PIERRE DELIGNE

Formes modulaires et représentations ℓ-adiques

Séminaire N. Bourbaki, 1971, exp. n^{o} 355, p. 139-172

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

Séminaire BOURBAKI
21e année, 1968/69, n° 355 Février 1969

FORMES MODULAIRES ET REPRÉSENTATIONS ℓ-ADIQUES

par Pierre DELIGNE

N° 1 - Introduction.

Soient

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

et

$$\Delta(z) = D(e^{2\pi i z}) \qquad (\mathrm{Im}(z) > 0) \quad .$$

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

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

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

se prolonge en une fonction entière de s et la fonction

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

est invariante par $s \longmapsto 12 - s$.

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 $\mathbf{Q}$. Ceci suggère, en première approximation, de tenter d'interpréter la fonction 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 le groupe de Galois $\mathrm{Gal}(K_\ell/\mathbb{Q})$, 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 $\mathrm{Gal}(K_\ell/\mathbb{Q})$ 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 $SL_2(\mathbb{R})$. 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-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 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 $\mathbb{A}$ 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

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

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

- 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 $n \in \mathbb{Z}$, on désigne par $\mathcal{L}^n$ sa puissance tensorielle n-ième $\mathcal{L}^{\otimes n}$.

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

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

(a) Le faisceau inversible $\omega_E = e^*\Omega^1_{E/S}$. L'algèbre de Lie relative $\underline{\mathrm{Lie}}_S(E)$ est le faisceau inversible ω^{-1} dual de ω . On a $f_*\Omega^1_{E/S} \xrightarrow{\sim} \omega$.

(b) Le système local de $\mathbf{Z}$-modules libres de rang 2 $R^1 f_* \underline{\mathbf{Z}}$. On posera $T_{\mathbf{Z}}(E) = R^1 f_* \underline{\mathbf{Z}}^{\vee}$ et $T_{\mathbf{Q}}(E) = T_{\mathbf{Z}}(E) \otimes \mathbf{Q}$ (système local de l'homologie de E sur S).

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

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

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

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

Désignons par $\mathrm{Hom}^+(\mathbf{R}^2, \mathbf{C})$ l'ensemble des isomorphismes (de $\mathbf{R}$-vectoriel) entre $\mathbf{R}^2$ et $\mathbf{C}$ qui ne respectent pas (sic) les orientations naturelles de $\mathbf{R}^2$ et $\mathbf{C}$ (définies par $e_1 \wedge e_2 > 0$ et $1 \wedge i > 0$). Un tel homomorphisme est déterminé par sa restriction à $\mathbf{Z}^2$, et on posera

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

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

$$0 \to \underline{\mathbf{Z}}^2 \xrightarrow{\alpha} \mathbf{G}_a \to E_o \to 0 .$$

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

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

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

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

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

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

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

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 $\alpha : \underline{\mathbb{Z}}^2 \xrightarrow{\sim} R^1f_*\underline{\mathbb{Z}}$, on associe $(E,\alpha \circ \gamma)$. Si on regarde X, muni de

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

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 $(f : \mathbb{R}^2 \to \mathbb{C}$, mod $\mathbb{C}^*)$ de X est repéré par $z = f(x_1)/f(x_2)$ ($\mathrm{Im}(z) > 0$) et la flèche q s'identifie à

$$q : \mathbb{R}^2 \to \mathbb{G}_a \ : \ ax_1 + bx_2 \mapsto az + b .$$

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

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

De l'identité

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

on déduit que dz est une section de $\omega^{-2}.\Omega^1_X$ 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^1_X.

(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

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

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

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

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 $\Gamma_o \subset \Gamma$ un tel sous-groupe et choisissons une base (x_1,x_2) de $\mathbb{R}^2$ telle que, dans cette base, Γ_o se représente comme l'ensemble des matrices

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

Soit z la coordonnée (2.3) sur X définie par (x_1,x_2) . Il existe N tel que la partie $X_N = \{z | \mathrm{Im}(z) > N\}$ de X soit disjointe de ses conjuguées pour tout $\gamma \in \Gamma \setminus \Gamma_o$, de sorte que $X_N/\Gamma_o \hookrightarrow X/\Gamma$. La fonction $q = e^{2\pi i z}$ établit un isomorphisme entre X_N/Γ_o et le disque épointé $0 < q < e^{-2\pi N}$. Si P_{Γ_o} est le point de $\overline{X/\Gamma} - X/\Gamma$ associé à Γ_o , cet isomorphisme s'étend en un isomorphisme d'un voisinage de P_{Γ_o} 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_o , 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_o} , la section de ω sur X_N/Γ_o définie par la fonction 1 se prolonge en une section inversible sur $\overline{X_N/\Gamma_o}$.

