

SÉMINAIRE N. BOURBAKI

PIERRE DELIGNE

Formes modulaires et représentations ℓ -adiques

Séminaire N. Bourbaki, 1971, exp. n° 355, p. 139-172

http://www.numdam.org/item?id=SB_1968-1969__11__139_0

© Association des collaborateurs de Nicolas Bourbaki, 1971, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

FORMES MODULAIRES ET REPRÉSENTATIONS ℓ -ADIQUES

par Pierre DELIGNE

N° 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

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

On sait que la fonction Δ est à un facteur constant près l'unique forme modulaire parabolique de poids 12 pour le groupe $SL_2(\mathbb{Z})$.

Posons, pour p premier,

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

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 $p^{-11/2}$ (i.e. 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 la fonction L_{τ} comme la fonc-

tion 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 le groupe de Galois $\text{Gal}(K_\ell/\mathbb{Q})$, de l'élément de Frobenius φ_p relatif à p . Ce dernier 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 $\text{Gal}(K_\ell/\mathbb{Q})$ dans un $\mathbb{Q}_\ell$ -vectoriel W_ℓ de rang 2 telle que, pour chaque $p \neq \ell$, on ait

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

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 $\text{SL}_2(\mathbb{R})$. 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 module S des courbes elliptiques (oublions qu'elle n'existe pas) et si E^k est le produit fibré itéré k -uplet de E avec elle-même sur S , alors $L_T(s)$ 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 pointes, 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].

Notations.

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

$$\mathbf{A}_S^f = \prod_{p \in S} \mathbf{Q}_p \times \prod_{p \notin S} \mathbf{Z}_p \subset \mathbf{A}^f.$$

Pour $S = \emptyset$, on écrit $\hat{\mathbf{Z}} = \mathbf{A}_{\emptyset}^f$.

- 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 additifs et multiplicatifs.

- Une courbe elliptique est une variété abélienne de dimension un, en particulier est munie d'une origine.

- Si $\mathcal{L}$ est un faisceau inversible et si $n \in \mathbf{Z}$, on désigne par $\mathcal{L}^n$ sa puissance tensorielle n -ième $\mathcal{L}^{\otimes n}$.

- On désigne par $\bar{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$.

- Le signe $\square$ marque la fin d'une démonstration ou son absence.

N° 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 S -groupe $\mu : E \times_S E \rightarrow E$, dont l'unité soit la section e . A une courbe elliptique sont associés :

(a) Le faisceau inversible $\omega_E = e^* \Omega_{E/S}^1$. L'algèbre de Lie relative $\underline{\text{Lie}}_S(E)$ 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 $R^1 f_* \underline{\mathbb{Z}}$. On posera $T_{\mathbb{Z}}(E) = R^1 f_* \underline{\mathbb{Z}}^\vee$ et $T_{\mathbb{Q}}(E) = T_{\mathbb{Z}}(E) \otimes \mathbb{Q}$ (système local de l'homologie de E sur S).

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

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

de sorte que la courbe elliptique E se reconstitue à partir de la flèche α .

Le système local $\Lambda^2 R^1 f_* \underline{\mathbb{Z}} \sim R^2 f_* \underline{\mathbb{Z}}$ est canoniquement isomorphe à $\underline{\mathbb{Z}}$. Un isomorphisme entre $\underline{\mathbb{Z}}^2$ et $R^1 f_* \underline{\mathbb{Z}}$ sera dit permis s'il induit -1 (sic) sur les puissances extérieures secondes.

Désignons par $\text{Hom}^+(\mathbb{R}^2, \mathbb{C})$ l'ensemble des isomorphismes (de $\mathbb{R}$ -vectoriel) entre $\mathbb{R}^2$ et $\mathbb{C}$ qui ne respectent pas (sic) les orientations naturelles de $\mathbb{R}^2$ et $\mathbb{C}$ (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 on posera

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

Cet espace est muni de la structure complexe déduite de son inclusion dans le vectoriel complexe $\text{Hom}(\mathbb{Z}^2, \mathbb{C})$. Au-dessus de cet espace, on dispose d'une suite exacte "universelle"

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

PROPOSITION 2.2.- (i) Le foncteur qui, à chaque espace analytique S , associe l'ensemble des classes d'isomorphie de courbes elliptiques E sur S , munies d'isomorphismes $\omega_E \sim \mathbb{G}_a$ et $R^1 f_* \underline{\mathbb{Z}} \sim \underline{\mathbb{Z}}^2$ (ce dernier étant permis) est représenté par l'espace analytique $\text{Hom}^+(\mathbb{R}^2, \mathbb{C})$, muni de la courbe elliptique universelle E_0

(ii) Le foncteur qui, à chaque espace analytique S , associe l'ensemble des

classes d'isomorphie de courbes elliptiques sur S , munies d'un isomorphisme permis $R^1 f_* \underline{\mathbb{Z}} \sim \underline{\mathbb{Z}}^2$, est représenté par l'espace analytique $X = \mathbb{C}^* \backslash \text{Hom}^+(\mathbb{R}^2, \mathbb{C})$ (demi-plan de Poincaré).

