

FORMES MODULAIRES ET REPRÉSENTATIONS ℓ -ADIQUES

Séminaire Bourbaki, 21e année, 1968/69, no. 355

Février 1969

Pierre Deligne

Note éditoriale. L'original français publié au Séminaire Bourbaki, pp. 139–172, est la source de contrôle de cette édition française. La ressaisie anglaise datée du 28 juin 2004 est une source de comparaison et contrôle l'édition anglaise. Les coquilles non mathématiques évidentes sont régularisées dans le texte courant; les restitutions substantielles ou non évidentes sont signalées sur place et enregistrées dans le registre d'alignement livré avec cette édition.

1 Introduction

Soient

$$D(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \quad (|q| < 1)$$

et

$$\Delta(z) = D(e^{2\pi iz}) \quad (\operatorname{Im} z > 0).$$

On sait que la fonction Δ est, à un facteur constant près, l'unique forme parabolique de poids 12 pour le groupe $\operatorname{SL}_2(\mathbb{Z})$. Posons, pour p premier,

$$H_p(X) = 1 - \tau(p)X + p^{11}X^2.$$

D'après la théorie de Hecke, la série de Dirichlet

$$L_{\tau}(s) = \sum \tau(n) n^{-s} = \prod_p \frac{1}{H_p(p^{-s})}$$

se prolonge en une fonction entière de s , et la fonction

$$(2\pi)^{-s} \Gamma(s) L_{\tau}(s)$$

est invariante par $s \mapsto 12 - s$. La conjecture de Ramanujan affirme que les racines du polynôme H_p sont de valeur absolue $p^{-11/2}$, c'est-à-dire que $|\tau(p)| < 2p^{11/2}$.

Ces propriétés, démontrées ou conjecturales, sont similaires aux propriétés conjecturales des fonctions zêta des variétés algébriques sur $\mathbb{Q}$. Ceci suggère, en première approximation, de tenter d'interpréter L_{τ} comme la fonction zêta d'une telle variété.

Pour chaque nombre premier ℓ , soit K_{ℓ} la plus grande extension de $\mathbb{Q}$ non ramifiée en dehors de ℓ et, pour $p \neq \ell$, soit F_p l'inverse, dans $\operatorname{Gal}(K_{\ell}/\mathbb{Q})$, de l'élément de Frobenius φ_p relatif à p . Ce dernier objet est bien défini à conjugaison près.

Traduisant ce qui précède en terme de cohomologie ℓ -adique, Serre a conjecturé l'existence, pour chaque ℓ , d'une représentation de $\operatorname{Gal}(K_{\ell}/\mathbb{Q})$ dans un $\mathbb{Q}_{\ell}$ -vectoriel W_{ℓ} de rang 2 telle que, pour chaque $p \neq \ell$,

$$H_p(X) = \det(1 - F_p X; W_{\ell}).$$

De plus, la représentation W_{ℓ} devrait être dans le champ d'application des conjectures de Weil, et la conjecture de Ramanujan un cas particulier de ces dernières.

Ce programme avait été mené à bien, par Kuga–Shimura [4], dans le cas analogue des formes modulaires relatives à certains sous-groupes à quotient compact du groupe $\operatorname{SL}_2(\mathbb{R})$. Réduite au cas présent, l'idée fondamentale de Sato–Kuga–Shimura est la suivante : si E est la courbe elliptique universelle sur le schéma de modules S des courbes elliptiques (en oubliant qu'il n'existe pas), et si E^k est le produit fibré itéré k -uple de E avec elle-même sur S , alors $L_{\tau}(s)$ est essentiellement la fonction zêta de E^k pour $k = 10 = 12 - 2$.

On explique dans ce qui suit comment résoudre les difficultés créées par les points à l'infini, et comment construire des représentations W_{ℓ} ayant les propriétés indiquées plus haut. Pour plus de détails historiques et pour des applications, on renvoie à Serre [6].

Note sur la source. L'original français imprime « les pointes »; la ressaisie anglaise donne « the difficulties created by the points ». La coquille évidente est régularisée en « les points », et « à l'infini » est restitué d'après la lecture anglaise et l'objet même de la construction qui suit.

Notations.

- On désigne par $\mathbb{A}$ l'anneau des adèles de $\mathbb{Q}$, par $\mathbb{A}_f$ l'anneau des adèles « à distance finie », produit restreint, étendu aux nombres premiers, des corps $\mathbb{Q}_p$, et, pour S ensemble de nombres premiers, on pose

$$\mathbb{A}_f^S = \prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p \subset \mathbb{A}_f.$$

Note sur la source. Dans le second produit, la ressaisie imprime $\mathbb{Q}_p$. La définition du produit restreint et l'identité immédiatement suivante $\widehat{\mathbb{Z}} = \mathbb{A}_f^\emptyset$ imposent $\mathbb{Z}_p$, comme livré ici. Pour $S = \emptyset$, on écrit $\widehat{\mathbb{Z}} = \mathbb{A}_f^\emptyset$.

- Si X est un espace topologique (ou le site étale d'un schéma) et G un ensemble, on désigne par $\underline{G}$ le faisceau constant sur X défini par G .
- On désigne par $\mathbb{G}_a$ et $\mathbb{G}_m$ les groupes additif et multiplicatif.
- Une courbe elliptique est une variété abélienne de dimension un; en particulier, elle est munie d'une origine.
- Si L est un faisceau inversible et si $n \in \mathbb{Z}$, L^n désigne la n -ième puissance tensorielle $L^{\otimes n}$.
- On note $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.
- Le symbole $\square$ marque la fin d'une démonstration, ou son absence.

2 L'isomorphisme de Shimura

(2.1) Une courbe elliptique sur un espace analytique complexe S est un morphisme propre et plat d'espaces analytiques $f : E \rightarrow S$, muni d'une section e , dont les fibres sont des courbes elliptiques. Une courbe elliptique sur S admet une et une seule loi de groupe sur S ,

$$\mu : E \times_S E \rightarrow E,$$

dont la section unité est e . À une courbe elliptique sont associés les objets suivants.

- (a) Le faisceau inversible

$$\omega_E = e^* \Omega_{E/S}^1.$$

L'algèbre de Lie relative $\text{Lie}_S(E)$ est le faisceau inversible ω^{-1} dual de ω . On a

$$f_* \Omega_{E/S}^1 \xrightarrow{\sim} \omega.$$

- (b) Le système local de $\mathbb{Z}$ -modules libres de rang 2, $R^1 f_* \mathbb{Z}$. On pose

$$T_{\mathbb{Z}}(E) = (R^1 f_* \mathbb{Z})^\vee, \quad T_{\mathbb{Q}}(E) = T_{\mathbb{Z}}(E) \otimes \mathbb{Q},$$

le système local d'homologie de E sur S .

L'application exponentielle définit une suite exacte de faisceaux de sections

$$0 \longrightarrow T_{\mathbb{Z}}(E) \xrightarrow{\alpha} \omega^{-1} \longrightarrow E \longrightarrow 0,$$

de sorte que la courbe elliptique E peut être reconstruite à partir de l'application α .

Le système local $\bigwedge^2 R^1 f_* \mathbb{Z} \simeq R^2 f_* \mathbb{Z}$ est canoniquement isomorphe à $\mathbb{Z}$. Un isomorphisme entre $\mathbb{Z}^2$ et $R^1 f_* \mathbb{Z}$ est dit permis s'il induit 1 sur les secondes puissances extérieures. Notons $\text{Hom}^+(\mathbb{R}^2, \mathbb{C})$ l'ensemble des isomorphismes d'espaces vectoriels réels entre $\mathbb{R}^2$ et $\mathbb{C}$ qui respectent les orientations naturelles de $\mathbb{R}^2$ et de $\mathbb{C}$, définies par $e_1 \wedge e_2 > 0$ et $1 \wedge i > 0$. Un tel homomorphisme est déterminé par sa restriction à $\mathbb{Z}^2$, et l'on pose

$$\text{Hom}^+(\mathbb{Z}^2, \mathbb{C}) = \text{Hom}^+(\mathbb{R}^2, \mathbb{C}).$$

Note sur la source. L'original imprime qu'un isomorphisme permis « induit -1 (sic) » et que les éléments de Hom^+ « ne respectent pas (sic) » les orientations. Le signe $+$, les orientations affichées, le demi-plan de Poincaré de 2.2(ii) et la suite de la construction imposent respectivement 1 et « respectent », comme livré ici. Cet espace est muni de la structure complexe obtenue par son inclusion dans l'espace vectoriel complexe $\text{Hom}(\mathbb{Z}^2, \mathbb{C})$. Sur cet espace, on dispose d'une suite exacte « universelle »

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\alpha} \mathbb{G}_a \longrightarrow E_0 \longrightarrow 0.$$

Proposition (2.2).

- (i) Le foncteur qui associe à tout espace analytique S l'ensemble des classes d'isomorphisme de courbes elliptiques E sur S , munies d'isomorphismes

$$\omega_E \simeq \mathbb{G}_a, \quad R^1 f_* \mathbb{Z} \simeq \mathbb{Z}^2$$

(le dernier étant permis), est représenté par l'espace analytique $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$, muni d'une courbe elliptique universelle E_0 .

- (ii) Le foncteur qui associe à tout espace analytique S l'ensemble des classes d'isomorphisme de courbes elliptiques sur S , munies d'un isomorphisme permis $R^1 f_* \mathbb{Z} \simeq \mathbb{Z}^2$, est représenté par l'espace analytique

$$X = \mathbb{C}^\times \setminus \mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C}),$$

le demi-plan de Poincaré.

- (iii) L'espace $\mathrm{Hom}^+(\mathbb{R}^2, \mathbb{C})$ est un espace principal homogène du groupe $\mathbb{G}_m$ sur X .

On peut encore regarder X comme l'ensemble des structures complexes sur $\mathbb{R}^2$. Cet espace est, d'après (ii), muni d'une courbe elliptique universelle E_X , dont le système local de cohomologie réelle est canoniquement isomorphe à $\mathbb{R}^2$. Soit ω le faisceau inversible associé à E_X .

Le faisceau analytique cohérent

$$R^1 f_* \mathbb{R} \otimes_{\mathbb{R}} \mathcal{O}_X$$

est le faisceau de cohomologie de De Rham relative de E_X sur X , et s'insère à ce titre dans une suite exacte, la filtration de Hodge,

$$0 \longrightarrow \omega \longrightarrow R^1 f_* \mathbb{R} \otimes_{\mathbb{R}} \mathcal{O}_X \xrightarrow{q} \omega^{-1} \longrightarrow 0,$$

puisque, par dualité de Serre, $\omega^{-1} \simeq R^1 f_* \mathcal{O}_{E_X}$.

La description fonctorielle de 2.2(ii) donne évidemment une action à droite du groupe $\mathrm{SL}_2(\mathbb{Z})$ sur (X, E_X) : à $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et à la courbe elliptique E munie de $\alpha : \mathbb{Z}^2 \xrightarrow{\sim} R^1 f_* \mathbb{Z}$, on associe $(E, \alpha \circ \gamma)$. Si l'on regarde X , muni de

$$q : \mathbb{R}^2 \otimes_{\mathbb{R}} \mathcal{O}_X \simeq R^1 f_* \mathbb{R} \otimes_{\mathbb{R}} \mathcal{O}_X \longrightarrow \omega^{-1},$$

comme classifiant les structures complexes sur $\mathbb{R}^2$, on a la même action évidente du groupe $\mathrm{GL}_2^+(\mathbb{R})$ sur $(X, \mathbb{R}^2, \omega, q)$.