(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

$$dq = de^{2\pi i z} = 2\pi i e^{2\pi i z}\, dz = 2\pi i q\, dz$$

résulte que la flèche

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

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

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

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

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

d'où une flèche, encore désignée par ι^k :

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

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 $U^k \otimes_{\mathbb{R}} \mathbb{C}$

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

induit une flèche

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

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 $H^o(X/\Gamma\ ,\ \Omega^1(U^k))$ dans $H^1(X/\Gamma\ ,\ U^k \otimes \mathbb{C})$. On obtient ainsi une flèche $sh_o = \delta . H^o(\iota^k) \oplus \bar{\delta} . H^o(\iota^k)$:

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

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

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

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 $\omega = e^*\Omega^1_{\bar{E}/(\overline{X/\Gamma})}$.

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

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

N° 3 - Opérateurs de Hecke et représentation ℓ-adique fondamentale.

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

(i) $\underline{F}_n$ est un faisceau localement constant de $\mathbf{Z}/(\ell^n)$-modules de type fini ;

(ii) si $n \leq m$, alors $\underline{F}_m \otimes \mathbf{Z}/(\ell^n) \xrightarrow{\sim} \underline{F}_n$.

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

Si S est connexe et muni d'un point géométrique s, la catégorie des $\mathbf{Z}_\ell$-faisceaux (resp. $\mathbf{Q}_\ell$-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 $\mathbf{Z}_\ell$-module de type fini (resp. un $\mathbf{Q}_\ell$-vectoriel de rang fini).

Si T est un ensemble fini de nombres premiers, un $\mathbf{A}^f_T$-faisceau l. c. c. consiste en la donnée, pour chaque nombre premier ℓ, d'un $\mathbf{Z}_\ell$-faisceau l. c. c. si $\ell \notin T$, d'un $\mathbf{Q}_\ell$-faisceau l. c. c. si $\ell \in T$. Pour $T = \emptyset$, on parlera de $\hat{\mathbf{Z}}$-faisceau l. c. c. plutôt que de $\mathbf{A}^f_\emptyset$-faisceau l. c. c..

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

$$\underline{\mathbb{Z}}_\ell = \varprojlim \mathbb{Z}/(\ell^n) \quad , \quad \underline{\mathbb{Q}}_\ell = \underline{\mathbb{Z}}_\ell \otimes \mathbb{Q}_\ell \quad ,$$
$$\hat{\underline{\mathbb{Z}}} = (\underline{\mathbb{Z}}_\ell) \quad \text{et} \quad \underline{\mathbb{A}}^f_T = \hat{\underline{\mathbb{Z}}} \otimes \mathbb{A}^f_T \ .$$

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 $f : E \to S$ 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 $u : E \to F$ 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 , $\underline{E}_1(S)$ _la catégorie des courbes elliptiques sur_ S _et_ $\underline{E}_2(S)$ _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_

$I : E \to (E \otimes \mathbb{Q}\ , T_f(E)\ , V_f(E) \sim T_f(E) \otimes \mathbb{A})$ _de_ $\underline{E}_1(S)$ _dans_ $\underline{E}_2(S)$ _est une équivalence de catégories._

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

(3.4) $$0 \to T_f(E) \to T_f(F) \to \mathrm{Ker}(f) \to 0 .$$

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 $\mathrm{Hom}_S(E,F)$ 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.

Soit $X \in \mathrm{Ob}(\underline{E}_2(S))$. 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). □

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

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 $\alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ (resp. et de $\alpha_\infty : T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$), est représenté par une courbe affine M_n (resp. par une surface affine M'_n) sur $\mathrm{Spec}(\mathbb{Z}[1/n])$. Pour $n|m$, le morphisme de M_m dans M_n défini par

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

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

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

On procède de même pour représenter F'_1 . □

(3.7) Le schéma M_∞ (resp. M'_∞) est muni d'une courbe elliptique universelle $f_\infty : E \to M_\infty$ 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 $(M_\infty , E_\infty \otimes \mathbb{Q} , \alpha \otimes \mathbb{A}^{f2})$ (resp. $(M_\infty , E_\infty \otimes \mathbb{Q} , \alpha \otimes \mathbb{A}^{f2} , \alpha_\infty)$), donnée sur le foncteur, pour $g \in GL_2(\mathbb{A}^f)$, par