(iii) L'espace $\text{Hom}^+(\mathbb{R}^2, \mathbb{C})$ est un espace principal homogène de groupe G_m sur X . $\square$

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

Le faisceau analytique cohérent $R^1 f_* \underline{\mathbb{R}} \otimes_{\mathbb{R}} \mathcal{O}_X$ est le faisceau de cohomologie de De Rham relative de E_X sur X , et comme tel s'insère dans une suite exacte (filtration de Hodge)

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

(car, par dualité de Serre, $\omega^{-1} \sim R^1 f_* \mathcal{O}$).

La description fonctorielle 2.2 (ii) rend évidente une action à droite du groupe $SL_2(\mathbb{Z})$ sur (X, E_X) : à $\gamma \in SL_2(\mathbb{Z})$ et à la courbe elliptique E , munie de $\alpha: \underline{\mathbb{Z}}^2 \xrightarrow{\sim} R^1 f_* \underline{\mathbb{Z}}$, on associe $(E, \alpha \circ \gamma)$. Si on regarde X , muni de

$$q: \underline{\mathbb{R}}^2 \otimes \mathcal{O}_X \sim R^1 f_* \underline{\mathbb{R}} \otimes_{\mathbb{R}} \mathcal{O}_X \rightarrow \omega^{-1}$$

comme classifiant les structures complexes sur $\mathbb{R}^2$, on met de même en évidence une action à droite du groupe $GL_2^+(\mathbb{R})$ sur $(X, \underline{\mathbb{R}}^2, \omega, q)$.

(2.3) Choisissons une base (x_1, x_2) de $\mathbb{R}^2$ telle que $x_1 \wedge x_2 > 0$. Un point $(f: \mathbb{R}^2 \rightarrow \mathbb{C}, \text{mod } \mathbb{C}^*)$ de X est repéré par $z = f(x_1)/f(x_2)$ ($\text{Im}(z) > 0$) et la flèche q s'identifie à

$$q: \mathbb{R}^2 \rightarrow G_a: ax_1 + bx_2 \mapsto az + b.$$

Ceci met en évidence une trivialisation, non équivariante, de ω^{-1} sur X . Relativement à cette trivialisation, une section $f(z)$ de ω^k sur X est transformée

par un élément $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$ de $GL^+(\mathbb{R}^2)$ (matrice dans la base (x_1, x_2)) en

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

De l'identité

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

on déduit que dz est une section de $\omega^{-2} \cdot \Omega_X^1$ invariante sous le groupe $SL_2(\mathbb{R})$.

Cette section est partout non nulle et définit un isomorphisme de $SL_2(\mathbb{R})$ -faisceaux équivariants 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 $SL_2(\mathbb{R})$. 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

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

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

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

Dans le cas particulier où $\Gamma \subset SL_2(\mathbb{Z})$, 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 des matrices

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \quad (n \in \mathbb{Z}).$$

Soit z la coordonnée (2.3) sur X définie par (x_1, x_2) . Il existe N tel que la partie $X_N = \{z \mid \text{Im}(z) > N\}$ 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 s'étend en un isomorphisme d'un voisinage de P_{Γ_0} avec le disque $0 \leq q < e^{-2\pi N}$.

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 , et d'un isomorphisme φ (2.3) entre les restrictions de ces faisceaux à X/Γ . De la formule

$$dq = de^{2\pi iz} = 2\pi ie^{2\pi iz} dz = 2\pi i q dz$$

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

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

d'où 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 $U^k \otimes_{\mathbb{R}} \mathbb{C}$

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

induit une flèche

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

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 $sh_0 = \delta.H^0(\iota^k) \oplus \bar{\delta}.H^0(\iota^k)$:

$$sh_0 : H^0(X/\Gamma, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(X/\Gamma, \Omega^1 \otimes \omega^k)} \rightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}) .$$

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

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

THÉORÈME 2.10 (Shimura [7]).- Il existe un isomorphisme sh rendant commutatif le diagramme suivant :

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

On appelle sh l'isomorphisme de Shimura.

(2.11) Dans le cas particulier où Γ est un sous-groupe d'indice fini de $SL_2(\mathbb{Z})$, la courbe elliptique E sur X/Γ provient d'un schéma en courbes elliptiques sur la courbe algébrique X/Γ (i.e., son invariant modulaire est méromorphe à l'infini) ; elle admet donc un modèle de Néron $\bar{E}$ sur $\overline{X/\Gamma}$. On peut montrer que les fibres de $\bar{E}$ en les points à l'infini sont de type multiplicatif, et que, sur $\overline{X/\Gamma}$ tout entier, on a $\omega = e^* \Omega_{\bar{E}/(X/\Gamma)}^1$.

