SÉMINAIRE N. BOURBAKI

ARMAND BOREL

Opérateurs de Hecke et fonctions zêta

Séminaire N. Bourbaki, 1966, exp. n° 307, p. 441-463

<http://www.numdam.org/item?id=SB_1964-1966__9__441_0>

Séminaire BOURBAKI
18e année, 1965/66, n°307

Juin 1966

OPÉRATEURS DE HECKE ET FONCTIONS ZÊTA

par Armand BOREL

Soit Γ un groupe d'automorphismes proprement discontinu du demi-plan de Poincaré H. Les travaux dont il est question dans cet exposé ont pour but d'exprimer, pour certains groupes arithmétiques Γ, la fonction zêta globale $Z(s; C/k)$ d'un modèle convenable C sur un corps de nombres k du quotient H/Γ (ou de certaines variétés fibrées sur H/Γ) à l'aide de séries de Dirichlet attachées à des opérateurs de Hecke agissant sur des espaces de formes automorphes. De ce rapprochement on déduit notamment des renseignements, d'une part sur la nature de $Z(s; C/k)$, et d'autre part sur les valeurs propres d'opérateurs de Hecke. En particulier, cela démontre (ou ramène aux conjectures de Weil) des analogues de la conjecture de Ramanujan-Petersson.

Ces résultats ont été tout d'abord obtenus par Eichler [1] pour certains sous-groupes de congruence de $\mathbf{SL}(2,\mathbf{Z})$ puis, dans des cas de généralité croissante, par Shimura [7,11] et Kuga-Shimura [6]. Cependant, la conjecture de Ramanujan proprement dite, qui est en somme à l'origine de ces recherches n'a pu jusqu'à présent être insérée dans ce cadre, (sinon heuristiquement).

Cet exposé est consacré principalement au cas le plus simple considéré dans [11]. Le dernier paragraphe donne quelques indications sur les cas plus généraux de [11, 6].

§ 1. Corps de quaternions. Anneau de Hecke.

1.1. L désignera toujours un corps de quaternions sur $\mathbf{Q}$, indéfini sur $\mathbf{R}$. Il existe donc deux entiers $q,d > 0$ tels que L puisse se représenter comme

l'ensemble des matrices

$$a = \begin{pmatrix} x & y \\ -q.\bar{y} & \bar{x} \end{pmatrix}, \qquad (x,y \in K = \mathbb{Q}(\sqrt{d})),$$

où $x \mapsto \bar{x}$ est l'automorphisme $u + v\sqrt{d} \mapsto u - v\sqrt{d}$, $(u,v \in \mathbb{Q})$, de K. L'involution fondamentale $a \mapsto a'$ de L est induite par l'involution

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \qquad (\alpha,\beta,\gamma,\delta \in \mathbb{R}),$$

de $M(2,\mathbb{R})$. La trace $tr(x)$ et la norme $n(x)$ de $x \in L$ sont données par

$$tr(x) = x + x', \qquad n(x) = x.x' = \det x,$$

et $n(x) \neq 0$ si $x \neq 0$.

Un ordre de L est un sous-anneau qui est un $\mathbb{Z}$-module de type fini contenant une $\mathbb{Q}$-base de L (et 1). Les éléments x d'un ordre sont entiers (i.e. $n(x)$, $tr(x) \in \mathbb{Z}$). On fixe une fois pour toutes un ordre maximal, qui sera noté $\underline{o}$. Par idéal, on entendra ici, sauf mention expresse du contraire, "$\underline{o}$-idéal entier à gauche" (sous-$\mathbb{Z}$-module de type fini de $\underline{o}$, stable par multiplication à gauche par $\underline{o}$). Ces idéaux sont toujours principaux (Eichler). La norme d'un idéal $\underline{o}.a$ est égale à $|n(a)|$.

Il existe un nombre fini ≥ 1 de nombres premiers p, dont le produit sera noté $d(L)$, tels que $L_p = L \otimes \mathbb{Q}_p$ est une algèbre à division si et seulement si $p \mid d(L)$. Si $p \nmid d(L)$, il existe un isomorphisme de L_p sur $M(2,\mathbb{Q}_p)$ qui applique $\underline{o}$ sur $M(2,\mathbb{Z}_p)$ et induit un isomorphisme de $\underline{o}/p.\underline{o}$ sur $M(2,\mathbb{Z}/p.\mathbb{Z})$.