(2.3) Choisissons une base (x_1, x_2) de $\mathbb{R}^2$ telle que $x_1 \wedge x_2 > 0$. Un point

$$(f : \mathbb{R}^2 \rightarrow \mathbb{C}) \quad \text{mod } \mathbb{C}^\times$$

de X est repéré par

$$z = \frac{f(x_1)}{f(x_2)} \quad (\mathrm{Im} z > 0),$$

et l'application q s'identifie à

$$q : \mathbb{R}^2 \rightarrow \mathbb{G}_a, \quad ax_1 + bx_2 \longmapsto az + b.$$

Ceci donne une trivialisat on  vidente de ω^{-1} sur X , qui n'est pas  quivariante. Relativement   cette trivialisat on, une section $f(z)$ de ω^k sur X est transform e par un  l ment

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathrm{GL}^+(\mathbb{R}^2)$$

(relativement   la base (x_1, x_2)) suivant la formule

$$f \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} (z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

Note sur la source. Dans la premi re matrice de la ligne imprim e, l'original fran ais et la ressaisie anglaise donnent tous deux $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$. La formule homographique de la m me ligne et la matrice du d terminant juste apr s imposent toutes deux $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$, comme livr  ici. De l'identit 

$$dz = (cz + d)^2 d\left(\frac{az + b}{cz + d}\right) \left| \begin{matrix} a & b \\ c & d \end{matrix} \right|^{-1},$$

on d duit que dz est une section de $\omega^{-2}\Omega_X^1$ invariante sous le groupe $\mathrm{SL}_2(\mathbb{R})$. Cette section est partout non nulle et d finit un isomorphisme de $\mathrm{SL}_2(\mathbb{R})$ -faisceaux  quivariants entre ω^2 et Ω_X^1 .

(2.4) Soit Γ un sous-groupe discret, sans élément d'ordre fini et à quotient de volume fini, du groupe $\mathrm{SL}_2(\mathbb{R})$. On sait alors que l'espace quotient X/Γ s'identifie à une courbe projective lisse $\overline{X}/\Gamma$, moins un nombre fini de points. Le groupe Γ opère sans points fixes sur X . Le système local équivariant $\underline{\mathbb{R}^2}$ sur X , ainsi que la suite exacte équivariante

$$0 \rightarrow \omega \rightarrow \mathbb{R}^2 \otimes_{\mathbb{R}} \mathcal{O} \rightarrow \omega^{-1} \rightarrow 0,$$

définissent donc un système local U sur X/Γ et une suite exacte

$$0 \rightarrow \omega \rightarrow U \otimes_{\mathbb{R}} \mathcal{O} \rightarrow \omega^{-1} \rightarrow 0. \quad (2.5)$$

Dans le cas particulier où $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, ces structures sont déduites de la courbe elliptique E sur X/Γ d'image réciproque la courbe elliptique équivariante E_X sur X .

(2.6) Les points à l'infini de X/Γ se décrivent comme suit (voir [9]) :

- (a) Ils correspondent aux classes de conjugaison, dans Γ , des sous-groupes non triviaux de Γ , maximaux parmi les sous-groupes de Γ formés d'éléments unipotents.
- (b) Soit $\Gamma_0 \subset \Gamma$ un tel sous-groupe et choisissons une base (x_1, x_2) de $\mathbb{R}^2$ telle que, dans cette base, Γ_0 se représente comme l'ensemble de matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

Soit z la coordonnée (2.3) sur X définie par (x_1, x_2) . Il existe N tel que le partie

$$X_N = \{z \mid \mathrm{Im}(z) > N\}$$

de X soit disjointe de ses conjuguées pour tout $\gamma \in \Gamma \setminus \Gamma_0$, de sorte que $X_N/\Gamma_0 \hookrightarrow X/\Gamma$. La fonction $q = e^{2\pi iz}$ établit un isomorphisme entre X_N/Γ_0 et le disque épointé

$$0 < |q| < e^{-2\pi N}.$$

Si P_{Γ_0} est le point de $\overline{X/\Gamma} - X/\Gamma$ associé à Γ_0 , cet isomorphisme se prolonge en un isomorphisme d'un voisinage de P_{Γ_0} avec le disque $0 \leq |q| < e^{-2\pi N}$.

Note sur la source. La ressaisie imprime les deux inégalités de disque sans valeurs absolues autour de la coordonnée complexe q . La description du disque impose $|q|$, rétabli dans les deux inégalités ci-dessus.

En vertu de (2.3), les sections de ω sur X_N , invariantes par Γ_0 , s'identifient aux fonctions holomorphes périodiques de période un sur X_N . On désigne encore par ω le faisceau inversible sur $\overline{X/\Gamma}$ qui prolonge ω et tel qu'au voisinage d'une pointe P_{Γ_0} , la section de ω sur X_N/Γ_0 définie par la fonction 1 se prolonge en une section inversible sur $\overline{X_N/\Gamma_0}$.

(2.7) Sur $\overline{X/\Gamma}$, on dispose des deux faisceaux inversibles Ω^1 et ω^2 , et d'un isomorphisme φ (2.3) entre les restrictions de ces faisceaux à X/Γ . De la formule

$$dq = d(e^{2\pi iz}) = 2\pi i e^{2\pi iz} dz = 2\pi i q dz$$

résulte que la flèche

$$\varphi : \Omega^1 \rightarrow \omega^2$$

se prolonge à $\overline{X/\Gamma}$, et présente un zéro simple en chacun des points à l'infini.

Définition (2.8). *L'espace des formes automorphes paraboliques de poids $k+2$, relatives au groupe Γ , est l'espace de sections globales*

$$H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k).$$

En vertu de (2.7), cet espace s'identifie encore à l'espace des sections globales de ω^{k+2} qui s'annulent à l'infini (i.e. à chaque « pointe »).

(2.9) Désignons par U^k le système local sur X/Γ puissance symétrique k -ième du système local U . La flèche (2.5) induit une flèche

$$\iota^k : \omega^k \rightarrow U^k \otimes_{\mathbb{R}} \mathcal{O},$$

puis une flèche, encore désignée par ι^k ,

$$\iota^k : \Omega^1 \otimes \omega^k \rightarrow \Omega^1(U^k),$$

de but le faisceau des formes différentielles holomorphes sur X/Γ , à coefficients dans le système local U^k .

La résolution de De Rham de $U^k \otimes_{\mathbb{R}} \mathbb{C}$,

$$0 \rightarrow U^k \otimes_{\mathbb{R}} \mathbb{C} \rightarrow U^k \otimes_{\mathbb{R}} \mathcal{O} \xrightarrow{d} U^k \otimes_{\mathbb{R}} \Omega^1 \rightarrow 0,$$

induit une application

$$\delta : H^0(X/\Gamma, \Omega^1(U^k)) \rightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}).$$

De plus, l'espace de cohomologie $H^1(X/\Gamma, U^k \otimes \mathbb{C})$ est muni d'une conjugaison complexe naturelle, de sorte que δ définit une application linéaire conjuguée $\bar{\delta}$ de l'espace complexe conjugué à $H^0(X/\Gamma, \Omega^1(U^k))$ dans $H^1(X/\Gamma, U^k \otimes \mathbb{C})$. On obtient ainsi une flèche

$$\begin{aligned} \text{sh}_0 &= \delta \cdot H^0(\iota^k) \oplus \bar{\delta} \cdot H^0(\bar{\iota}^k) \\ \text{sh}_0 : H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} &\longrightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}). \end{aligned}$$

Quel que soit le faisceau F sur un espace Y , on désignera par $\tilde{H}^i(Y, F)$ l'image de la cohomologie à support compact $H_c^i(Y, F)$ dans la cohomologie sans support $H^i(Y, F)$.

Le théorème 4.2.6 de [9] est essentiellement équivalent au théorème suivant; dans loc. cit. k est supposé pair, mais la même démonstration vaut en général.

Théorème (2.10, Shimura [7]). *Il existe un isomorphisme sh rendant commutatif le diagramme suivant :*

$$\begin{array}{ccc} H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} & \xrightarrow{\text{sh}} & \tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \\ \cap & & \cap \\ H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} & \xrightarrow{\text{sh}_0} & H^1(X/\Gamma, U^k \otimes \mathbb{C}). \end{array}$$

On appelle sh l'isomorphisme de Shimura.

(2.11) Dans le cas particulier où Γ est un sous-groupe d'indice fini de $\text{SL}_2(\mathbb{Z})$, la courbe elliptique E sur X/Γ provient d'un schéma en courbes elliptiques sur la courbe algébrique $\overline{X/\Gamma}$ (i.e., son invariant modulaire est méromorphe à l'infini) ; elle admet donc un modèle de Néron $\overline{E}$ sur $\overline{X/\Gamma}$. On peut montrer que les fibres de $\overline{E}$ aux points à l'infini sont de type multiplicatif, et que sur tout $\overline{X/\Gamma}$ on a

$$\omega = e^* \Omega_{\overline{E}/\overline{X/\Gamma}}^1.$$

Dans ce cas particulier, on a $U = R^1 f_* \mathbb{Z} \otimes \mathbb{R}$, de sorte que le but de l'isomorphisme de Shimura peut s'écrire

$$\tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \simeq \tilde{H}^1(X/\Gamma, \text{Sym}^k(R^1 f_* \mathbb{Z})) \otimes_{\mathbb{Z}} \mathbb{C}.$$

Note sur la source. Le texte imprimé donne deux fois la coquille anglaise « furnishes »; les deux occurrences sont livrées sous la forme correcte « furnishes » dans l'édition anglaise.

3 Opérateurs de Hecke et représentation ℓ -adique fondamentale

(3.1) Rappelons (cf. [3]) que la catégorie des $\mathbb{Z}_{\ell}$ -faisceaux « localement constants » constructibles (en abrégé, l.c.c.) sur un schéma S est la catégorie des systèmes projectifs de faisceaux $(F_n)_{n \in \mathbb{N}}$ sur le site étale $S_{\text{ét}}$ de S qui vérifient :

- (i) F_n est un faisceau localement constant de $\mathbb{Z}/(\ell^n)$ -modules de type fini;
- (ii) si $n \leq m$, alors

$$F_m \otimes \mathbb{Z}/(\ell^n) \xrightarrow{\sim} F_n.$$

Les $\mathbb{Z}_\ell$ -faisceaux l.c.c. forment un champ en catégories abéliennes sur S ; le champ des $\mathbb{Q}_\ell$ -faisceaux l.c.c. est le quotient de ce champ par le sous-champ épais des $\mathbb{Z}_\ell$ -faisceaux l.c.c. tués par une puissance de ℓ . On désigne par $\otimes_{\mathbb{Q}_\ell}$ le foncteur canonique de la catégorie des $\mathbb{Z}_\ell$ -faisceaux l.c.c. dans celle des $\mathbb{Q}_\ell$ -faisceaux l.c.c.