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

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

N° 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_{et} 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 $\mathbf{A}_T^f$ -faisceau l. c. c. consiste en la donnée, pour chaque nombre premier ℓ , d'un $\mathbb{Z}_\ell$ -faisceau l. c. c. si $\ell \notin T$, d'un $\mathbb{Q}_\ell$ -faisceau l. c. c. si $\ell \in T$. Pour $T = \emptyset$, on parlera de $\hat{\mathbb{Z}}$ -faisceau l. c. c. plutôt que de $\mathbf{A}_\emptyset^f$ -faisceau l. c. c..

Pour T quelconque, la catégorie des $\mathbf{A}_T^f$ -faisceaux l. c. c. est la limite inductive des catégories de $\mathbf{A}_{T'}^f$ -faisceaux l. c. c. pour T' fini dans T . On pose :

$$\begin{aligned}\underline{\mathbb{Z}}_\ell &= \varprojlim \mathbb{Z}/(\ell^n) \quad , \quad \mathbb{Q}_\ell = \underline{\mathbb{Z}}_\ell \otimes \mathbb{Q}_\ell \quad , \\ \hat{\underline{\mathbb{Z}}} &= (\underline{\mathbb{Z}}_\ell) \quad \text{et} \quad \underline{\mathbb{A}}_T^f = \hat{\underline{\mathbb{Z}}} \otimes \underline{\mathbb{A}}_T^f .\end{aligned}$$

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 à isogénie près sous-jacente. 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 dans E , la flèche de transition de E_{ℓ^n} dans E_{ℓ^m} ($n \geq m$) étant la multiplication par ℓ^{n-m} . Procédant de même pour $\mathbb{G}_m$, on pose $T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(1)$. Si ℓ est inversible sur S , $T_\ell(E)$ et $\mathbb{Z}_\ell(1)$ sont des $\mathbb{Z}_\ell$ -faisceaux sur S . On définit $T_\infty(E)$ comme étant l'algèbre de Lie relative de E sur S (le faisceau inversible dual du faisceau inversible ω de (2.1 (a))).

Supposons S de caractéristique 0. On définit alors le $\hat{\mathbb{Z}}$ -faisceau $T_f(E)$ sur S comme étant le système des $T_\ell(E)$ et on pose $V_f(E) = T_f(E) \otimes \mathbb{A}^f$. Si $u: E \rightarrow F$ est une isogénie, 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 triples formés d'une courbe elliptique à isogénie près E sur S , d'un $\hat{\mathbb{Z}}$ -faisceau T , forme tordue de $\hat{\mathbb{Z}}^2$ et d'un isomorphisme $\beta : V_f(E) \xrightarrow{\sim} T \otimes \mathbb{A}$. Le foncteur $I : E \rightarrow (E \otimes \mathbb{Q}, T_f(E), V_f(E) \sim T_f(E) \otimes \mathbb{A})$ de $E_1(S)$ dans $E_2(S)$ est une équivalence de catégories.

La question est locale sur S , qu'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

$$(3.4) \quad 0 \rightarrow T_f(E) \rightarrow T_f(F) \rightarrow \text{Ker}(f) \rightarrow 0.$$

Le morphisme f est divisible par n si et seulement si il annule 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 on en déduit que $\text{Hom}_S(E, F)$ est le sous-groupe de $\text{Hom}_S(E \otimes \mathbb{Q}, F \otimes \mathbb{Q})$ formé des morphismes f tels que $V_f(f)$ envoie $T_f(E)$ dans $T_f(F)$. Le foncteur I est donc pleinement fidèle.

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 que $T_f(E) \subset T$.

Le quotient $K = T/T_f(E)$ est alors canoniquement isomorphe à un sous-groupe fini de E , et X est image par I de E/K (cf. 3.4). $\square$

COROLLAIRE 3.5.- Le foncteur $F_1(S)$ (resp. $F'_1(S)$) qui, à chaque schéma S de caractéristique 0 , associe l'ensemble des classes d'isomorphie de courbes elliptiques E sur S , munies d'un isomorphisme $\alpha : T_f(E) \xrightarrow{\sim} \hat{\mathbb{Z}}^2$ (resp. et d'un isomorphisme $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathbb{G}_a)$ est isomorphe au foncteur $F_2(S)$ (resp.