1.2. Soient

$$\Gamma = \{a \in \underline{o},\ \det a = 1\}, \qquad \Delta = \{a \in \underline{o},\ \det a > 0\}.$$

Pour tout $a \in \Delta$, les groupes $a.\Gamma.a^{-1}$ et Γ sont commensurables (i.e. leur inter-

section est d'indice fini dans chacun d'eux). On notera $R(\Gamma,\Delta)$ ou R l'anneau de Hecke associé à Γ et Δ. C'est le groupe abélien libre sur les doubles classes $\Gamma.a.\Gamma$ $(a\in\Delta)$ muni d'un produit défini par la règle suivante : soient $u = \Gamma.a.\Gamma$, $v = \Gamma.b.\Gamma$ deux doubles classes, et $u = \cup\, \Gamma.a_i$, $v = \cup\, \Gamma.b_j$ des décompositions de u et v en classes à droite disjointes. Pour $c\in\Delta$, soit $d(u,v;c)$ le nombre de paires (i,j) telles que $a_i.b_j \subset \Gamma.c$. Alors

$$(\Gamma.a.\Gamma).(\Gamma.b.\Gamma) = \Sigma\, d(u,v;c)\ \Gamma.c.\Gamma\ ,$$

la somme étant étendue aux doubles classes $\Gamma.c.\Gamma \subset \Gamma.a.\Gamma.b.\Gamma$. On montre que R est un anneau associatif, et commutatif, car $\Gamma.a.\Gamma = \Gamma.a'.\Gamma$ pour tout $a\in\Delta$ ([11], p.281).

[Soit M le $\mathbb{Z}$-module libre engendré par les éléments de $\Gamma\backslash\Delta$. Associons à u un endomorphisme s_u de M défini par $s_u(\Gamma.c) = \Sigma\, \Gamma a_i.c$. Alors le produit précédent est défini de manière à ce que l'on ait $s_u.s_v = s_{u,v}$.]

1.3. Pour tout entier $n \geqslant 1$ on note $T(n)$ la somme des doubles classes $\Gamma.a.\Gamma$ $(a\in\Delta,\ \det a = n)$, (somme qui est finie, et se réduit à un terme si n est premier). Les opérateurs $T(n)$ ont des propriétés formelles analogues à celles des opérateurs de Hecke dans le cas classique $(\Gamma = SL(2,\mathbb{Z}))$ dont on déduit que la série de Dirichlet formelle à coefficients dans R,

$$D(s) = \Sigma\, (\Gamma.a.\Gamma).(\det a)^{-s} = \sum_{n\geqslant 1} T(n).n^{-s}\ ,$$

admet une décomposition en produit eulérien

$$D(s) = \prod_{p\ \text{premier}} H(p^{-s};p)^{-1}$$

avec

$$H(u;p) = 1 - T(p).u \qquad (p\,|\,d(L)),$$

$$H(u;p) = 1 - T(p).u + p.T(p,p).u^2 \qquad (p\nmid d(L);T(p,p) = \Gamma.p.\Gamma)\ .$$

1.4. On note $d(\Gamma.a.\Gamma)$ le nombre de classes à droite $\Gamma.b$ contenues dans $\Gamma.a.\Gamma$, (qui est ici égal au nombre de classes à gauche dans $\Gamma.a.\Gamma$, vu $\Gamma.a^{-1}.\Gamma = \Gamma.a.\Gamma$). Soit $\Gamma(a) = a^{-1}.\Gamma.a \cap \Gamma$. On voit immédiatement que

$$(1) \qquad \Gamma = \cup\, \Gamma(a).c_i \Rightarrow \Gamma.a.\Gamma = \cup\, \Gamma.a.c_i \ ,$$

les deux unions étant simultanément disjointes ou non. En particulier $d(\Gamma.a.\Gamma) = [\Gamma : \Gamma(a)]$. On a $d(T(p,p)) = 1$ et, si $p \nmid d(L)$, $d(T(p)) = p+1$. Notons encore que les classes à droite contenues dans $T(p)$ sont les intersections de $T(p)$ avec les idéaux de norme p.

§ 2. Formes automorphes. Opérateurs de Hecke.