Si S est connexe et muni d'un point géométrique s , la catégorie des $\mathbb{Z}_\ell$ -faisceaux (resp. $\mathbb{Q}_\ell$ -faisceaux) l.c.c. sur S est équivalente, par le foncteur « fibre en s », à la catégorie des représentations continues du groupe fondamental $\pi_1(S, s)$ sur un $\mathbb{Z}_\ell$ -module de type fini (resp. un $\mathbb{Q}_\ell$ -vectoriel de rang fini).

Si T est un ensemble fini de nombres premiers, un faisceau lcc en $\mathbb{A}_T^f$ consiste à se donner, pour chaque nombre premier ℓ , un faisceau lcc en $\mathbb{Z}_\ell$ si $\ell \notin T$, et un faisceau lcc en $\mathbb{Q}_\ell$ si $\ell \in T$. Pour $T = \emptyset$, on parle de faisceaux lcc en $\widehat{\mathbb{Z}}$ plutôt que de faisceaux lcc en $\mathbb{A}_\emptyset^f$.

Pour T général, la catégorie des faisceaux lcc en $\mathbb{A}_T^f$ est la limite inductive des catégories de faisceaux lcc en $\mathbb{A}_{T'}^f$ pour $T' \subset T$ fini. On pose

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/(\ell^n), \quad \mathbb{Q}_\ell = \mathbb{Z}_\ell \otimes \mathbb{Q}_\ell, \quad \widehat{\mathbb{Z}} = (\mathbb{Z}_\ell)_\ell, \quad \mathbb{A}_T^f = \widehat{\mathbb{Z}} \otimes \mathbb{A}_T^f.$$

Note sur la source. Les coquilles orthographiques évidentes de la réédition anglaise sur cette page—notamment « Shiumra », « particluar », « schme », « constant » et « number »—sont régularisées sans modification mathématique.

Le champ des courbes elliptiques à isogénie près sur S est le champ déduit du champ des courbes elliptiques sur S en « inversant formellement les isogénies ». On désigne par $\otimes \mathbb{Q}$ le foncteur associant à une courbe elliptique la courbe elliptique sous-jacente à isogénie près. Pour S quasi-compact, on a

$$\mathrm{Hom}(E, F) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{Hom}(E \otimes \mathbb{Q}, F \otimes \mathbb{Q}),$$

et, pour S normal, toute courbe elliptique à isogénie près sur S est sous-jacente à une courbe elliptique sur S .

(3.2) Soit $f : E \rightarrow S$ une courbe elliptique sur un schéma S . On désigne par $T_\ell(E)$ le système projectif des noyaux E_{ℓ^n} de la multiplication par ℓ^n sur E , la flèche de transition de E_{ℓ^n} dans E_{ℓ^m} , pour $n \geq m$, étant la multiplication par ℓ^{n-m} . En procédant de même pour $\mathbb{G}_m$, on pose $T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(1)$. Si ℓ est inversible sur S , alors $T_\ell(E)$ et $\mathbb{Z}_\ell(1)$ sont des faisceaux en $\mathbb{Z}_\ell$ sur S . On définit $T_\infty(E)$ comme étant l'algèbre de Lie relative de E sur S , c'est-à-dire le dual inversible du faisceau inversible ω de (2.1(a)).

Supposons S de caractéristique 0. On définit alors le $\widehat{\mathbb{Z}}$ -faisceau $T_f(E)$ sur S comme étant le système des $T_\ell(E)$, et l'on pose

$$V_f(E) = T_f(E) \otimes \mathbb{A}_f.$$

Si $u : E \rightarrow F$ est une isogénie, alors u induit un isomorphisme de $V_f(E)$ sur $V_f(F)$ et de $T_\infty(E)$ sur $T_\infty(F)$; les foncteurs V_f et T_∞ se factorisent donc par la catégorie des courbes elliptiques à isogénie près sur S .

Proposition (3.3). *Soient S un schéma de caractéristique 0, $E_1(S)$ la catégorie des courbes elliptiques sur S et $E_2(S)$ la catégorie des triplets formés d'une courbe elliptique à isogénie près E sur S , d'un faisceau en $\widehat{\mathbb{Z}}$, T , forme tordue de $\widehat{\mathbb{Z}}^2$, et d'un isomorphisme*

$$\beta : V_f(E) \xrightarrow{\sim} T \otimes \mathbb{A}_f.$$

Alors le foncteur

$$I : E \longmapsto (E \otimes \mathbb{Q}, T_f(E), V_f(E) \simeq T_f(E) \otimes \mathbb{A}_f)$$

de $E_1(S)$ vers $E_2(S)$ est une équivalence de catégories.

La question est locale sur S , que l'on peut supposer quasi-compact. Si $f : E \rightarrow F$ est un morphisme de S -courbes elliptiques, et si f est une isogénie, on dispose d'une suite exacte

$$0 \rightarrow T_f(E) \rightarrow T_f(F) \rightarrow \ker(f) \rightarrow 0. \quad (3.4)$$

Le morphisme f est divisible par n si et seulement s'il tue le noyau E_n de la multiplication par n , car la flèche « multiplication par n » de E/E_n dans E est un isomorphisme. Par (3.4), ceci a lieu si et seulement si $T_f(f)$ est divisible par n , et l'on en déduit que $\mathrm{Hom}_S(E, F)$ est le sous-groupe de $\mathrm{Hom}_S(E \otimes \mathbb{Q}, F \otimes \mathbb{Q})$ formé des morphismes f tels que $V_f(f)$ envoie $T_f(E)$ dans $T_f(F)$. Le foncteur I est donc pleinement fidèle.

Note sur la source. L'original français conclut bien que I est « pleinement fidèle ». La mention « faithfully flat » appartient uniquement à la réédition anglaise héritée et y est corrigée en « fully faithful ». Les lapsus de casse évidents $u : e \rightarrow F$ et $E_1(s)$ dans cette réédition sont normalisés en $u : E \rightarrow F$ et $E_1(S)$.

Soit $X \in \text{Ob}(E_2(S))$. Localement sur S , X est défini par une courbe elliptique à isogénie près $E \otimes \mathbb{Q}$, et par un « réseau » T dans $V_f(E)$ qui, pour presque tout ℓ , coïncide avec $T_\ell(E)$. Pour $q \in \mathbb{Q}$, $(E \otimes \mathbb{Q}, T)$ est isomorphe à $(E \otimes \mathbb{Q}, qT)$, ce qui permet de supposer $T_f(E) \subset T$. Le quotient $K = T/T_f(E)$ est alors canoniquement isomorphe à un sous-groupe fini de E , et X est l'image de E/K par I (cf. 3.4). $\square$

Corollaire (3.5). *Le foncteur $F_1(S)$, respectivement $F'_1(S)$, qui, à chaque schéma S de caractéristique 0, associe l'ensemble des classes d'isomorphisme de courbes elliptiques sur S munies d'un isomorphisme*

$$\alpha : T_f(E) \xrightarrow{\sim} \widehat{\mathbb{Z}}^2$$

respectivement aussi d'un isomorphisme

$$\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathbb{G}_a,$$

est isomorphe au foncteur $F_2(S)$, respectivement $F'_2(S)$, qui associe à S l'ensemble des classes d'isomorphisme de courbes elliptiques à isogénie près sur S , munies d'un isomorphisme

$$\beta : V_f(F) \xrightarrow{\sim} \mathbb{A}_f^2$$

respectivement aussi d'un isomorphisme

$$\beta_\infty : T_\infty(F) \xrightarrow{\sim} \mathbb{G}_a.$$

Proposition (3.6). *Le foncteur F_1 (respectivement F'_1) est représentable par un schéma M_∞ (respectivement M'_∞) sur $\mathbb{Q}$.*

Soit $n \geq 3$ un entier. Le foncteur qui associe à chaque schéma S l'ensemble des classes d'isomorphisme de courbes elliptiques, munies d'un isomorphisme

$$\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$$

respectivement aussi de $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, est représenté par une courbe affine M_n (respectivement par une surface affine M'_n) sur $\text{Spec}(\mathbb{Z}[1/n])$. Pour $n \mid m$, le morphisme de M_m vers M_n défini par

$$(E, \alpha_m : E_m \xrightarrow{\sim} (\mathbb{Z}/m)^2) \longmapsto (E, (n/m)\alpha_m : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2)$$

est fini et étale sur $\text{Spec}(\mathbb{Z}[1/m])$, et l'on a

$$M_\infty = \varprojlim M_n.$$

On procède de même pour représenter F'_1 . $\square$

Note sur la source. L'original français donne $\mathcal{O}_S$ et le facteur $(n/m)\alpha_m$. Les leçons héritées $\mathcal{O}_X$ et $(m/n)\alpha_m$, incompatibles avec la base du foncteur et avec la restriction de niveau pour $n \mid m$, sont corrigées dans les deux éditions. Les formes fautives « schem » et « One goes one proceeds » de la réédition anglaise sont en outre régularisées en « scheme » et « One proceeds ».

(3.7) Le schéma M_∞ (respectivement M'_∞) est muni d'une courbe elliptique universelle $f_\infty : E_\infty \rightarrow M_\infty$ et d'un isomorphisme

$$\alpha : T_f(E_\infty) \xrightarrow{\sim} \widehat{\mathbb{Z}}^2,$$

respectivement aussi d'un isomorphisme

$$\alpha_\infty : T_\infty(E_\infty) \xrightarrow{\sim} \mathbb{G}_a.$$

D'après (3.5), le schéma M_∞ (respectivement M'_∞) représente le foncteur F_2 (respectivement F'_2), ce qui donne une action évidente à gauche du groupe adélique $\text{GL}_2(\mathbb{A}_f)$ sur

$$(M_\infty, E_\infty \otimes \mathbb{Q}, \alpha \otimes \mathbb{A}_f)$$

respectivement sur

$$(M'_\infty, E_\infty \otimes \mathbb{Q}, \alpha \otimes \mathbb{A}_f, \alpha_\infty).$$

Sur le foncteur, cette action est donnée, pour $g \in \mathrm{GL}_2(\mathbb{A}_f)$, par

$$g : (F, \beta : V_f(F) \xrightarrow{\sim} \mathbb{A}_f^2, \beta_\infty) \mapsto (F, g \circ \beta : V_f(F) \xrightarrow{\sim} \mathbb{A}_f^2, \beta_\infty).$$

Note sur la source. Les deux témoins imprimés abrègent la trivialisatation induite en $\alpha \otimes \mathbb{A}_f^2$ et écrivent $V_f(E)$ dans un triplet dont la courbe est F . Comme $\alpha : T_f(E_\infty) \rightarrow \widehat{\mathbb{Z}}^2$, l'extension des scalaires est $\alpha \otimes \mathbb{A}_f$, et le domaine de l'action est $V_f(F)$; ces lectures requises par les types sont livrées ci-dessus. L'original emploie en outre la même courbe universelle E_∞ dans les deux cas; la prime héritée sur E'_∞ est supprimée dans les deux éditions. Šafarevič, le premier, a noté ce fait.