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

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

$$M'^{an}_\infty \sim \mathrm{Hom}(\mathbb{Q}^2 \otimes \mathbb{A} , \mathbb{C} \times \mathbb{A}^{f2})/GL_2(\mathbb{Q})$$

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

soient, moins canoniquement

$$M'^{an}_\infty \sim GL_2(\mathbb{A})/GL_2(\mathbb{Q})$$

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

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

La notion de courbe elliptique à isogénie près, et leur sorite, s'étendent tels quels au cas analytique complexe. En outre, une isogénie $\varphi : E \to F$ 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 $u : T_{\mathbb{Q}} \to T_\infty$ 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 $f : E \to S$ sur S , munies d'un isomorphisme $\varphi : \underline{\mathbb{Q}}^2 \xrightarrow{\sim} T_{\mathbb{Q}}(E)$, 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 $V_f(E) \xrightarrow{\sim} \underline{\mathbb{A}}^2$, 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 :

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

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

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

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. $M_n'^{an}$) 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 $X \to M_n^{an}$ (resp. $X \to M_n'^{an}$) 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

$$M'^{an}_n \sim K_n \backslash \mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A} , \mathbb{C} \times \mathbb{A}^{f^2})/GL_2(\mathbb{Q}) .$$

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 $\mathrm{Isom}(\mathbb{Q}^2 \otimes \mathbb{A} , \mathbb{C} \times \mathbb{A}^{f^2})/GL_2(\mathbb{Q})$ s'identifie à un "réseau" L_x de $\mathbb{C} \times \mathbb{A}^{f^2}$, et la courbe correspondant à x est

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

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

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

DÉFINITION 3.9.- <u>On désigne par</u> W <u>(ou par</u> ${}^kW$, <u>s'il y a risque de confusion) le</u> <u>$\mathbb{Q}$-vectoriel</u>

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

Ce vectoriel ne dépend que de la courbe elliptique (à isogénie près) universelle $f_\infty : E \to M_\infty$ de sorte que, par transport de structure, il est muni d'une action à gauche du groupe adélique $GL_2(\mathbb{A}^f)$.

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) $$W_\ell = \varinjlim_n \tilde{H}^1(M_n \otimes \bar{\mathbb{Q}} , \mathrm{Sym}^k(R^1 f_{n*}(\underline{\mathbb{Q}_\ell}))) = \varinjlim {}_nW_\ell$$

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

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 ω le faisceau inversible sur M_n défini par E , la théorie de Shimura (2.10) donne

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

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 $R^1 f_* \underline{\mathbb{Q}}_\ell$ soit trivial sur M_∞ , j'ignore s'il existe une relation entre W_ℓ et $\varinjlim(\tilde{H}^1(M_n \otimes \bar{\mathbb{Q}}, \underline{\mathbb{Q}}_\ell)) \otimes \mathrm{Sym}^k(\mathbb{Q}_\ell^2)$.

(3.12) Soient $n \geq 3$ un entier et K_n comme en (3.8). On a alors $W^{K_n} = {}_nW$. 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

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

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 $GL_2(\mathbb{Q}_p)/GL_2(\mathbb{Z}_p)$ invariantes à gauche par $GL_2(\mathbb{Z}_p)$: cette sous-algèbre de l'algèbre du groupe $GL_2(\mathbb{Q}_p)$ agit sur $\mathbf{W}$ en respectant $\mathbf{W}^{(p)}$. Cette algèbre agit déjà sur chacun des ${}_n\mathbf{W}$ 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)
$$\begin{tikzcd} & \mathbb{Z}/(n)^2 & \\ E_n \arrow[ur, "\alpha"] \arrow[rr] & & F_n \arrow[ul, "\alpha'"'] \\ E \arrow[u, hook] \arrow[rr, "\varphi"] & & F \arrow[u, hook] \end{tikzcd}$$

où φ est une p-isogénie entre courbes elliptiques et α un isomorphisme. On désigne par q_1 et q_2 : $F_{n,p} \to \mathbf{M}_n$ 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 $\mathbf{M}_{n,p}$, et les morphismes q_1 , q_2 : $\mathbf{M}_{n,p} \to \mathbf{M}_n$ sont finis.

