham, H.: Singularités de Klein I, II. Lecture Notes in Math **777**, 1–20 (1980)

[27] Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math. IHES **38**, 27–76 (1970)

[28] Ribet, K.: Galois representations attached to eigenforms with Nebentypus. Lecture Notes in Math. **601**, 17–52 (1977)

[29] Ribet, K.: Congruence relations between modular forms. Proc. International Congress of Mathematicians 1983, 503–514

[30] Ribet, K.: On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. **100**, 431–476 (1990)

[31] Ribet, K.: On the Component Groups and the Shimura Subgroup of $J_o(N)$. Sém. Th. Nombres, Université Bordeaux, 1987–88, exposé 6

[32] Ribet, K.: Multiplicities of Galois representations in Jacobians of Shimura curves. Israel Mathematical Conference Proceedings **3**, 221–236 (1990)

[33] Rosenlicht, M.: Equivalence relations on algebraic curves. Ann. of Math. **56**, 169–191 (1952)

[34] Serre, J-P.: Sur la topologie des variétés algébriques en caractéristique p. Symp. Int. de Top. Alg. (Mexico, 1958), 24–53

[35] Serre, J-P.: Groupes Algébriques et Corps de Classes (deuxième édition revue et corrigée). Paris: Hermann 1959

[36] Serre, J-P.: Lettre à J-F. Mestre (13 août 1985). Contemporary Mathematics **67** , 263–268 (1987)

[37] Serre, J-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**, 179–230 (1987)

[38] Serre, J-P.: Lettre à K. Ribet (15 avril 1987)

[39] Shafarevitch, I.: Lectures on Minimal Models. Tata Institute Lecture Notes. Bombay 1966

[40] Shimura, G.: A reciprocity law in non-solvable extensions. Journal für reine und angewandte Mathematik **221**, 209–220 (1966)

[41] Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton: Princeton University Press 1971

[42] Tate, J.: p-divisible groups. Proceedings of a Conference on Local Fields (Driebergen 1966). Berlin-Heidelberg-New York: Springer 1967

[43] Tilouine, J.: Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke. Bull. SMF **115**, 329–360 (1987)

B. Mazur
Harvard Mathematics Department
1 Oxford Street
Cambridge, MA 02138
USA

K. A. Ribet
Mathematics Department
University of California
Berkeley CA 94720
USA

General abstract

This book originates from K. Ribet's paper *"On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms"* (Invent. Math. 100, 1989), proving in particular that the Taniyama–Weil conjecture implies the Fermat conjecture. The first three papers are issued from conferences at a Seminar on that paper held in Orsay in 1987–88 and organised by G. Henniart and K. Ribet. The other four papers give new original results and generalisations on topics related to Ribet's paper. Altogether they give an overview of the present knowledge on the arithmetics of modular curves and Shimura curves.

More specifically the first two papers by **Raynaud** and **Illusie** describe the reduction mod p of the Néron model of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$, at a prime p dividing exactly N (meaning $p|N$, but $p^2 \nmid N$; they give all necessary previsions concerning the Hecke and Galois actions on this reduction. The third paper, by **Boutot** and **Carayol** is a detailed exposition with complete proofs of Drinfeld's method for obtaining the p–adic uniformisation of Shimura curves (a result due originally to Čerednik). Such Shimura curves are used in a crucial way in Ribet's paper but are equally important in other aspects of number theory.

The last four papers deal only with modular curves. Edixhoven's paper proves that the Hecke action on the group of components of the Néron model at p of $J_0(N)$ is of Eisenstein type, for p a prime dividing N, thereby generating results of Mazur and Ribet. **Ling** and **Oesterlé**'s article deals with a related finite subgroup of $J_0(N)$, the Shimura subgroup, together with its Hecke and Galois action. **Diamond**'s paper investigates the process (used by Ribet in weight 2) of raising the level of a modular form in weight $k > 2$. Finally Mazur and Ribet show that multiplicity one theorem mod p used by Ribet to complete his proof can be extended somewhat to level pM where p is prime to M, but not to the general situation. The introduction to the volume gives more details on the connection between the different papers and helps the reader get the global picture.