Soit Y un schéma sur $\mathbb{C}$, limite projective de schémas Y_i de type fini sur $\mathbb{C}$, les morphismes de transition étant finis. L'espace localement compact annelé Y^{an} , égal à la limite projective des Y_i^{an} , ne dépend que de Y et non de sa représentation comme limite projective. Si Y est un schéma sur $\mathbb{Q}$, limite projective de schémas Y_i de type fini sur $\mathbb{Q}$ à morphismes de transition finis, on pose $Y^{\mathrm{an}} = (Y \otimes \mathbb{C})^{\mathrm{an}}$. Ceci s'applique à M_∞ et à M'_∞ .

Proposition (3.8). *On a canoniquement*

$$M'^{\mathrm{an}}_\infty \simeq \mathrm{Hom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \mathrm{GL}_2(\mathbb{Q})$$

et

$$M^\infty_\infty \simeq \mathbb{C}^\times \backslash \mathrm{Hom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \mathrm{GL}_2(\mathbb{Q}),$$

et, moins canoniquement,

$$M'^{\mathrm{an}}_\infty \simeq \mathrm{GL}_2(\mathbb{A}) / \mathrm{GL}_2(\mathbb{Q}), \quad M^\infty_\infty \simeq K_\infty \backslash \mathrm{GL}_2(\mathbb{A}) / \mathrm{GL}_2(\mathbb{Q}),$$

où K_∞ est le sous-groupe compact maximal à l'infini, augmenté des homothéties réelles. Ces isomorphismes sont compatibles à l'action de $\mathrm{GL}_2(\mathbb{A}_f)$.

Note sur la source. La réédition anglaise contient ici les marques non résolues « [a/the, bad copy] » et « [bad copy] ». L'original français donne exactement « le sous-groupe compact maximal à l'infini, augmenté des homothéties réelles »; cette lecture directement établie est livrée ci-dessus.

La notion de courbe elliptique à isogénie près, et leur sorite, s'étendent tels quels au cas analytique complexe. En outre, une isogénie $\varphi : E \rightarrow F$ induit un isomorphisme φ^* entre les systèmes locaux de cohomologie rationnelle de E et de F , ce qui permet de définir ce dernier pour une courbe elliptique à isogénie près. Soit S un espace analytique complexe. On voit à l'aide de (2.1) qu'il revient au même de se donner une courbe elliptique à isogénie près sur S , ou de se donner un faisceau inversible T_∞ , un système local de $\mathbb{Q}$ -vectoriels $T_\mathbb{Q}$, et un morphisme $u : T_\mathbb{Q} \rightarrow T_\infty$ induisant point par point un isomorphisme $T_\mathbb{Q} \otimes \mathbb{R} \rightarrow T_\infty$.

Soit n un entier et soit K_n le noyau de l'application naturelle

$$\prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{GL}_2(\mathbb{Z}/n).$$

Soit G_1 le foncteur qui associe à S l'ensemble des classes d'isomorphisme de courbes elliptiques $f : E \rightarrow S$ sur S , munies d'un isomorphisme

$$\varphi : \mathbb{Q}^2 \xrightarrow{\sim} T_\mathbb{Q}(E),$$

d'un isomorphisme $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, et d'un isomorphisme $\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$. Comme en (3.3), on voit que G_1 est isomorphe au foncteur G_2 qui associe à S l'ensemble des classes d'isomorphisme de courbes elliptiques à isogénies près E sur S , munies de $\varphi : \mathbb{Q}^2 \xrightarrow{\sim} T_\mathbb{Q}(E)$, de $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$, et d'un isomorphisme $V_f(E) \xrightarrow{\sim} \mathbb{A}_f^2$ donné localement sur S à composition par un élément de K_n près.

Un tel objet est déterminé par l'application composée φ' (donnée localement modulo K_n) obtenue à partir de

$$\varphi' : \mathbb{Q}^2 \xrightarrow{\varphi} T_\mathbb{Q}(E) \longrightarrow T_\infty(E) \times V_f(E) \xrightarrow{\sim} \mathcal{O}_S \times \mathbb{A}_f^2.$$

On a

$$E = \mathcal{O}_S / \varphi'(\mathbb{Q}^2 \cap \varphi'^{-1}(T_\infty(E) \times T_f(E))) = \widehat{\mathbb{Z}}^2 \backslash (\mathcal{O}_S \times \mathbb{A}_f^2) / \varphi'(\mathbb{Q}^2),$$

de sorte que, cf. 2.2, G_1 et G_2 sont représentés par

$$K_n \backslash \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2).$$

Supposons maintenant que $n \geq 3$, de sorte que $\mathrm{GL}_2(\mathbb{Q})$ agisse librement sur l'espace précédent. L'espace analytique M_n^{an} , respectivement $M_n'^{\mathrm{an}}$, représente le foncteur analogue, en géométrie analytique, au foncteur représenté par M_n , respectivement M_n' , parce que ce foncteur, disons X , est représentable et que la flèche $X \rightarrow M_n^{\mathrm{an}}$, respectivement $X \rightarrow M_n'^{\mathrm{an}}$, induit une bijection sur les ensembles de points à valeurs dans toute $\mathbb{C}$ -algèbre de rang fini. On déduit dès lors de ce qui précède que

$$M_n'^{\mathrm{an}} \simeq K_n \backslash \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \mathrm{GL}_2(\mathbb{Q}).$$

Procédant de même pour M_n , on obtient la première assertion de (3.8) par passage à la limite sur n .

Un point x de

$$\mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}_f^2) / \mathrm{GL}_2(\mathbb{Q})$$

s'identifie à un « réseau » L_x de $\mathbb{C} \times \mathbb{A}_f^2$, et la courbe correspondante est

$$E_x \simeq \widehat{\mathbb{Z}}^2 \backslash (\mathbb{C} \times \mathbb{A}_f^2) / L_x,$$

munie de

$$V_f(E_x) \simeq L_x \otimes \mathbb{A}_f \xrightarrow{\sim} \mathbb{A}_f^2.$$

De là, sort aisément la dernière assertion de (3.8). □

Désignons par $f_n : E \rightarrow M_n$ la courbe elliptique universelle sur M_n . L'entier k étant fixé, on pose la

Définition (3.9). On désigne par W (ou par ${}^k W$, s'il y a risque de confusion) le $\mathbb{Q}$ -vectoriel

$$W = \varinjlim_n \tilde{H}^1(M_n^{\mathrm{an}}, \mathrm{Sym}^k(R^1 f_{n*} \mathbb{Q})) = \varinjlim_n W.$$

Note sur la source. Les coquilles de la réédition anglaise « beause », « arros » et « Once deduces » sont régularisées. Dans la description de la courbe correspondant à x , le $V_f(E)$ imprimé est livré sous la forme $V_f(E_x)$, seul objet qui vient d'être défini à cet endroit. La réédition anglaise imprime ensuite que W « doesn't depend on » la courbe universelle, renversant le français « ne dépend que de »; la lecture « ne dépend que de »/« depends only on » est donc rétablie dans les deux éditions. Enfin, l'indice de niveau n , visible dans le f_{n*} de l'original français, est rétabli dans la première formule définissant W .

Ce vectoriel ne dépend que de la courbe elliptique (à isogénie près) universelle $f_\infty : E \rightarrow M_\infty$, de sorte que, par transport de structure, il est muni d'une action à gauche du groupe adélique $\mathrm{GL}_2(\mathbb{A}_f)$.

Si ℓ est un nombre premier, le vectoriel $W_\ell = W \otimes \mathbb{Q}_\ell$ admet une définition purement algébrique, en terme de cohomologie ℓ -adique des schémas sur la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ déduits par extension des scalaires des schémas M_n :

$$W_\ell = \varinjlim_n \tilde{H}^1(M_n \otimes \overline{\mathbb{Q}}, \mathrm{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)) = \varinjlim_n W_\ell. \quad (3.10)$$

de sorte que le groupe de Galois de $\overline{\mathbb{Q}}$ sur $\mathbb{Q}$ agit, par transport de structure, sur W_ℓ et les ${}_n W_\ell$.

Enfin, l'espace M_n^{an} est somme disjointe de quotients du demi-plan de Poincaré par des sous-groupes de congruence du groupe $\mathrm{SL}_2(\mathbb{Z})$, de sorte que, désignant par ω le faisceau inversible sur M_n défini par E , la théorie de Shimura (2.10) donne

$$W_\infty = W \otimes \mathbb{C} = \varinjlim_n \left(H^0(\overline{M}_n^{\mathrm{an}}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{M}_n^{\mathrm{an}}, \Omega^1 \otimes \omega^k)} \right). \quad (3.11)$$

Note sur la source. La transcription héritée avait perdu les barres des courbes compactifiées $\overline{M}_n^{\mathrm{an}}$ dans les deux termes de (3.11); elles sont rétablies ci-dessus. Le « if is equipped » de la réédition anglaise est régularisé en « it is equipped » dans l'édition anglaise. Cette décomposition de $W \otimes \mathbb{C}$ en deux sous-espaces complexes conjugués, dont l'un est l'espace de toutes formes automorphes holomorphes paraboliques de poids $k+2$, relative à un quelconque sous-groupe de congruence du groupe $\mathrm{SL}_2(\mathbb{Z})$, est analogue à une décomposition de Hodge, « de type »

$$(0, k+1) + (k+1, 0).$$

L'action du groupe adélique commute à l'action du groupe de Galois et respecte la décomposition précédente.

Bien que le système local ℓ -adique $R^1 f_{*} \mathbb{Q}_\ell$ soit trivial sur M_∞ , je ne sais pas s'il existe une relation entre W_ℓ et

$$\varinjlim_n (\tilde{H}^1(M_n \otimes \overline{\mathbb{Q}}, \mathbb{Q}_\ell)) \otimes \mathrm{Sym}^k(\mathbb{Q}_\ell^2).$$

(3.12) Soient $n \geq 3$ un entier et K_n comme en (3.8). On a alors

$$W^{K_n} = {}_n W.$$

Cela se vérifie par passage à la limite, et résulte de ce qu'en cohomologie rationnelle, la cohomologie du quotient d'un espace par un groupe fini s'obtient en prenant les invariants de ce groupe dans la cohomologie.

Posons, pour p premier,

$$W^{(p)} = W^{\mathrm{GL}_2(\mathbb{Z}_p)}.$$

Par passage à la limite, on obtient

$$W^{(p)} = \varinjlim_{(n,p)=1} {}_n W.$$

Sur cet espace de cohomologie agissent encore :

- (i) le sous-groupe $\prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{Q}_\ell)$ de $\mathrm{GL}_2(\mathbb{A}_f)$, car ce sous-groupe centralise $\mathrm{GL}_2(\mathbb{Z}_p)$;
- (ii) l'algèbre de Hecke $\mathcal{H}(\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p))$, qui est l'algèbre des mesures entières sur l'espace discret $\mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p)$ invariantes à gauche par $\mathrm{GL}_2(\mathbb{Z}_p)$. Cette sous-algèbre de l'algèbre du groupe $\mathrm{GL}_2(\mathbb{Q}_p)$ agit sur W en respectant $W^{(p)}$. Cette algèbre agit déjà sur chacun des ${}_n W$ pour n premier à p .