L'automorphisme σ de $F_{n,p}$ envoyant $\varphi : E \to F$ sur ${}^t\varphi : F \to E$ 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 $\mathrm{car}(k(s)) \neq p$, un seul (le noyau de Frobenius) si $\mathrm{car}(k(s)) = p$.□

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 .

Ces morphismes q_i s'insèrent dans un diagramme commutatif

(3.16)
$$\begin{tikzcd}
 & q_1^*E \arrow[rr, "\varphi"] \arrow[dl] \arrow[dr, "u"'] & & q_2^*E \arrow[dl, "v"] \arrow[dr] & \\
E \arrow[dr, "f_n"'] & & M_{n,p} \arrow[dl, "q_1"] \arrow[dr, "q_2"'] & & E \arrow[dl, "f_n"] \\
 & M_n & & M_n &
\end{tikzcd}$$

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 : $(E,\alpha) \mapsto (E,\alpha/p)$:

$$I_p^*(E,\alpha) = (E,\alpha/p)$$

(3.17)
$$\begin{tikzcd}
E \arrow[r] \arrow[d] & E \arrow[d] \\
M_n \arrow[r, "I_p"'] & M_n
\end{tikzcd} .$$

I_p^* est un automorphisme de $\tilde{H}^i(M_n^{an} , \mathrm{Sym}^k(R^1 f_{n*} \underline{\mathbb{Z}}))$.

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

$$\tilde{H}^1(M_n^{an}, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}})) \xrightarrow{q_2^*} \tilde{H}^1(M_{n,p}^{an}, \mathrm{Sym}^k(R^1 v_*\underline{\mathbb{Q}}))$$

$$\xrightarrow{\varphi^*} \tilde{H}^1(M_n^{an}, \mathrm{Sym}^k(R^1 u_*\underline{\mathbb{Q}})) \xrightarrow[q_{1*}]{} \tilde{H}^1(M_n^{an}, \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}}))$$

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 ${}_nW = W^{K_n}$, de sorte que

$${}_1W = {}_nW^{GL_2(\mathbb{Z}/(n))} .$$

Si S_{k+2} désigne l'espace des formes modulaires paraboliques, pour le groupe $SL_2(\mathbb{Z})$, de poids $k+2$, l'isomorphisme de Shimura (3.11) induit un isomorphisme

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

Il est pénible, mais routinier, de démontrer que

PROPOSITION 3.19.- L'endomorphisme T_p de ${}_1^kW_\infty$ 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 $\mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell)$ 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

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

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

d'où

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

Faisant $X = \bar{M}_n$ et $\underline{F} = \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Q}}_\ell)$ dans ces considérations, on définit sur ${}^k_nW_\ell$ 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 $\psi : M_m \to M_n$ est de degré d, on a

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

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 $f_n : E \to M_n$ 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 $\underline{F}$ 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. $R^i\tilde{a}(Y,\underline{F})$) le $\mathbb{Z}_\ell$- ou $\mathbb{Q}_\ell$-faisceau sur $\mathrm{Spec}(\mathbb{Z})$ i-ième image directe supérieure de $\underline{F}$ par a (resp.

i-ième image directe à supports propres, resp. $\mathrm{Im}(R^i a_!(Y,\underline{F}) \to R^i a_*(Y,\underline{F}))$).
On pose, pour $m \in \mathbf{N}$, $Y[1/m] = Y \times \mathrm{Spec}(\mathbf{Z}[1/m])$.

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

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

L'invariant modulaire j de la courbe universelle sur M_n est un morphisme de M_n dans la droite affine A^1 sur $\mathrm{Spec}(\mathbf{Z}[1/n])$. 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 $\mathrm{Spec}(\mathbf{Z})$, 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 $\underline{\mathrm{Isom}}(S;E,F)$ des isomorphismes entre E et F est étale sur S ([8] 6.3). Dans le diagramme

$$\begin{tikzcd}
\underline{\mathrm{Isom}}(M_n \times_{A^1} M_n \,;\, pr_1^*E \,,\, pr_2^*E) \arrow[r, phantom, "\sim"] \arrow[d, "u"] & M_n \times GL_2(\mathbf{Z}/(n)) \arrow[d, "v"] \\
M_n \times_{A^1} M_n \arrow[r, "pr_1"] & M_n
\end{tikzcd} ,$$