Le groupe $G = \{g \in \mathbb{GL}(2,\mathbb{R}),\ \det g > 0\}$ opère à la manière usuelle sur H, l'automorphisme associé à $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ étant $z \mapsto (az + b).(cz + d)^{-1}$. On pose $j(g,z) = cz + d$. Le groupe discret Γ opère proprement, et H/Γ est compact. Soit $S_k(\Gamma)$, ou S_k l'espace des formes automorphes pour Γ de poids k. Ses éléments sont les fonctions holomorphes sur H vérifiant

$$f(\gamma.z) = j(\gamma,z)^k.f(z) \qquad (\gamma \in \Gamma;\ z \in H) \ .$$

A une double classe $\Gamma.a.\Gamma = \cup\, \Gamma.a_i$ $(a \in \Delta)$ on associe un endomorphisme $(\Gamma.a.\Gamma)_k$ de S_k défini par

$$(f|(\Gamma.a.\Gamma)_k(z) = (\det a)^{k-1} \Sigma_i\ f(a_i.z).j(a_i,z)^{-k} .$$

On voit facilement que le membre de droite ne dépend que de f et de $\Gamma.a.\Gamma$, et que l'on obtient ainsi une représentation de $R(\Gamma,\Delta)$ dans $S_k(\Gamma)$. Les opérateurs $(\Gamma.a.\Gamma)_k$ sont des opérateurs de Hecke. Ils sont self-adjoints par rapport à la métrique de Petersson, donc simultanément diagonalisables, à valeurs propres réelles. Une majoration aisée [6, p.491] fait voir que la série de Dirichlet, à valeurs dans $\mathrm{End}(S_k(\Gamma))$:

$$(1) \qquad D(s,k) = \Sigma(\Gamma.a.\Gamma)_k(\det a)^{-s} = \Sigma\, T(n)_k\, n^{-s} = \prod_p H(p^{-s};p,k)^{-1},$$

où

$$H(u;p,k) = 1 - T(p)_k \qquad \text{si } p \mid d(L)$$

$$H(u;p,k) = 1 - T(p)_k.u + p.T(p,p)_k.u^2 \qquad \text{si } p \nmid d(L)$$

converge pour $Rs > (k/2) + 1$. Shimura [11, 1.6] a montré que $D(s,k)$ se prolonge analytiquement en une fonction entière, avec équation fonctionnelle reliant $D(s,k)$ et $D(k-s,k)$. Comme $-1 \in \Gamma$, on a $S_k(\Gamma) = 0$ si k est impair. Si k est pair, les opérateurs de Hecke laissent invariant un réseau de S_k, donc leurs valeurs propres sont des entiers algébriques [12, Prop.9.1 ; 17, 5.2.5].

§ 3. Résultats.

3.1. Soient X une variété projective irréductible sur le corps $\mathbb{F}_p$ à p éléments (p premier) et $Z = Z(u;X)$ la fonction zêta de X sur $\mathbb{F}_p$. On a donc

$$(1) \qquad \frac{d}{du}(\log Z) = \sum_{m \geq 1} N_m.u^{m-1}\ , \quad Z(0) = 1\ ,$$

où N_m désigne le nombre de points de X rationnels sur l'extension de degré m de $\mathbb{F}_p$. On sait (Dwork) que Z est une fonction rationnelle de u. Si X est une courbe lisse, alors

$$(2) \qquad Z(u;X) = (1-u)^{-1}.(1-p.u)^{-1}.\det(1-M_\ell(\pi).u)\ ,$$

où $M_\ell(\pi)$ est une représentation ℓ-adique (ℓ premier, $\ell \neq p$) de l'endomorphisme de Frobenius de la jacobienne $J(X)$ de X, et les valeurs propres de $M_\ell(\pi)$ sont des entiers algébriques de valeur absolue $p^{\frac{1}{2}}$ [18]. Si X est lisse de dimension n, alors [2] :

$$(3) \qquad Z(u;X) = \prod_{0 \leqslant i \leqslant 2n} F_i(u)^{(-1)^{i+1}} ,$$

où F_i est un polynôme dont on espère (conjectures de Weil) que les racines sont des entiers algébriques de valeur absolue $p^{-i/2}$. On a en particulier

$$F_o = 1 - u, \; F_{2n} = 1 - p^n.u \quad .$$

3.2. Soit maintenant $X \subset P(n,\mathbb{C})$ une variété projective irréductible lisse sur $\mathbb{Q}$. Le plongement projectif définit une structure sur $\mathbb{Z}$, donc, pour tout nombre premier, un cycle $p(X)$ sur $\mathbb{F}_p$, la réduction mod p de X. Pour presque tout p, (les "bons" p), $p(X)$ est une variété irréductible lisse, avec multiplicité un. La fonction zêta globale de X sur $\mathbb{Q}$ est, par définition pour certains, au produit par une fonction rationnelle de s près pour d'autres, le produit

$$(1) \qquad Z(s;X/\mathbb{Q}) = \prod_p Z(p^{-s};p(X)) ,$$

étendu aux bons p. Il converge pour Rs assez grand et, suivant Hasse-Weil, on conjecture qu'il se prolonge en une fonction méromorphe sur le plan complexe.