L'algèbre de Hecke admet pour base les (mesures associées aux fonctions caractéristiques des) doubles classes de $\mathrm{GL}_2(\mathbb{Z}_p)$ dans $\mathrm{GL}_2(\mathbb{Q}_p)$, et l'on sait que

$$\mathcal{H}(\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p)) = \mathbb{Z}[T_p, R_p, R_p^{-1}],$$

où T_p et R_p sont les doubles classes de

$$\begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{pmatrix}.$$

(3.13) Soient p un nombre premier, $n \geq 3$ un entier premier à p , et $F_{n,p}$ le foncteur qui, à chaque schéma S , associe l'ensemble des classes d'isomorphie de diagrammes commutatifs de S -schémas

$$\begin{array}{ccccc} & & \mathbb{Z}/(n)^2 & & \\ & \nearrow \alpha & & \nwarrow \alpha' & \\ E_n & \longrightarrow & F_n & & \\ \cap & & \cap & & \\ E & \xrightarrow{\varphi} & F & & \end{array} \quad (3.14)$$

où φ est une p -isogénie entre courbes elliptiques et α un isomorphisme. On désigne par q_1 et $q_2 : F_{n,p} \rightarrow M_n$ les morphismes de foncteurs associant à un diagramme (3.14) les sous-diagrammes (E, E_n, α) et (F, F_n, α') .

Proposition (3.15). *Le foncteur $F_{n,p}$ est représenté par un schéma $M_{n,p}$, et les morphismes $q_1, q_2 : M_{n,p} \rightarrow M_n$ sont finis.*

L'automorphisme σ de $F_{n,p}$ envoyant $\varphi : E \rightarrow F$ sur ${}^t\varphi : F \rightarrow E$ échange q_1 et q_2 ; il suffit donc de considérer q_1 . Ce morphisme identifie $F_{n,p}$ au foncteur des sous-groupes d'ordre p de la courbe elliptique universelle E sur M_n , de sorte que, par la théorie des schémas de Hilbert, $F_{n,p}$ est représentable et $M_{n,p}$ propre sur M_n . Si s est un point géométrique de M_n , $q_1^{-1}(s)$ est l'ensemble des sous-groupes d'ordre p de E_s , et a $p+1$ éléments si $\mathrm{char}(k(s)) \neq p$, un seul (le noyau de Frobenius) si $\mathrm{char}(k(s)) = p$. $\square$

On peut montrer que $M_{n,p}$ est régulier, et que q_1 et q_2 sont finis et plats; nous n'utiliserons pas ce résultat délicat, nous contentant ici de noter qu'au-dessus de $\mathrm{Spec}(\mathbb{Z}[1/p])$, chaque q_i fait de $M_{n,p}$ un revêtement étale de degré $p+1$ de M_n .

Les morphismes q_i s'insèrent dans un diagramme commutatif

$$\begin{array}{ccccc} & q_1^* E & \xrightarrow{\varphi} & q_2^* E & \\ & \swarrow & & \searrow & \\ E & & & & E \\ & \searrow u & & \swarrow v & \\ & M_{n,p} & & & \\ & \swarrow q_1 & & \searrow q_2 & \\ E & & & & E \\ & \searrow f_n & & \swarrow f_n & \\ & M_n & & & M_n \end{array} \quad (3.16)$$

où (φ, u, v) fait partie du diagramme universel (3.14).

Note sur la source. Dans le TeX hérité, le diagramme (3.16) attachait u et v à l'objet inférieur $M_{n,p}$ et confondait les deux applications diagonales de changement de base. La source donne $u : q_1^* E \rightarrow M_{n,p}$ et $v : q_2^* E \rightarrow M_{n,p}$, avec deux applications diagonales non étiquetées de chaque changement de base vers E ; le diagramme natif ci-dessus restitue cette topologie.

On désignera par I_p le morphisme de M_n dans M_n correspondant au morphisme de foncteur $(E, \alpha) \mapsto (E, \alpha/p) :$

$$\begin{array}{ccc} E & \longrightarrow & E \\ \downarrow & & \downarrow \\ M_n & \xrightarrow{I_p} & M_n \end{array} \quad I_p^*(E, \alpha) = (E, \alpha/p). \quad (3.17)$$

I_p^* est un automorphisme de $\tilde{H}^i(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}))$. Il est pénible, mais routinier, de démontrer que

Proposition (3.18).

(i) *L'endomorphisme T_p de ${}_n W$ s'exprime, à l'aide de (3.16), comme la flèche composée*

$$\begin{aligned} \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Q})) &\xrightarrow{q_2^*} \tilde{H}^1(M_{n,p}^{\text{an}}, \text{Sym}^k(R^1 v_* \mathbb{Q})) \\ &\xrightarrow{\varphi^*} \tilde{H}^1(M_{n,p}^{\text{an}}, \text{Sym}^k(R^1 u_* \mathbb{Q})) \xrightarrow{q_1^*} \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \mathbb{Q})). \end{aligned}$$

où q_{1*} est le « morphisme trace » pour le revêtement q_1 .

(ii) *De même, $R_p = p^k I_p^*$.*

□

Le lecteur méfiant pourrait oublier les préliminaires adéliques et définir T_p par (i). Pour $n = 1$ ou 2 , on pose ${}_n W = W^{K_n}$, de sorte que

$${}_1 W = {}_n W^{\text{GL}_2(\mathbb{Z}/(n))}.$$

Si S_{k+2} désigne l'espace des formes modulaires paraboliques, pour le groupe $\text{SL}_2(\mathbb{Z})$, de poids $k+2$, l'isomorphisme de Shimura (3.11) induit un isomorphisme

$${}_1^k W_\infty = {}_1^k W \otimes \mathbb{C} = S_{k+2} \oplus \bar{S}_{k+2}.$$

Il est pénible, mais routinier, de démontrer que

Proposition (3.19). *L'endomorphisme T_p de ${}_1^k W_\infty$ s'identifie, par l'isomorphisme de Shimura, à la somme directe de l'opérateur de Hecke sur S_{k+2} (y compris le facteur p^{k-1}), et de son conjugué.*

□

(3.20) On a canoniquement

$$\bigwedge^2 R^1 f_{n*} \mathbb{Z}_\ell \simeq R^2 f_{n*} \mathbb{Z}_\ell \simeq \mathbb{Z}_\ell(-1),$$

de sorte que $\text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell)$ est muni d'une forme bilinéaire (symétrique pour k pair, alternée pour k impair) à valeurs dans $\mathbb{Z}_\ell(-k)$. La forme qui s'en déduit par tensorisation par $\mathbb{Q}_\ell$ est non dégénérée.

Si F est un $\mathbb{Q}_\ell$ -faisceau l.c.c. sur un schéma X lisse purement de dimension n sur un corps algébriquement clos k , alors la dualité de Poincaré donne

$$H^i(X, F)^\vee \simeq H_c^{2n-i}(X, \text{Hom}(F, \mathbb{Q}_\ell(n))),$$

$$H_c^i(X, F)^\vee \simeq H^{2n-i}(X, \text{Hom}(F, \mathbb{Q}_\ell(n))),$$

$$\tilde{H}^i(X, F)^\vee \simeq \tilde{H}^{2n-i}(X, \text{Hom}(F, \mathbb{Q}_\ell(n))).$$

Faisant $X = \bar{M}_n$ et $F = \text{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)$ dans ces considérations, on définit sur ${}_n^k W_\ell$ une forme bilinéaire ${}_n(\cdot, \cdot)$ non dégénérée à valeurs dans $\mathbb{Q}_\ell(-k-1)$. Cette forme est symétrique pour k impair, alternée pour k pair. C'est l'analogue ℓ -adique du produit scalaire de Petersson. Si $n \mid m$, et si le revêtement $\psi : M_m \rightarrow M_n$ est de degré d , on a

$${}_m(\psi^* x, \psi^* y) = d \cdot {}_n(x, y).$$

Note sur la source. Le texte imprimé écrit « Peterson » ici et dans la preuve de (5.6), puis « Pertersson » à la fin. Le nom usuel « Petersson » est rétabli partout. La coquille évidente « isomprhism » de la réédition anglaise sur la même page est également régularisée en « isomorphism » dans l'édition anglaise.

4 La formule de congruence

On se fixe dans ce numéro des entiers $k \geq 0$ et $n \geq 3$, et des nombres premiers p et ℓ . On suppose p premier à ℓ et à n . On désigne par $f_n : E \rightarrow M_n$ la courbe elliptique universelle sur M_n , munie de $\alpha : E_n \xrightarrow{\sim} \mathbb{Z}/(n)^2$.

Quel que soit le schéma Y , on désigne par a l'unique morphisme de Y dans $\mathrm{Spec}(\mathbb{Z})$, ou, le cas échéant, dans un sous-schéma de $\mathrm{Spec}(\mathbb{Z})$. Si Y est séparé et de type fini sur $\mathrm{Spec}(\mathbb{Z})$, et si F est un $\mathbb{Z}_\ell$ - ou $\mathbb{Q}_\ell$ -faisceau sur Y , on note $R^i a_*(Y, F)$, respectivement $R^i a_!(Y, F)$, respectivement $R^i \tilde{a}(Y, F)$, le $\mathbb{Z}_\ell$ - ou $\mathbb{Q}_\ell$ -faisceau sur $\mathrm{Spec}(\mathbb{Z})$ qui est la i -ième image directe supérieure de F par a , respectivement la i -ième image directe à supports propres, respectivement $\mathrm{Im}(R^i a_!(Y, F) \rightarrow R^i a_*(Y, F))$. Pour $m \in \mathbb{N}$, on pose

$$Y[1/m] = Y \times \mathrm{Spec}(\mathbb{Z}[1/m]).$$

Théorème (4.1, Igusa [1]). *Le schéma M_n se compactifie en un schéma en courbes M_n^* , projectif et lisse sur $\mathrm{Spec}(\mathbb{Z}[1/n])$, tel que $M_n^* \setminus M_n$ soit un revêtement étale de $\mathrm{Spec}(\mathbb{Z}[1/n])$.*

Le schéma M_n est formellement lisse, donc lisse sur $\mathrm{Spec}(\mathbb{Z})$. L'invariant modulaire j de la courbe universelle sur M_n est un morphisme de M_n dans la droite affine $\mathbb{A}^1$ sur $\mathrm{Spec}(\mathbb{Z}[1/n])$. Ce morphisme j est fini, et est un revêtement étale en dehors des sections 0 et 1728 de $\mathbb{A}^1$; en effet:

- (a) Deux courbes elliptiques sur un corps algébriquement clos de même invariant j sont isomorphes (par exemple [8] 6.3), donc les fibres géométriques de j sont finies. Les schémas M_n et $\mathbb{A}^1$ étant lisses de même dimension relative sur $\mathrm{Spec}(\mathbb{Z})$, j est quasi-fini et plat.
- (b) Si E est une courbe elliptique sur le corps des fractions K d'un anneau de valuation discrète R , d'invariant j dans R , et dont les points d'ordre n sont rationnels sur K , alors E a une bonne réduction. Le critère valuatif de propreté montre donc que j est propre.
- (c) Si E et F sont deux courbes elliptiques sur un schéma S , de même invariant j , et si j et $j - 1728$ sont inversibles, alors le schéma $\mathrm{Isom}(S; E, F)$ des isomorphismes entre E et F est étale sur S ([8] 6.3). Dans le diagramme

$$\begin{array}{ccc} \mathrm{Isom}(M_n \times_{\mathbb{A}^1} M_n; \mathrm{pr}_1^* E, \mathrm{pr}_2^* E) & \sim & M_n \times \mathrm{GL}_2(\mathbb{Z}/(n)) \\ \downarrow u & & \downarrow v \\ M_n \times_{\mathbb{A}^1} M_n & \xrightarrow{\mathrm{pr}_1} & M_n, \end{array}$$

où $j \neq 0, 1728$, u et v sont étales surjectifs; donc pr_1 est étale et, par descente plate, j est étale.