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 $\mathrm{Spec}(\mathbb{Z}[1/n])$ est un diviseur régulier, de point générique de caractéristique 0 , dans un schéma régulier. Il résulte alors d'un théorème d'Abyankhar (voir [5]) que, le long de ce diviseur $j = \infty$, $\mathbb{M}_n$ est modérément ramifié sur $\mathbb{P}^1$, et que le normalisé $\mathbb{M}_n^*$ de $\mathbb{P}^1$ dans $\mathbb{M}_n$ vérifie (4.1).□

Du même théorème résulte que les $\mathbb{Z}_\ell$-faisceaux l. c. c. $R^i f_{n*}\underline{\mathbb{Z}}_\ell$ sur $\mathbb{M}_n[1/\ell]$ 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 $R^i a_*(\mathbb{M}_n\ , \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell))$, $R^i a_!(\mathbb{M}_n\ , \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell))$ et donc $R^i \tilde{a}(\mathbb{M}_n\ , \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell))$ 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 3.2.- <u>Le module galoisien</u> ${}_nW_\ell$ <u>est la fibre en le point géométrique</u> $\bar{\mathbb{Q}}$ <u>de</u> $\mathrm{Spec}(\mathbb{Z}[1/n\ , 1/\ell])$ <u>du</u> $\mathbb{Q}_\ell$<u>-faisceau l. c. c.</u> $R^i \tilde{a}(\mathbb{M}_n\ , \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell)) \otimes \mathbb{Q}_\ell$. <u>Il est non ramifié en dehors de</u> n <u>et de</u> ℓ . □

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

$$\begin{tikzcd}
 & \mathbb{Z}/(n)^2 & \\
E_n \arrow[ur, "\alpha"] \arrow[rr] \arrow[d, hook] & & E_n^{(p)} \arrow[ul, "\alpha^{(p)}"'] \arrow[d, hook] \\
E \arrow[rr, "F"] & & E^{(p)}
\end{tikzcd}
\qquad \text{et} \qquad
\begin{tikzcd}
 & \mathbb{Z}/(n)^2 & \\
E_n^{(p)} \arrow[ur, "p\cdot\alpha^{(p)}"] \arrow[rr] \arrow[d, hook] & & E_n \arrow[ul, "\alpha"'] \arrow[d, hook] \\
E^{(p)} \arrow[rr, "V"] & & E
\end{tikzcd}$$

soit en abrégé :

$F : (E,\alpha) \to (E^{(p)},\alpha^{(p)})$ et $V : (E^{(p)},p\alpha^{(p)}) \to (E,\alpha)$, où F est le morphisme de Frobenius et V, son transposé, le "Verschiebung". Ces diagrammes définissent des morphismes Φ_1 et Φ_2 de $\mathcal{M}_n \otimes \mathbf{F}_p$ dans $\mathcal{M}_{n,p}$. Ces morphismes sont finis, en tant que section de q_1 ou q_2, et définissent un morphisme

$$\Phi = \Phi_1 \amalg \Phi_2 : \mathcal{M}_n \otimes \mathbf{F}_p \amalg \mathcal{M}_n \otimes \mathbf{F}_p \to \mathcal{M}_{n,p} \otimes \mathbf{F}_p .$$

Soit Φ^h la restriction de Φ aux ouverts de $\mathcal{M}_n^h$ et $\mathcal{M}_{n,p}^h$ de $\mathcal{M}_n \otimes \mathbf{F}_p$ et $\mathcal{M}_{n,p} \otimes \mathbf{F}_p$ correspondant aux courbes d'invariant de Hasse h non nul.

PROPOSITION 4.3.- Φ^h <u>est un isomorphisme</u>.

Soit $\varphi : E_1 \to E_2$ 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 $\mathrm{Ker}(\varphi)$ de φ est étale sur S, ou bien son dual de Cartier, isomorphe à $\mathrm{Ker}({}^t\varphi)$, est étale sur S. La propriété " $\mathrm{Ker}(\varphi)$ est étale" est une propriété ouverte, de sorte que, localement sur S, ou bien $\mathrm{Ker}(\varphi)$ est purement infinitésimal, ou bien $\mathrm{Ker}({}^t\varphi)$ 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 $F : E_1 \to E_1^{(p)}$ et dans le second, ${}^t\varphi$ est isomorphe à $F : E_2 \to E_2^{(p)}$ donc φ à $V : E_2^{(p)} \to E_2$. $\square$

PROPOSITION 4.4.- (i) <u>Le schéma</u> $\mathcal{M}_{n,p}$ <u>est lisse sur</u> $\mathrm{Spec}(\mathbf{Z})$ <u>en dehors des points de caractéristique</u> p <u>où</u> $h = 0$.