$F'_2(S)$) qui, à S , associe l'ensemble des classes d'isomorphie de courbes elliptiques à isogénie près F sur S , munies d'un isomorphisme

$$\beta : V_f(F) \xrightarrow{\sim} \mathbb{A}^{f2}, \text{ (resp. et d'un isomorphisme } \beta_\infty : T_\infty(F) \xrightarrow{\sim} \mathbb{G}_a \text{)}.$$

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

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

$$\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2 \text{ (resp. et de } \alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathbb{G}_S \text{), est représenté par une}$$

courbe affine M_n (resp. par une surface affine M'_n) sur $\text{Spec}(\mathbb{Z}[1/n])$. Pour

$n|m$, le morphisme de M_m dans M_n défini par

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

est fini et étale au-dessus de $\text{Spec}(\mathbb{Z}[1/m])$, et on a

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

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

(3.7) Le schéma M_∞ (resp. M'_∞) est muni d'une courbe elliptique universelle

$f_\infty : E \rightarrow M_\infty$ et d'un isomorphisme $\alpha : T_f(E) \xrightarrow{\sim} \hat{\mathbb{Z}}^2$ (resp. ainsi que d'un isomorphisme $\alpha_\infty : T_\infty(E_\infty) \xrightarrow{\sim} \mathbb{G}_a$).

D'après (3.5), le schéma M_∞ (resp. M'_∞) représente le foncteur F_2 (resp. F'_2), ce qui met en évidence une action à gauche du groupe adélique $GL_2(\mathbb{A}^f)$

sur $(M_\infty, E_\infty \otimes Q, \alpha \otimes A^{f2})$ (resp. $(M_\infty, E_\infty \otimes Q, \alpha \otimes A^{f2}, \alpha_\infty)$), donnée sur le foncteur, pour $g \in GL_2(A^f)$, par

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

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 flèches de transition étant finies. L'espace annelé localement compact Y^{an} , 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 des schémas Y_i de type fini sur $\mathbb{Q}$, les flèches de transition étant finies, on pose $Y^{an} = (Y \otimes \mathbb{C})^{an}$. Ceci s'applique à M_∞ et M'_∞ .

PROPOSITION 3.8.- On a canoniquement

$$M_\infty^{an} \sim \text{Hom}(Q^2 \otimes A, \mathbb{C} \times A^{f2})/GL_2(Q)$$

$$M_\infty^{an} \sim \mathbb{C}^* \backslash \text{Hom}(Q^2 \otimes A, \mathbb{C} \times A^{f2})/GL_2(Q),$$

soient, moins canoniquement

$$M_\infty^{an} \sim GL_2(A)/GL_2(Q)$$

$$M_\infty^{an} \sim K_\infty \backslash GL_2(A)/GL_2(Q)$$

où K_∞ est le sous-groupe compact maximal à l'infini, augmenté des homothéties réelles. Ces isomorphismes sont compatibles à l'action de $GL_2(A^f)$.

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 F , ce qui permet de définir ce dernier pour une courbe 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 entre $T_{\mathbb{Q}} \otimes \mathbb{R}$ et T_∞ .

Soit n un entier et soit K_n le noyau de l'application naturelle de $\prod GL_2(\mathbb{Z}_\ell)$ sur $GL_2(\mathbb{Z}/(n))$.

Soit G_1 le foncteur qui à S associe l'ensemble des classes d'isomorphie 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 $\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/(n))^2$. On voit comme en (3.3) que G_1 est isomorphe au foncteur G_2 qui à S associe l'ensemble des classes d'isomorphie 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 $V_f(E) \xrightarrow{\sim} \mathbb{A}^2$, donné localement sur S à la composition par un élément de K_n près. Un tel objet est déterminé par la flèche composée φ' (donnée, localement, mod K_n) qui s'en déduit :

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

on a

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

de sorte que (cf. 2.2) G_1 et G_2 soient représentés par

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

Supposons maintenant que $n \geq 3$, de sorte que $GL_2(\mathbb{Q})$ agisse librement sur l'espace précédent. L'espace analytique M_n^{an} (resp. $M_n'^{\text{an}}$) représente le foncteur analogue, en géométrie analytique, au foncteur que représente M_n (resp. M_n') car ce foncteur, soit X , est représentable et la flèche $X \rightarrow M_n^{\text{an}}$ (resp. $X \rightarrow M_n'^{\text{an}}$) induit une bijection sur les ensembles de points à valeurs dans une quelconque algèbre de rang fini sur $\mathbb{C}$.

On déduit dès lors de ce qui précède que

$$M_n^{\text{an}} \sim \mathbb{K}_n \backslash \text{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f^2}) / \text{GL}_2(\mathbb{Q}) .$$

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 $\text{Isom}(\mathbb{Q}^2 \otimes \mathbb{A}, \mathbb{C} \times \mathbb{A}^{f^2}) / \text{GL}_2(\mathbb{Q})$ s'identifie à un "réseau" L_x de $\mathbb{C} \times \mathbb{A}^{f^2}$, et la courbe correspondant à x est

$$E_x \sim \mathbb{A}^2 \backslash \mathbb{C} \times \mathbb{A}^{f^2} / L_x$$

munie de $V_f(E) \sim L_x \otimes \mathbb{A}^f \simeq \mathbb{A}^{f^2}$. De là, sort aisément la dernière assertion de (3.8). $\square$

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

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

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 $\text{GL}_2(\mathbb{A}^f)$.