La section à l'infini de la droite projective $\mathbb{P}^1 \supset \mathbb{A}^1$ sur $\mathrm{Spec}(\mathbb{Z}[1/n])$ est un diviseur régulier, de point générique de caractéristique 0, dans un schéma régulier. Il résulte alors d'un théorème d'Abhyankar (voir [5]) que, le long de ce diviseur $j = \infty$, M_n est modérément ramifié sur $\mathbb{P}^1$, et que le normalisé M_n^* de $\mathbb{P}^1$ dans M_n vérifie (4.1). $\square$

Note sur la source. Les deux témoins imprimés donnent « Abyankhar »; le nom usuel « Abhyankar » est rétabli. L'hésitation de la réédition anglaise « moderately (tamely?) ramified » est résolue, dans l'édition anglaise, par le terme mathématique standard « tamely ramified »; le français diplomatique conserve exactement « modérément ramifié ».

Du même théorème résulte que les $\mathbb{Z}_\ell$ -faisceaux l.c.c. $R^i f_{n*} \mathbb{Z}_\ell$ sur $M_n[1/\ell]$ sont modérément ramifiés à l'infini. De là, de (4.1) et des théorèmes de spécialisation en cohomologie ℓ -adique (voir [5]), il résulte que $R^i a_*(M_n, \mathrm{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$, $R^i a_!(M_n, \mathrm{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$, et donc $R^i \tilde{a}(M_n, \mathrm{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$ sont des $\mathbb{Z}_\ell$ -faisceaux l.c.c. sur $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$, de formation compatible à tout changement de base.

Corollaire (4.2). *Le module galoisien ${}_n W_\ell$ est la fibre en le point géométrique $\overline{\mathbb{Q}}$ de $\mathrm{Spec}(\mathbb{Z}[1/n, 1/\ell])$ du $\mathbb{Q}_\ell$ -faisceau l.c.c.*

$$R^1 \tilde{a}(M_n, \mathrm{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell)) \otimes \mathbb{Q}_\ell$$

Il est non ramifié en dehors de n et de ℓ .

$\square$

Note sur la source. L'original français numérote ce corollaire « 3.2 » au milieu du §4. La suite après le Théorème 4.1 et la réédition anglaise imposent 4.2; cette coquille de numérotation est corrigée visiblement ici.

Soient sur $M_n \otimes \mathbb{F}_p$ les deux diagrammes commutatifs

$$\begin{array}{ccc}
 & \mathbb{Z}/(n)^2 & \\
 \alpha \nearrow & & \nwarrow \alpha^{(p)} \\
 E_n & \xrightarrow{\quad} & E_n^{(p)} \\
 \downarrow & & \downarrow \\
 E & \xrightarrow{\quad F \quad} & E^{(p)}
 \end{array}
 \qquad
 \begin{array}{ccc}
 & \mathbb{Z}/(n)^2 & \\
 p\alpha^{(p)} \nearrow & & \nwarrow \alpha \\
 E_n^{(p)} & \xrightarrow{\quad} & E_n \\
 \downarrow & & \downarrow \\
 E^{(p)} & \xrightarrow{\quad V \quad} & E
 \end{array}$$

plus brièvement sous la forme

$$F : (E, \alpha) \rightarrow (E^{(p)}, \alpha^{(p)}) \quad \text{et} \quad V : (E^{(p)}, p\alpha^{(p)}) \rightarrow (E, \alpha),$$

où F est le morphisme de Frobenius et V , son transposé, le « Verschiebung ». Ces diagrammes définissent des morphismes Φ_1 et Φ_2 de $M_n \otimes \mathbb{F}_p$ dans $M_{n,p}$. Ces morphismes sont finis, en tant que section de q_1 ou q_2 , et définissent un morphisme

$$\Phi = \Phi_1 \amalg \Phi_2 : M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p \rightarrow M_{n,p} \otimes \mathbb{F}_p.$$

Note sur la source. Les tableaux hérités répétaient à tort les étiquettes F et V sur les flèches induites entre les sous-schémas de n -torsion. Dans la source, ces flèches horizontales supérieures ne sont pas étiquetées; seules les applications entre courbes elliptiques portent F et V . Les diagrammes natifs ci-dessus rétablissent cette distinction. Soit Φ^h la restriction de Φ aux ouverts M_n^h et $M_{n,p}^h$ de $M_n \otimes \mathbb{F}_p$ et de $M_{n,p} \otimes \mathbb{F}_p$ correspondant aux courbes d'invariant de Hasse h non nul.

Proposition (4.3). Φ^h est un isomorphisme.

Soit $\varphi : E_1 \rightarrow E_2$ une p -isogénie entre courbes elliptiques d'invariant de Hasse inversible sur un schéma S de caractéristique p . En chaque point géométrique de S , ou bien le noyau $\ker(\varphi)$ de φ est étale sur S , ou bien son dual de Cartier, isomorphe à $\ker({}^t\varphi)$, est étale sur S . La propriété « $\ker(\varphi)$ est étale » est une propriété ouverte, de sorte que, localement sur S , ou bien $\ker(\varphi)$ est purement infinitésimal, ou bien $\ker({}^t\varphi)$ l'est. Le seul sous-groupe infinitésimal d'ordre p de E_1 ou E_2 étant le noyau de Frobenius, dans le premier cas, φ est isomorphe à $F : E_1 \rightarrow E_1^{(p)}$, et dans le second, ${}^t\varphi$ est isomorphe à $F : E_2 \rightarrow E_2^{(p)}$, donc φ à $V : E_2^{(p)} \rightarrow E_2$. $\square$

Proposition (4.4).

- (i) Le schéma $M_{n,p}$ est lisse sur $\text{Spec}(\mathbb{Z})$ en dehors des points de caractéristique p où $h = 0$.
- (ii) Les morphismes q_1 et q_2 induisent des morphismes finis plats q'_1 et q'_2 de la normalisation $M'_{n,p}$ de $M_{n,p}$ vers M_n .
- (iii) Le morphisme Φ se factorise par un morphisme surjectif

$$\Phi' : M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p \rightarrow M'_{n,p} \otimes \mathbb{F}_p.$$

L'automorphisme σ de (3.15) échange φ et ${}^t\varphi$; il suffit donc de prouver (i) en les points de caractéristique p de $M_{n,p}$ où le noyau de φ est infinitésimal: il n'y a pas d'obstruction à relever infinitésimalement une courbe elliptique et la partie infinitésimale du noyau de la multiplication par p .

Là où $p = h = 0$, la fibre du morphisme fini (3.15) $q_i : M_{n,p} \rightarrow M_n$ est réduite à un point, de sorte que l'ouvert de lissité de $M_{n,p}$ est dense dans $M_{n,p}$ et que $M'_{n,p}$ est partout de dimension 2. Le schéma M_n étant régulier, d'après EGA 0_{IV} 16.5.1 et 17.3.5(ii), le morphisme $q_i : M'_{n,p} \rightarrow M_n$ est plat. Enfin, (iii) résulte de ce que Φ est fini et $M_n \otimes \mathbb{F}_p$ une courbe normale. $\square$

L'endomorphisme de Hecke T_p de ${}_nW_\ell$, tel qu'il est explicité en (3.18), est le tensorisé par $\mathbb{Q}_\ell$ de la fibre au point géométrique $\overline{\mathbb{Q}}$ de $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$ de l'endomorphisme (encore désigné par T_p) de $R^1\tilde{a}(M_n, \text{Sym}^k(R^1f_{n*}\mathbb{Z}_\ell))$

défini par la « correspondance »

$$\begin{array}{ccccc}
q_1'^* E & \xrightarrow{\varphi} & q_2'^* E & & \\
\swarrow & & \searrow & & \\
E & & M'_{n,p} & & E \\
\searrow & & \swarrow & & \swarrow \\
M_n & & M_n & & M_n
\end{array}
\quad (4.5)$$

avec

$$T_p = q'_{1*} \varphi^* q'^*_{2*} \quad (\text{cf. 3.18}).$$

Note sur la source. Comme dans la version héritée de (3.16), le tableau hérité de (4.5) attachait u et v à l'objet modulaire inférieur et confondait deux applications distinctes des changements de base vers les courbes. Le diagramme natif rétablit les neuf flèches de la source. Les endomorphismes R_n et I_n s'interprètent de même.

Lemme (4.6). Soient sur un schéma noethérien S quatre schémas séparés de type fini X, Y, Z_1, Z_2 , F un $\mathbb{Z}_\ell$ -faisceau sur X , G un $\mathbb{Z}_\ell$ -faisceau sur Y , et désignons par a chacune des flèches structurelles de X, Y, Z_1 ou Z_2 dans S .

Soient un diagramme commutatif de S -schémas, et des morphismes de faisceaux:

$$\begin{array}{ccccc} y_1^* G & \xrightarrow{z_1} & x_1^* F & & y_2^* G & \xrightarrow{z_2} & x_2^* F \\ & & & & & & \\ & & Z_1 & \xrightarrow{f} & Z_2 & & \\ & \swarrow x_1 & & & & \searrow y_2 & \\ X & & & & & & Y \\ & \nwarrow x_2 & & & \nearrow y_1 & & \end{array}$$

*Supposons que $f^*z_2 = z_1$, que y_1 et y_2 sont propres, que x_1 et x_2 sont finis et plats, et que, pour tout point géométrique s de Z_2 , la multiplicité de s dans sa fibre $x_2^{-1}(x_2(s))$ est égale à la somme des multiplicités dans leur fibre (pour x_1) des points géométriques de Z_1 image réciproque de s par f . Alors, le diagramme*

$$\begin{array}{ccccccc}
R^i \widetilde{a}(Y, G) & \xrightarrow{y_1^*} & R^i \widetilde{a}(Z_1, G) & \xrightarrow{z_1} & R^i \widetilde{a}(Z_1, F) & \xrightarrow{x_1^*} & R^i \widetilde{a}(X, F) \\
\parallel & & \uparrow f^* & & \uparrow f^* & & \parallel \\
R^i \widetilde{a}(Y, G) & \xrightarrow{y_2^*} & R^i \widetilde{a}(Z_2, G) & \xrightarrow{z_2} & R^i \widetilde{a}(Z_2, F) & \xrightarrow{x_2^*} & R^i \widetilde{a}(X, F)
\end{array}$$

est commutatif.