(ii) <u>Les morphismes</u> q_1 <u>et</u> q_2 <u>induisent des morphismes finis et plats</u> q_1' <u>et</u> q_2' <u>du normalisé</u> $\mathcal{M}_{n,p}'$ <u>de</u> $\mathcal{M}_{n,p}$ <u>dans</u> $\mathcal{M}_n$.

(iii) <u>Le morphisme</u> Φ <u>se factorise par un morphisme surjectif</u>

$$\Phi' : \mathcal{M}_n \otimes \mathbf{F}_p \amalg \mathcal{M}_n \otimes \mathbf{F}_p \to \mathcal{M}_{n,p}' \otimes \mathbf{F}_p .$$

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) $q_i : M_{n,p} \to M_n$ 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 $q_i : M'_{n,p} \to M_n$ est plat. Enfin, (iii) résulte de ce que Φ est fini et $M_n \otimes \mathbf{F}_p$ une courbe normale. □

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

(4.5)
$$\begin{tikzcd}[column sep=small]
 & q_1'^*E \arrow[rr, "\varphi"] \arrow[dl] \arrow[dr, "u"] & & q_2'^*E \arrow[dl, "v"'] \arrow[dr] & \\
E \arrow[dr, "f_n"'] & & M'_{n,p} \arrow[dl, "q_1'"] \arrow[dr, "q_2'"'] & & E \arrow[dl, "f_n"] \\
 & M_n & & M_n &
\end{tikzcd}$$

$$T_p = q'_{1*}\varphi^* q_2'^* \quad \text{(cf. 3.18).}$$

Les endomorphismes R_p et I_p s'interprètent de même.

LEMME 4.6.- <u>Soient sur un schéma noethérien</u> S <u>quatre schémas séparés de type fini</u> X , Y , Z_1 , Z_2 , $\underline{F}$ <u>un</u> $\mathbf{Z}_\ell$<u>-faisceau sur</u> X , $\underline{G}$ <u>un</u> $\mathbf{Z}_\ell$<u>-faisceau sur</u> Y <u>et désignons par</u> a <u>chacune des flèches structurelles de</u> X , Y , Z_1 <u>ou</u> Z_2 <u>dans</u> S .

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

$$y_1^*\underline{G} \xrightarrow{z_1} x_1^*\underline{F} \qquad\qquad y_2^*\underline{G} \xrightarrow{z_2} x_2^*\underline{F}$$

$$\begin{tikzcd}
& Z_1 \arrow[r, "f"] \arrow[dl, "x_1"'] \arrow[drr, "y_1"] & Z_2 \arrow[dll, "x_2"'] \arrow[dr, "y_2"] & \\
X & & & Y
\end{tikzcd}$$

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

$$\begin{tikzcd}
R^i\tilde{a}(Y,\underline{G}) \arrow[r, "y_1^*"] \arrow[d, equal] & R^i\tilde{a}(Z_1,\underline{G}) \arrow[r, "z_1"] & R^i\tilde{a}(Z_1,\underline{F}) \arrow[r, "x_{1*}"] & R^i\tilde{a}(X,\underline{F}) \arrow[d, equal] \\
R^i\tilde{a}(Y,\underline{G}) \arrow[r, "y_2^*"] & R^i\tilde{a}(Z_2,\underline{G}) \arrow[r, "z_2"] \arrow[u] & R^i\tilde{a}(Z_2,\underline{F}) \arrow[r, "x_{2*}"] \arrow[u] & R^i\tilde{a}(X,\underline{F})
\end{tikzcd}$$

est commutatif.