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 $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ déduits par extension des scalaires des schémas M_n :

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

de sorte que le groupe de Galois de $\bar{\mathbb{Q}}$ 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 $SL_2(\mathbb{Z})$, de sorte que, désignant par w le faisceau inversible sur M_n défini par E , la théorie de Shimura (2.10) donne

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

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 $SL_2(\mathbb{Z})$, 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_∞ , j'ignore s'il existe une relation entre W_ℓ et $\varinjlim_n (H^1(M_n \otimes \bar{\mathbb{Q}}, \mathbb{Q}_\ell)) \otimes \text{Sym}^k(\mathbb{Q}_\ell^2)$.

(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 d'un quotient d'un espace par un groupe fini s'obtient en prenant les invariants de ce groupe dans la cohomologie.

Posons, pour p premier, $W^{(p)} = W^{GL_2(\mathbb{Z}_p)}$. 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 $\prod_{\ell \neq p} GL_2(\mathbb{Q}_\ell)$ de $GL_2(\mathbb{A}^f)$, car ce sous-groupe centralise $GL_2(\mathbb{Z}_p)$;
- (ii) l'algèbre de Hecke $\underline{H}(GL_2(\mathbb{Q}_p), GL_2(\mathbb{Z}_p))$, algèbre des mesures entières sur

l'espace discret $GL_2(\mathbb{Q}_p)/GL_2(\mathbb{Z}_p)$ invariante à gauche par $GL_2(\mathbb{Z}_p)$: cette sous-algèbre de l'algèbre du groupe $GL_2(\mathbb{Q}_p)$ agit sur W en respectant $W^{(p)}$. Cette algèbre agit déjà sur chacun des ${}_nW$ pour n premier à p .

L'algèbre de Hecke admet pour base les (mesures associées aux fonctions caractéristiques des) doubles classes de $GL_2(\mathbb{Z}_p)$ dans $GL_2(\mathbb{Q}_p)$, et on sait que

$$\underline{H}(GL_2(\mathbb{Q}_p), GL_2(\mathbb{Z}_p)) = \mathbb{Z}[T_p, R_p, R_p^{-1}]$$

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

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

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) , ou (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 $\text{car}(k(s)) \neq p$, un seul (le noyau de Frobenius) si $\text{car}(k(s)) = p$. $\square$

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 $\text{Spec}(\mathbb{Z}[1/p])$, chaque q_i fait de $M_{n,p}$ un revêtement étale de degré $p+1$ de M_n .

Ces morphismes q_i s'insèrent dans un diagramme commutatif

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

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

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

$$(3.17) \quad \begin{array}{ccc} E & \xrightarrow{\quad} & E \\ \downarrow & & \downarrow \\ M_n & \xrightarrow{I_p} & M_n \end{array} .$$

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 ${}_nW$ s'exprime, à l'aide de (3.16), comme la flèche composée

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

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).

Lorsque $n = 1$ ou 2 , on pose ${}_nW = W^{\mathbb{K}_n}$, de sorte que

$${}_1W = {}_nW^{\text{GL}_2(\mathbb{Z}/(n))}.$$

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

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

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

$$\Lambda^2 R^1 f_{n*} \underline{\mathbb{Z}}_{\ell} \sim R^2 f_{n*} \underline{\mathbb{Z}}_{\ell} \sim \underline{\mathbb{Z}}_{\ell}(-1),$$

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

Si $\underline{F}$ 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

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

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

$$\text{d'où} \quad \widetilde{H}^i(X, \underline{F})^\vee \sim \widetilde{H}^{2n-i}(X, \underline{\text{Hom}}(\underline{F}, \mathbb{Q}_\ell(n))) .$$

Faisant $X = \bar{M}_n$ et $\underline{F} = \text{Sym}^k(R^1 f_{n*} \mathbb{Q}_\ell)$ dans ces considérations, on définit sur ${}^k W_n^\ell$ une forme bilinéaire ${}_n(\ , \)$ 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 Peterson. Si $n|m$, et si le revêtement

$\psi : M_m \rightarrow M_n$ est de degré d , on a

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

N° 4 - La formule de congruence.