Note sur la source. Les tableaux hérités avaient perdu la paire d'objets partagée $Z_1 \rightarrow Z_2$ du diagramme structural et désignaient les applications verticales dans les deux diagrammes cohomologiques. Les diagrammes sont reconstruits nativement avec les objets partagés de la source et ses flèches diagonales, verticales, d'égalité, de changement de base et de trace distinctes. Une réparation antérieure avait dupliqué $Z_1 \rightarrow Z_2$ en deux copies disjointes; la relecture directe de l'original français, p. 164, a révélé cette erreur topologique résiduelle, désormais corrigée dans les deux éditions.

Ce lemme résulte des lemmes analogues pour $R^i a_!$ et $R^i a_{*}$. La commutativité des premiers carrés est triviale. Le dernier se réécrit

$$\begin{array}{ccccc} R^i \widetilde{a}(Z_1, x_1^* F) & \xleftarrow{\sim} & R^i \widetilde{a}(X, x_{1*} x_1^* F) & \xrightarrow{\mathrm{Tr}} & R^i \widetilde{a}(X, F) \\ \uparrow & & \uparrow & & \parallel \\ R^i \widetilde{a}(Z_2, x_2^* F) & \xleftarrow{\sim} & R^i \widetilde{a}(X, x_{2*} x_2^* F) & \xrightarrow{\mathrm{Tr}} & R^i \widetilde{a}(X, F) \end{array}$$

et l'on rappelle la définition de la trace pour vérifier que le carré

$$\begin{array}{ccc} x_{1*}x_1^*F & \xrightarrow{\text{Tr}} & F \\ \uparrow & & \parallel \\ x_{2*}x_2^*F & \xrightarrow{\text{Tr}} & F \end{array}$$

est commutatif. $\square$

(4.7) On désignera par $T_p/\mathbb{F}_p$ l'endomorphisme induit par T_p sur la restriction à $\text{Spec}(\mathbb{F}_p)$ du $\mathbb{Z}_\ell$ -faisceau l.c.c. $R^1\tilde{a}(M_n, \text{Sym}^k R^1 f_{n*}\mathbb{Z}_\ell)$. On a

$$R^1\tilde{a}(M_n, \text{Sym}^k R^1 f_{n*}\mathbb{Z}_\ell)|_{\text{Spec}(\mathbb{F}_p)} \xrightarrow{\sim} R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k R^1 f_{n*}\mathbb{Z}_\ell);$$

la formation du morphisme trace pour un morphisme fini et plat est compatible au changement de base, de sorte que $T_p/\mathbb{F}_p$ peut se construire, sur le modèle (3.18), à partir de la fibre en $\mathbb{F}_p$ de la « correspondance » (4.5). Le lemme (4.6), appliqué au diagramme commutatif

$$\begin{array}{ccc} M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p & \xrightarrow{\Phi'} & M'_{n,p} \otimes \mathbb{F}_p \\ \downarrow & \swarrow q'_1 & \\ M_n \otimes \mathbb{F}_p & & \end{array} \quad \begin{array}{ccc} M_n \otimes \mathbb{F}_p \amalg M_n \otimes \mathbb{F}_p & \xrightarrow{\Phi'} & M'_{n,p} \otimes \mathbb{F}_p \\ & \searrow q'_2 & \downarrow \\ & & M_n \otimes \mathbb{F}_p, \end{array}$$

fournit alors une décomposition de $T_p/\mathbb{F}_p$ en la somme des endomorphismes définis par les deux correspondances suivantes:

$$(a) \quad \begin{array}{ccccc} & (E, \alpha) & \xrightarrow{F} & (E^{(p)}, \alpha^{(p)}) = F^*(E, \alpha) & \\ & \parallel & \searrow & \swarrow & \\ (E, \alpha) & & M_n \otimes \mathbb{F}_p & & (E, \alpha) \\ & \searrow & \parallel & \searrow & \\ & M_n \otimes \mathbb{F}_p & & M_n \otimes \mathbb{F}_p & \end{array}$$

où F est le Frobenius absolu. On reconnaît dans cette correspondance le Frobenius géométrique

$$(b) \quad \begin{array}{ccccc} & x^*(E, \alpha) = (E^{(p)}, p\alpha^{(p)}) & \xrightarrow{V} & (E, \alpha) & \\ & \swarrow & \searrow f_n^{(p)} & \swarrow f_n & \\ (E, \alpha) & & M_n \otimes \mathbb{F}_p & & (E, \alpha) \\ & \searrow & \swarrow x & \searrow & \\ & M_n \otimes \mathbb{F}_p & & M_n \otimes \mathbb{F}_p & \end{array}$$

Note sur la source. Les tableaux hérités des correspondances (a) et (b) ne conservaient que quatre des huit relations descendantes de la source et représentaient deux relations d'égalité par des flèches. Les diagrammes natifs rétablissent toutes les diagonales, les deux relations d'égalité de chaque correspondance, ainsi que les étiquettes $f_n^{(p)}$, f_n , x et F à leurs points d'attache imprimés. La flèche x est la flèche composée $I_p^{-1} \circ F$:

$$\begin{array}{ccccc} (E, \alpha) & \longleftarrow & (E, p\alpha) & \longleftarrow & (E^{(p)}, p\alpha^{(p)}) \\ \downarrow & & \downarrow & & \downarrow \\ M_n \otimes \mathbb{F}_p & \xleftarrow{I_p^{-1}} & M_n \otimes \mathbb{F}_p & \xleftarrow{F} & M_n \otimes \mathbb{F}_p. \end{array}$$

L'endomorphisme correspondant est donc le composé de

$$V : R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k(R^1 f_{n*}\mathbb{Z}_\ell)) \xrightarrow{V^*} R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k(R^1 f_{n*}^{(p)}\mathbb{Z}_\ell)) \xrightarrow{\text{Tr}_F} R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k(R^1 f_{n*}\mathbb{Z}_\ell))$$

et de

$$I_p^* = \text{Tr}_{I_p^{-1}} : \text{endomorphisme de } R^1\tilde{a}(M_n \otimes \mathbb{F}_p, \text{Sym}^k R^1 f_{n*}\mathbb{Z}_\ell).$$

Proposition (4.8). *On a $T_p/\mathbb{F}_p = F + I_p^*V$, et*

- (i) *F s'identifie à l'inverse de l'élément de Frobenius (« arithmétique ») φ_p du groupe de Galois $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ agissant sur $\tilde{H}^1(M_n \otimes \overline{\mathbb{F}}_p, \text{Sym}^k(R^1 f_{n*}\mathbb{Z}_\ell))$;*
- (ii) *F et V sont transposés l'un de l'autre relativement au produit scalaire (3.20);*
- (iii) *$FV = VF = p^{k+1}$.*

Pour la relation (i) entre Frobenius géométrique et arithmétique, on renvoie à l'exposé de C. Houzel (SGA 5.XV). Le composé VF est le composé des homomorphismes déduits des flèches suivantes:

$$\begin{array}{ccccccc}
 E & \longleftarrow & E^{(p)} & \xrightarrow{F_E} & E & \xrightarrow{V_E} & E^{(p)} \longrightarrow E \\
 \downarrow & & & \searrow & \downarrow & \swarrow & \\
 M_n & \xrightarrow{\quad F \quad} & M_n & & M_n & \xrightarrow{\quad F \quad} & M_n
 \end{array}$$

Note sur la source. Le tableau hérité réduisait le diagramme imprimé à cinq objets $E \leftarrow E^{(p)} \rightarrow E \rightarrow E^{(p)} \rightarrow E$ à trois objets, omettant ainsi les deux tordus de Frobenius intermédiaires et leurs applications structurales diagonales. Le diagramme natif complet ci-dessus rétablit les cinq objets et les onze flèches de la source. Ainsi

$$VF = \text{Tr}_F \circ F_E^* \circ V_E^* \circ F^*.$$

La flèche $F_E^* V_E^* = (F_E V_E)^* = (p \cdot 1_E)^*$ agit par multiplication par p^k sur $\text{Sym}^k R^1 f_{n*}\mathbb{Z}_\ell$, de sorte que

$$VF = p^k \text{Tr}_F \circ F^* = p^k \cdot p = p^{k+1},$$

car $F : M_n \rightarrow M_n$ est de degré p .

Par transport de structure, φ_p respecte le produit scalaire (3.20), à valeur dans $\mathbb{Q}_\ell(-k-1)$, groupe sur lequel φ_p agit par multiplication par p^{-k-1} . On a donc

$$(Fx, y) = p^{k+1}(\varphi_p Fx, \varphi_p y) = (x, p^{k+1} F^{-1}y) = (x, Vy).$$

□

Le théorème suivant, synonyme de (4.8), remonte à Eichler.

Théorème (4.9, formule de congruence). *Soient $K_{n,\ell}$ la plus grande sous-extension de $\overline{\mathbb{Q}}$ non ramifiée en dehors de n et ℓ , φ_p un élément de Frobenius relatif à p dans $\text{Gal}(K_{n,\ell}/\mathbb{Q})$, F l'endomorphisme φ_p^{-1} de ${}_n W_\ell$ et V le transposé de F relativement au produit scalaire (3.20). Alors,*

$$T_p = F + I_p^*V, \quad FV = p^{k+1}, \quad 1 - T_p X + p R_p X^2 = (1 - FX)(1 - I_p^*VX).$$

□

5 Weil implique Ramanujan

Si p est un nombre premier et X un schéma sur $\mathbb{F}_p$, on désignera par $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, par $F : X \rightarrow X$ l'endomorphisme de Frobenius (« géométrique »), et on posera $\overline{X} = X \otimes \overline{\mathbb{F}}_p$; ℓ désignera toujours un nombre premier distinct de p .

Par « conjectures de Weil », on entendra l'énoncé suivant: soient X un schéma projectif et lisse sur $\mathbb{F}_p$ et ℓ un nombre premier distinct de p . Alors, les valeurs propres de l'endomorphisme F^* de $H^i(\overline{X}, \mathbb{Q}_\ell)$ sont des entiers algébriques dont tous les conjugués complexes sont de valeur absolue $p^{i/2}$.

Avec les hypothèses et notations de 4.9, on a (rappelons que $(p, n) = 1$):

Théorème (5.1). *Si les conjectures de Weil sont vraies, alors les valeurs propres de l'endomorphisme F de ${}_n W_\ell$ sont des entiers algébriques (dont tous les conjugués complexes sont) de valeur absolue $p^{(k+1)/2}$.*

Note sur la source. L'énoncé imprimé parle des « valeurs absolues de l'endomorphisme » et donne $p^{k+1/2}$. Le théorème porte sur les valeurs propres de F , et le poids est $k+1$; on livre donc la lecture mathématiquement requise $p^{(k+1)/2}$.

Admettons les conjectures de Weil.

Lemme (5.2, modulo Weil). *Soit X un schéma lisse sur $\mathbb{F}_p$, qui puisse se représenter comme un ouvert dans un schéma projectif et lisse X^* . Alors, les valeurs propres de l'endomorphisme F^* de $\tilde{H}^i(X, \mathbb{Q}_\ell)$ sont des entiers algébriques de valeur absolue $p^{i/2}$.*

Note sur la source. La formule imprimée « valeurs absolues de l'endomorphisme » est corrigée en « valeurs propres de l'endomorphisme »; la valeur absolue $p^{i/2}$ est inchangée.