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

$$\begin{tikzcd}
R^i\tilde{a}(Z_1,x_1^*\underline{F}) & R^i\tilde{a}(X,x_{1*}x_1^*\underline{F}) \arrow[l, "\simeq"'] \arrow[r, "\mathrm{Tr}"] & R^i\tilde{a}(X,\underline{F}) \arrow[d, equal] \\
R^i\tilde{a}(Z_2,x_2^*\underline{F}) \arrow[u] & R^i\tilde{a}(X,x_{2*}x_2^*\underline{F}) \arrow[l, "\simeq"'] \arrow[r, "\mathrm{Tr}"] \arrow[u] & R^i\tilde{a}(X,\underline{F})
\end{tikzcd}$$

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

$$\begin{tikzcd}
x_{1*}x_1^*\underline{F} \arrow[r, "\mathrm{Tr}"] & \underline{F} \arrow[d, equal] \\
x_{2*}x_2^*\underline{F} \arrow[r, "\mathrm{Tr}"] \arrow[u] & \underline{F}
\end{tikzcd}$$

est commutatif. □

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

$$R^1\tilde{a}(\mathbf{M}_n\ ,\ \mathrm{Sym}^k\ R^1 f_{n*}\underline{\mathbb{Z}}_\ell)\,|\,\mathrm{Spec}(\mathbb{F}_p)\ \xrightarrow{\sim}\ R^1\tilde{a}(\mathbf{M}_n\otimes\mathbb{F}_p\ ,\ \mathrm{Sym}^k\ R^1 f_{n*}\underline{\mathbb{Z}}_\ell)\quad ;$$

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

$$\begin{tikzcd}
& \mathbf{M}_n\otimes\mathbb{F}_p \amalg \mathbf{M}_n\otimes\mathbb{F}_p \arrow[r, "\Phi'"] \arrow[dl] \arrow[drr] & \mathbf{M}'_{n,p}\otimes\mathbb{F}_p \arrow[dll, "q'_1"'] \arrow[dr, "q'_2"] & \\
\mathbf{M}_n\otimes\mathbb{F}_p & & & \mathbf{M}_n\otimes\mathbb{F}_p\ ,
\end{tikzcd}$$

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

(a)

$$\begin{tikzcd}
& (E,\alpha) \arrow[r, mapsto] \arrow[dl, equal] \arrow[dr] & (E^{(p)},\alpha^{(p)}) = F^*(E,\alpha) \arrow[d] \arrow[drr] & & \\
(E,\alpha) \arrow[d] & & \mathbf{M}_n\otimes\mathbb{F}_p \arrow[dll, equal] \arrow[dr, "F"] & & (E,\alpha) \arrow[dl] \\
\mathbf{M}_n\otimes\mathbb{F}_p & & & \mathbf{M}_n\otimes\mathbb{F}_p &
\end{tikzcd}$$

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

(b)

$$\begin{tikzcd}
& x^*(E,\alpha) = (E^{(p)},p\alpha^{(p)}) \arrow[r, "V"] \arrow[dl] \arrow[d, "f_n^{(p)}"'] & (E,\alpha) \arrow[dl, "f_n"] \arrow[dr, equal] & \\
(E,\alpha) \arrow[d] & \mathbf{M}_n\otimes\mathbb{F}_p \arrow[dl, "x"] \arrow[dr, equal] & & (E,\alpha) \arrow[dl] \\
\mathbf{M}_n\otimes\mathbb{F}_p & & \mathbf{M}_n\otimes\mathbb{F}_p &
\end{tikzcd}$$

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

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

L'endomorphisme correspondant est donc le composé de

$$V : R^1\widetilde{a}(\mathbb{M}_n \otimes \mathbb{F}_p\ ,\ \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell)) \xrightarrow{V^*} R^1\widetilde{a}(\mathbb{M}_n \otimes \mathbb{F}_p\ ,\ \mathrm{Sym}^k(R^1 f^{(p)}_{n*}\underline{\mathbb{Z}}_\ell))$$
$$\xrightarrow{\mathrm{Tr}_F} R^1\widetilde{a}(\mathbb{M}_n \otimes \mathbb{F}_p\ ,\ \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell)$$

et de

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

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 $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ agissant sur $\widetilde{H}^1(\mathbb{M}_n \otimes \bar{\mathbb{F}}_p\ ,\ \mathrm{Sym}^k(R^1 f_{n*}\underline{\mathbb{Z}}_\ell))$;

(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 :

$$\begin{tikzcd} E \arrow[d] & E^{(p)} \arrow[l] \arrow[r, "F_E"] \arrow[dr] & E \arrow[r, "V_E"] \arrow[d] & E^{(p)} \arrow[r] \arrow[dl] & E \arrow[d] \\ \mathbb{M}_n & & \mathbb{M}_n \arrow[ll, "F"'] \arrow[rr, "F"] & & \mathbb{M}_n \end{tikzcd}$$