On se fixe dans ce n° des entiers $k \geq 0$ et $n \geq 3$, et des nombres premiers p et ℓ . On suppose p premier à ℓ et 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 $\text{Spec}(\mathbb{Z})$, ou, le cas échéant, dans un sous-schéma de $\text{Spec}(\mathbb{Z})$. Si Y est séparé et de type fini sur $\text{Spec}(\mathbb{Z})$, et si $\underline{F}$ est un $\mathbb{Z}_\ell$ - ou $\mathbb{Q}_\ell$ -faisceau sur Y , on désigne par $R^i a_* (Y, \underline{F})$ (resp. $R^i a_! (Y, \underline{F})$, resp. $R^{i\sim} a (Y, \underline{F})$) le $\mathbb{Z}_\ell$ - ou $\mathbb{Q}_\ell$ -faisceau sur $\text{Spec}(\mathbb{Z})$ i -ième image directe supérieure de $\underline{F}$ par a (resp.

i -ième image directe à supports propres, resp. $\text{Im}(R^i a_!(Y, \underline{F}) \rightarrow R^i a_*(Y, \underline{F}))$).

On pose, pour $m \in \mathbb{N}$, $Y[1/m] = Y \times \text{Spec}(\mathbb{Z}[1/m])$.

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

Le schéma M_n est formellement lisse, donc lisse sur $\text{Spec}(\mathbb{Z})$.

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

(a) deux courbes elliptiques sur un corps algébriquement clos de même invariant j sont isomorphes (p. ex. [8] 6.3), donc les fibres géométriques de j sont finies.

Les schémas M_n et A^1 étant lisses de même dimension relative sur $\text{Spec}(\mathbb{Z})$,

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 $\text{Isom}(S; E, F)$ des isomorphismes entre E et F est étale sur S ([8] 6.3). Dans le diagramme

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

là 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 $\text{Spec}(\mathbb{Z}[1/n])$ est un diviseur régulier, de point générique de caractéristique 0, dans un schéma régulier. Il résulte alors d'un théorème d'Abyankhar (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). $\square$

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 $R^i a_*(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$, $R^i a_!(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$ et donc $R^i \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell))$ sont des $\mathbb{Z}_\ell$ -faisceaux l. c. c. sur $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$, de formation compatible à tout changement de base.

COROLLAIRE 3.2.- Le module galoisien n^W_ℓ est la fibre en le point géométrique $\bar{Q}$ de $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$ du $\mathbb{Q}_\ell$ -faisceau l. c. c. $R^i \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*} \mathbb{Z}_\ell)) \otimes \mathbb{Q}_\ell$. Il est non ramifié en dehors de n et de ℓ . $\square$

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

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

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

soit en abrégé :

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

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

$$\Phi = \Phi_1 \sqcup \Phi_2 : M_n \otimes F_p \sqcup M_n \otimes F_p \rightarrow M_{n,p} \otimes F_p.$$

Soit Φ^h la restriction de Φ aux ouverts de M_n^h et $M_{n,p}^h$ de $M_n \otimes F_p$ et $M_{n,p} \otimes F_p$ 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 $\text{Ker}(\varphi)$ de φ est étale sur S , ou bien son dual de Cartier, isomorphe à $\text{Ker}({}^t\varphi)$, est étale sur S . La propriété " $\text{Ker}(\varphi)$ est étale" est une propriété ouverte, de sorte que, localement sur S , ou bien $\text{Ker}(\varphi)$ est purement infinitésimal, ou bien $\text{Ker}({}^t\varphi)$ 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 et plats q'_1 et q'_2 du normalisé $M'_{n,p}$ de $M_{n,p}$ dans M_n .

(iii) Le morphisme Φ se factorise par un morphisme surjectif

$$\Phi' : M_n \otimes F_p \sqcup M_n \otimes F_p \rightarrow M'_{n,p} \otimes F_p.$$

L'automorphisme σ de (3.15) échange φ et ${}^t\varphi$, de sorte qu'il suffit 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 ${}_n W_\ell$, tel qu'il est explicité en (3.18), est le tensorisé par $\mathbb{Q}_\ell$ de la fibre au point géométrique $\bar{Q}$ de $\text{Spec}(\mathbb{Z}[1/n, 1/\ell])$ de l'endomorphisme (encore désigné par T_p) de $R^1 \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*}(\underline{Z}_\ell)))$ défini par la "correspondance"

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

$$T_p = q_1'^* \varphi^* q_2'^* \quad (\text{cf. 3.18}).$$

Les endomorphismes R_p et I_p 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 , $\underline{F}$ un $\mathbb{Z}_\ell$ -faisceau sur X , $\underline{G}$ 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 :

$$\begin{array}{ccc}
 y_1^* \underline{G} & \xrightarrow{z_1} & x_1^* \underline{F} \\
 & & \\
 & & y_2^* \underline{G} \xrightarrow{z_2} x_2^* \underline{F} \\
 & & \\
 & \begin{array}{ccc} & z_1 & \xrightarrow{f} z_2 \\ & \swarrow \quad \searrow & \\ x_1 & & y_2 \\ \swarrow \quad \searrow & & \swarrow \quad \searrow \\ x & x_2 & y_1 & y \\ \swarrow \quad \searrow & & \swarrow \quad \searrow & \\ & & & \end{array}
 \end{array}$$