La flèche naturelle de $H_c^i(X, \mathbb{Q}_\ell)$ dans $H^i(X, \mathbb{Q}_\ell)$ se factorise par $H^i(X^*, \mathbb{Q}_\ell)$:

$$H_c^i(X, \mathbb{Q}_\ell) \rightarrow H^i(X^*, \mathbb{Q}_\ell) \rightarrow H^i(X, \mathbb{Q}_\ell),$$

de sorte qu'en tant que $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ -module, $\tilde{H}^i(X, \mathbb{Q}_\ell)$ est quotient d'un sous-objet de $H^i(X^*, \mathbb{Q}_\ell)$. $\square$

Lemme (5.3, modulo Weil). *Soient S un schéma lisse sur $\mathbb{F}_p$ et $f : A \rightarrow S$ un schéma abélien sur S . Supposons que A puisse se représenter comme un ouvert dans un schéma A^* projectif et lisse sur $\mathbb{F}_p$. Alors, l'endomorphisme de Frobenius géométrique F^* de $\tilde{H}^i(S, R^j f_* \mathbb{Q}_\ell)$ a pour valeurs propres des entiers algébriques de valeur absolue $p^{(i+j)/2}$.*

Note sur la source. L'exposant imprimé est $i + j/2$. Le poids cohomologique étant $i + j$, l'exposant requis est $(i + j)/2$, comme livré ci-dessus et comme l'exige l'application de (5.2) dans la preuve.

Soit m un entier > 1 , et considérons les suites spectrales de Leray

$$E : E_2^{ij} = H^i(\bar{S}, R^j f_* \mathbb{Q}_\ell) \implies H^{i+j}(\bar{A}, \mathbb{Q}_\ell), \quad {}_c E : {}_c E_2^{ij} = H_c^i(\bar{S}, R^j f_* \mathbb{Q}_\ell) \implies H_c^{i+j}(\bar{A}, \mathbb{Q}_\ell).$$

L'endomorphisme de multiplication par m , $\psi_m = m \cdot 1_A$, définit des endomorphismes de E et de ${}_c E$ qui s'insèrent dans un diagramme commutatif

$$\begin{array}{ccc} {}_c E & \longrightarrow & E \\ \psi_m^* \downarrow & & \psi_m^* \downarrow \\ {}_c E & \longrightarrow & E. \end{array}$$

ψ_m^* agit sur $R^j f_* \mathbb{Q}_\ell$ par multiplication par m^j , de sorte que sur les termes ${}_c E_r^{ij}$ et E_r^{ij} de ${}_c E$ et de E , ψ_m^* est la multiplication par m^j . Les flèches d_r pour $r \geq 2$ commutent à ψ_m^* et envoient E_r^{ij} (resp. ${}_c E_r^{ij}$) dans E_{r-1}^{i+j} (resp. ${}_c E_{r-1}^{i+j}$), avec $j \neq j'$. Elles sont donc nulles, et E_2^{ij} (resp. ${}_c E_2^{ij}$) s'identifie au sous-espace de $H^{i+j}(\bar{A}, \mathbb{Q}_\ell)$ (resp. de $H_c^{i+j}(\bar{A}, \mathbb{Q}_\ell)$) où $\psi_m^* = m^j$. Dès lors, $\tilde{H}^i(S, R^j f_* \mathbb{Q}_\ell)$ s'identifie, comme module galoisien, au sous-espace de $\tilde{H}^{i+j}(A, \mathbb{Q}_\ell)$ où $\psi_m^* = m^j$, et on applique (5.2). L'astuce utilisée ici est due à Lieberman. $\square$

Note sur la source. La preuve imprimée affirme que ces différentielles sont non nulles. Comme elles commutent à ψ_m^* tout en reliant les espaces propres distincts m^j et $m^{j'}$, avec $j \neq j'$, elles sont nulles; c'est exactement la dégénérescence utilisée dans l'identification suivante.

Soit $f_n : E \rightarrow M_n \otimes \mathbb{F}_p$ la courbe elliptique universelle sur $M_n \otimes \mathbb{F}_p$, et soit $f_{n,k} : E_k \rightarrow M_n \otimes \mathbb{F}_p$ son produit fibré itéré k -uple avec elle-même. La formule de Kunneth montre que le $\mathbb{Q}_\ell$ -faisceau $R^k f_{n,k*} \mathbb{Q}_\ell$ admet comme facteur direct la puissance tensorielle k -ième de $R^1 f_{n*} \mathbb{Q}_\ell$; celle-ci à son tour contient comme facteur direct le $\mathbb{Q}_\ell$ -faisceau $\text{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)$. Le théorème 5.1 résulte donc de (5.3) et du lemme suivant.

Lemme (5.4). *Le schéma E_k est un ouvert d'un schéma E_k^* projectif et lisse sur $\mathbb{F}_p$.*

Soit E^* le modèle minimal de Néron de E sur $M_n^* \otimes \mathbb{F}_p$ (4.1). Le schéma E^* est projectif et lisse sur $\mathbb{F}_p$. Puisque $n \geq 3$ et que les points d'ordre n de E forment un revêtement trivial de $M_n \otimes \mathbb{F}_p$, ce modèle de Néron est « semi-stable » (cas a ou b_m dans la classification de Néron). En particulier, la projection $f_n : E^* \rightarrow M_n^*$ n'a qu'un nombre fini de points de non lissité, et, en ces points, f_n est non dégénérée (présente une singularité quadratique ordinaire).

Soit E_k^{**} le produit fibré itéré k -uple de E^* sur M_n^* . Pour prouver (5.4), il suffit de résoudre les singularités de E_k^{**} sans toucher à l'ouvert E_k . Prouvons tout d'abord:

Lemme (5.5). *Soit V la sous-variété de l'espace affine sur un corps k , de coordonnées $(X_i)_{0 \leq i \leq r}$, $(Y_i)_{0 \leq i \leq r}$, $(T_i)_{1 \leq i \leq s}$, d'équation*

$$X_0 Y_0 = X_1 Y_1 = \cdots = X_r Y_r.$$

Soit $\mathfrak{m}$ l'idéal de $\mathcal{O}_V$ engendré par les monômes qui se déduisent du monôme $\prod_{i=0}^r X_i^i$ par une permutation des coordonnées qui respecte l'ensemble des paires $\{X_i, Y_i\}$, $0 \leq i \leq r$. Alors $\mathfrak{m} = \mathcal{O}_V$ en dehors du lieu singulier de V , et la variété $\tilde{V}$ déduite de V en éclatant $\mathfrak{m}$ est lisse sur k .

Le lieu singulier est le lieu où quatre coordonnées X_i, Y_i, X_j, Y_j ($i \neq j$) s'annulent. L'ouvert affine de $\tilde{V}$ défini par l'élément $\prod_{i=1}^r X_i^i$ de l'idéal à éclater $\mathfrak{m}$ est le spectre de l'anneau régulier

$$k[Y_0/X_1, X_0/X_1, X_1/X_2, \dots, X_{r-1}/X_r, X_r, T_1, \dots, T_s]$$

(pour le vérifier, noter que $X_i/X_{i+1} = Y_{i+1}/Y_i$), et 5.5 en résulte. $\square$

On montre maintenant que, localement pour la topologie étale, les singularités de E_k^{**} sont isomorphes à celles de V (pour $r = k - 1$), et que ceci permet de définir sur E_k^{**} un idéal $\mathfrak{m}$ analogue à l'idéal $\mathfrak{m}$ de (5.5). Éclatant cet idéal, on obtient E_k^* . $\square$

Une approximation du théorème suivant a été démontrée par Ihara [2]:

Théorème (5.6). *Les conjectures de Weil impliquent la conjecture de Ramanujan.*

Notons tout d'abord que (5.1) reste vrai pour $n = 1$, car ${}^k_1W_\ell$ est le sous-module galoisien de ${}^k_mW_\ell$ invariant par $\mathrm{GL}_2(\mathbb{Z}/(m))$. Sur ${}^k_1W_\ell$, I_p^* induit l'identité, et (4.8) se réduit à

$$1 - T_p X + p^{k+1} X^2 = (1 - FX)(1 - VX).$$

Les endomorphismes F et V sont transposés l'un de l'autre, de sorte que

$$\det(1 - FX; {}^k_1W_\ell) = \det(1 - VX; {}^k_1W_\ell).$$

L'action de T_p sur ${}^k_1W_\ell$ est induite par son action sur k_1W , et est compatible à la décomposition de ${}^k_1W \otimes \mathbb{C}$ en la somme de l'espace S_{k+2} des formes modulaires paraboliques relatives à $\mathrm{SL}_2(\mathbb{Z})$, de poids $k + 2$, et de l'espace complexe conjugué. Du caractère hermitien de T_p (pour le produit scalaire de Petersson) et de (3.19), on déduit alors que

$$\det(1 - T_p X + p^{k+1} X^2; {}^k_1W_\ell) = \det(1 - T_p X + p^{k+1} X^2; S_{k+2})^2,$$

et

$$\det(1 - T_p X + p^{k+1} X^2; S_{k+2})^2 = \det(1 - FX; {}^k_1W_\ell)^2,$$

soit

$$\det(1 - T_p X + p^{k+1} X^2; S_{k+2}) = \det(1 - FX; {}^k_1W_\ell). \quad (5.7)$$

Reprenons les notations du n° 1 et faisons $k = 10$. En vertu de la théorie de Hecke et de (3.19), (5.7) se réécrit

$$H_p(X) = \det(1 - FX; {}^{10}_1W_\ell),$$

et l'on applique (5.1). $\square$

On vérifie de même que les conjectures de Weil impliquent la généralisation par Petersson de la conjecture de Ramanujan.

Références

- [1] J. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Am. J. of Math. **81** (1959), 561–577.
- [2] Y. Ihara, *Hecke polynomials as congruence zeta functions in elliptic modular case*, Ann. of Math., S.2 **85** (1967), 267–295.
- [3] J.-P. Jouanolou, exposés V et VI de SGA 5.
- [4] M. Kuga et G. Shimura, *On the zeta function of a fibre variety whose fibres are abelian varieties*, Ann. of Math., S.2 **82** (1965), 478–539.
- [5] M. Raynaud, exposé XIII de SGA 1 et appendice (à paraître).
- [6] J.-P. Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Sémin. Delange–Pisot–Poitou, 1967/68, no. 14.
- [7] G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. of Japan **11** (1959), 291–311.
- [8] J. Tate, *Courbes elliptiques: formulaire*, mis au goût du jour par P. Deligne, notes miméographiées par l'I.H.E.S.
- [9] J.-L. Verdier, *Sur les intégrales attachées aux formes automorphes* (d'après G. Shimura), Sémin. Bourbaki, février 1961, exp. 216.

Sigles. EGA: *Éléments de géométrie algébrique*, par A. Grothendieck et J. Dieudonné, Publ. Math. I.H.E.S.

SGA: *Séminaire de géométrie algébrique du Bois-Marie*, Notes miméographiées par l'I.H.E.S., à paraître à North-Holland.