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

La flèche $F_E^* V_E^* = (F_E V_E)^* = (p.1_E)^*$ agit par multiplication par p^k sur $\mathrm{Sym}^k R^1 f_{n*}\underline{\mathbb{Z}}_\ell$, de sorte que $VF = p^k.\mathrm{Tr}_F \circ F^* = p^k.p = p^{k+1}$ puisque $F : \mathbb{M}_n \to \mathbb{M}_n$ 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

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

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* $\mathrm{Gal}(K_{n\ell}/\mathbb{Q})$, F *l'endomorphisme* φ_p^{-1} *de* ${}_nW_\ell$ *et* V *le transposé de* F *relativement au produit scalaire* (3.20). *Alors,*

$$T_p = F + I_p^* V \quad , \qquad FV = p^{k+1}$$

et

$$1 - T_p X + pR_p X^2 = (1 - FX)(1 - I_p^* VX) . \square$$

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 $F : X \to X$ 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 $(p,n) = 1$) :

THÉORÈME 5.1.- Si les conjectures de Weil sont vraies, alors les valeurs propres de l'endomorphisme F de ${}^{k}_{n}W_{\ell}$ 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 $\widetilde{H}^i(\bar{X},\mathbb{Q}_{\ell})$ sont des entiers algébriques de valeur absolue $p^{i/2}$.

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

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

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

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 $\widetilde{H}^i(\bar{S},R^jf_*\underline{\mathbb{Q}}_{\ell})$ 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

$$E \ : \ E_2^{ij} = H^i(\bar{S},R^jf_*\underline{\mathbb{Q}}_{\ell}) \Rightarrow H^{i+j}(\bar{A},\mathbb{Q}_{\ell})$$

$$_cE \ : \ {}_cE_2^{ij} = H^i_c(\bar{S},R^jf_*\underline{\mathbb{Q}}_{\ell}) \Rightarrow H^{i+j}_c(\bar{A},\underline{\mathbb{Q}}_{\ell}) \ .$$

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

$$\begin{array}{ccc} {}_cE & \to & E \\ \psi_m^* \downarrow & & \psi_m^* \downarrow \\ {}_cE & \to & E \end{array} .$$

Sur $R^jf_*\mathbb{Q}_\ell$, ψ_m^* agit par multiplication par m^j , de sorte que sur les termes ${}_cE_r^{ij}$ et E_r^{ij} de ${}_cE$ 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. ${}_cE_r^{ij}$) dans $E_r^{i'j'}$ (resp. ${}_cE_r^{i'j'}$) avec $j \neq j'$. Elles sont donc nulles, et E_2^{ij} (resp. ${}_cE_2^{ij}$) 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, $\tilde{H}^i(\bar{S},R^jf_*\mathbb{Q}_\ell)$ 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. □

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

$$X_oY_o = X_1Y_1 = \dots = X_rY_r .$$

Soit m l'idéal de $\mathcal{O}_V$ engendré par les monômes qui se déduisent du monôme $\prod_{i=o}^{r} X_i^i$ 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 $\widetilde{V}$ 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 $\widetilde{V}$ défini par l'élément $\prod_1^r X_i^i$ de l'idéal à éclater m est le spectre de l'anneau régulier

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

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

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^*. □

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 ${}_1^kW_\ell$ 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

$$\det(1 - FX ; {}^k_1 W_\ell) = \det(1 - VX ; {}^k_1 W_\ell) .$$

L'action de T_p sur ${}^k_1 W_\ell$ est induite par son action sur ${}^k_1 W$, et est compatible à la décomposition de ${}^k_1 W \otimes \mathbb{C}$ 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

$$\det(1 - T_p X + p^{k+1} X^2 ; {}^k_1 W_\ell) = \det(1 - T_p X + p^{k+1} X^2 ; S_{k+2})^2 ,$$

et

$$\det(1 - T_p X + p^{k+1} X^2 ; S_{k+2})^2 = \det(1 - FX ; {}^k_1 W_\ell)^2$$

soit

$$\det(1 - T_p X + p^{k+1} X^2 ; S_{k+2}) = \det(1 - FX ; {}^k_1 W_\ell) . \tag{5.7}$$

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

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

et on applique (5.1). □

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. JOUANOLOU - 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, Sém. 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), Sém. 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.