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

$$\begin{array}{ccccccc}
 R^{i\sim}_a(Y, \underline{G}) & \xrightarrow{y_1^*} & R^{i\sim}_a(Z_1, \underline{G}) & \xrightarrow{z_1} & R^{i\sim}_a(Z_1, \underline{F}) & \xrightarrow{x_1^*} & R^{i\sim}_a(X, \underline{F}) \\
 || & & \uparrow & & \uparrow & & || \\
 R^{i\sim}_a(Y, \underline{G}) & \xrightarrow{y_2^*} & R^{i\sim}_a(Z_2, \underline{G}) & \xrightarrow{z_2} & R^{i\sim}_a(Z_2, \underline{F}) & \xrightarrow{x_2^*} & R^{i\sim}_a(X, \underline{F})
 \end{array}$$

est commutatif.

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

$$\begin{array}{ccccc}
 R^{i\sim}_a(Z_1, x_1^* \underline{F}) & \simeq & R^{i\sim}_a(X, x_1^* x_1^* \underline{F}) & \xrightarrow{\text{Tr}} & R^{i\sim}_a(X, \underline{F}) \\
 \uparrow & & \uparrow & & || \\
 R^{i\sim}_a(Z_2, x_2^* \underline{F}) & \simeq & R^{i\sim}_a(X, x_2^* x_2^* \underline{F}) & \xrightarrow{\text{Tr}} & R^{i\sim}_a(X, \underline{F})
 \end{array}$$

et on revient à la définition de la trace pour vérifier que le carré

$$\begin{array}{ccc}
 x_1^* x_1^* \underline{F} & \xrightarrow{\text{Tr}} & \underline{F} \\
 \uparrow & & || \\
 x_2^* x_2^* \underline{F} & \xrightarrow{\text{Tr}} & \underline{F}
 \end{array}$$

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

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

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

(a)

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

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

(b)

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

La flèche x est la flèche composée $I_p^{-1} \circ F$:

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

L'endomorphisme correspondant est donc le composé de

$$\begin{aligned}
 V : R^1 \tilde{a}(M_n \otimes F_p, \text{Sym}^k(R^1 f_{n*} \underline{Z}_\ell)) &\xrightarrow{V^*} R^1 \tilde{a}(M_n \otimes F_p, \text{Sym}^k(R^1 f_{n*}^{(p)} \underline{Z}_\ell)) \\
 &\xrightarrow{\text{Tr}_F} R^1 \tilde{a}(M_n \otimes F_p, \text{Sym}^k(R^1 f_{n*} \underline{Z}_\ell))
 \end{aligned}$$

et de

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

PROPOSITION 4.8.- On a $T_p / F_p = F + I_p^* V$, et

- (i) F s'identifie à l'inverse de l'élément de Frobenius ("arithmétique") φ_p du groupe de Galois $\text{Gal}(\bar{F}_p / F_p)$ agissant sur $\tilde{H}^1(M_n \otimes \bar{F}_p, \text{Sym}^k(R^1 f_{n*} \underline{Z}_\ell))$;
- (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 :

$$\begin{array}{ccccccc}
 E & \leftarrow & E^{(p)} & \xrightarrow{F_E} & E & \xrightarrow{V_E} & E^{(p)} \rightarrow E \\
 \downarrow & & \searrow & & \downarrow & \swarrow & \downarrow \\
 M_n & \xleftarrow{F} & & & M_n & \xrightarrow{F} & M_n
 \end{array}$$

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

La flèche $F_E^* V_E^* = (F_E V_E)^* = (p \cdot 1_E)^*$ agit par multiplication par p^k sur

$\text{Sym}^k R^1 f_{n*} \underline{Z}_\ell$, de sorte que $VF = p^k \cdot \text{Tr}_F \circ F^* = p^k \cdot p = p^{k+1}$ puisque $F : M_n \rightarrow M_n$ 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

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

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 $\bar{\mathbb{Q}}$ 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_ℓ et V le transposé de F relativement au produit scalaire (3.20). Alors,

$$\begin{aligned} T_p &= F + I_p^* V, & FV &= p^{k+1} \\ \text{et} \quad 1 - T_p X + p R_p X^2 &= (1 - FX)(1 - I_p^* VX) . \quad \square \end{aligned}$$

N° 5 - Weil implique Ramanujan.

Si p est un nombre premier et X un schéma sur $\mathbb{F}_p$, on désignera par $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, par $F : X \rightarrow X$ l'endomorphisme de Frobenius ("géométrique"), et on posera $\bar{X} = X \otimes \bar{\mathbb{F}}_p$; 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 $H^i(\bar{X}, \mathbb{Q}_\ell)$ 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 $(p, n) = 1$) :

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

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 $\tilde{H}^i(\bar{X}, \mathbb{Q}_\ell)$ sont des entiers algébriques de valeur absolue $p^{i/2}$.

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

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

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

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 $\tilde{H}^i(\bar{S}, R^j f_* \mathbb{Q}_\ell)$ a pour valeurs propres des entiers algébriques de valeur absolue $p^{i+j/2}$.

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

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

L'endomorphisme de multiplication par $m : \Psi_m = m1_A$, définit des endomorphismes de E et ${}_c E$ qui s'insèrent dans un diagramme commutatif :

$$\begin{array}{ccc}
 {}_C E & \rightarrow & E \\
 \Psi_m^* \downarrow & & \Psi_m^* \downarrow \\
 {}_C E & \rightarrow & E
 \end{array}
 .$$

Sur $R^j f_{*\mathbb{Q}_\ell}$, Ψ_m^* agit par multiplication par m^j , de sorte que sur les termes ${}_C E_r^{ij}$ et E_r^{ij} de ${}_C E$ et E , Ψ_m^* est la multiplication par m^j . Les flèches d_r ($r \geq 2$) commutent à Ψ_m^* , et envoient E_r^{ij} (resp. ${}_C E_r^{ij}$) dans $E_r^{i'j'}$ (resp. ${}_C E_r^{i'j'}$) 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, $\tilde{H}^i(\bar{S}, R^j f_{*\mathbb{Q}_\ell})$ s'identifie, comme module galoisien, au sous-espace de $\tilde{H}^{i+j}(\bar{A}, \mathbb{Q}_\ell)$ où $\Psi_m^* = m^j$ et on applique (5.2). L'astuce utilisée ici est due à Lieberman. $\square$

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 -uplé 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 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 ordi-

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 (coordonnées $(X_i)_{0 \leq i \leq r}$, $(Y_i)_{0 \leq i \leq r}$, $(T_i)_{1 \leq i \leq s}$) d'équation

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

Soit 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, $m = \mathcal{O}_V$ en dehors du lieu singulier de V , et la variété $\tilde{V}$ déduite de V en éclatant 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 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 m analogue à l'idéal m de (5.5). Eclatant 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 $\prod_{i=1}^k w_i$ est le sous-

module galoisien de ${}_m W_\ell^k$ invariant par $GL_2(\mathbb{Z}/(m))$. Sur ${}_1 W_\ell^k$, 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

$$\det(1 - FX ; {}_1 W_\ell^k) = \det(1 - VX ; {}_1 W_\ell^k) .$$

L'action de T_p sur ${}_1 W_\ell^k$ est induite par son action sur ${}_1 W^k$, et est compatible à la décomposition de ${}_1 W \otimes \mathbb{C}$ en la somme de l'espace S_{k+2} des formes modulaires paraboliques relatives à $SL_2(\mathbb{Z})$, de poids $k + 2$, et de l'espace complexe conjugué. Du caractère hermitien de T_p (pour le produit scalaire de Peterson) et de (3.19), on déduit alors que

$$\det(1 - T_p X + p^{k+1} X^2 ; {}_1 W_\ell^k) = \det(1 - T_p X + p^{k+1} X^2 ; S_{k+2})^2 ,$$

et

$$\det(1 - T_p X + p^{k+1} X^2 ; S_{k+2})^2 = \det(1 - FX ; {}_1 W_\ell^k)^2$$

soit

$$(5.7) \quad \det(1 - T_p X + p^{k+1} X^2 ; S_{k+2}) = \det(1 - FX ; {}_1 W_\ell^k) .$$

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

$$H_p(X) = \det(1 - FX ; {}_1 W_\ell^{10})$$

et on applique (5.1). $\square$

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

BIBLIOGRAPHIE

- [1] J. IGUSA - Kroneckerian model of fields of elliptic modular functions, Am. J. of Math., 81 1959, p. 561-577.
- [2] Y. IHARA - Hecke polynomials as congruence zêta functions in elliptic modular case, Ann. of Math., S.2 85 1967, p. 267-295.
- [3] J.-P. JOUANLOU - Exposés V et VI de SGA 5.
- [4] M. KUGA et G. SHIMURA - On the zêta function of a fibre variety whose fibres are abelian varieties, Ann. of Math., S.2 82 1965, p. 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, n° 14.
- [7] G. SHIMURA - Sur les intégrales attachées aux formes automorphes, J. Math. Soc. of Japan, 11 1959, p. 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 : Eléments 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.