3.3. THÉORÈME. *On reprend les notations des §§ 1, 2. Il existe un modèle projectif lisse sur $\mathbb{Q}$, C de H/Γ tel que l'on ait*

$$(i) \qquad Z(u;p(C)) = (1-u)^{-1}.(1-p.u)^{-1}.\det M(u;p,2)$$

pour presque tout nombre premier p ne divisant pas d(L) ;

$$(ii) \qquad Z(s,C/\mathbb{Q}) = f(s).\zeta(s).\zeta(s-1).(\det D(s,2))^{-1}$$

où f est une fonction élémentaire et ζ la fonction zêta de Riemann.

Il est clair que (ii) résulte de (i) et des définitions. La démonstration de (i) est l'objet des §§ 4,5. Le point central en est la formule de congruence (4.4), qui relie la caractéristique zéro et la caractéristique p. Elle permet de transporter en caractéristique zéro des calculs relatifs à l'application de Frobenius, et

d'utiliser l'isomorphisme de $S_2(\Gamma)$ avec l'espace des différentielles holomorphes de degré un sur C.

3.4. Conséquences. (1) Joint au résultat mentionné à la fin du § 2, le théorème montre que $Z(s;C/\mathbb{Q})$ est une fonction méromorphe sur le plan complexe, conformément à la conjecture de Hasse-Weil. Jusqu'à présent, cette dernière a été vérifiée principalement dans les cas mentionnés dans cet exposé, dont 3.3 est un exemple typique [1, 6, 7, 11], et pour des variétés abéliennes à multiplication complexe [16, Chap.IV].

(2) Les valeurs propres de $M_\ell(\pi)$, (cf. 3.1), étant égales à $p^{\frac{1}{2}}$ en valeur absolue, 3.3 entraîne que les valeurs propres de $T(p)_2$ sont $\leqslant 2p^{\frac{1}{2}}$ en valeur absolue, ce qui établit l'analogue de la conjecture de Ramanujan-Petersson pour le groupe Γ considéré ici, $k = 2$, et presque tout p.

§ 4. Correspondances modulaires. Démonstration du théorème à partir de la formule de congruence.

Dans tout ce paragraphe, H/Γ est identifiée au modèle C sur lequel porte 3.3.

4.0. Soient X, Y, u des indéterminées, et $H(u;X,Y) = 1 - X.u + Y.u^2 \in \mathbb{Z}[X,Y][u]$. Il existe évidemment des polynômes $f_m(X,Y) \in \mathbb{Z}[X,Y]$ tels que

$$(1)\quad \frac{d}{du}(\log H(u;X,Y)^{\pm 1}) = \pm(1 - X + 2Yu).H(u;X,Y)^{-1} = \mp \sum_{m \geqslant 1} f_m(X,Y).u^{m-1}.$$

Soient V_i des espaces vectoriels de dimension finie sur $\mathbb{C}$ et a_i des entiers $(1 \leqslant i \leqslant q)$. Si X_i, Y_i sont des endomorphismes de V_i commutant entre eux, on déduit immédiatement de (1) que l'on a, dans $\mathbb{C}[[u]]$:

$$(2)\quad \frac{d}{du}(\log \prod_i (\det H(u;X_i,Y_i))^{-a_i} = \Sigma_{i,m}\, a_i.\mathrm{tr}(f_m(X_i,Y_i).u^{m-1}).$$

4.1. Une correspondance (propre) d'une courbe algébrique lisse V est un diviseur de $V \times V$ (sans composante de la forme $v \times V$ ou $V \times v$ $(v \in V)$). Les correspondances propres sur V forment un anneau : l'addition est définie par celle des

diviseurs, et le produit $X \circ Y$ de X,Y est la projection pr_{13}, sur le produit du premier et du troisième facteur de $V \times V \times V$, du cycle $(V \times X).(Y \times V)$. La permutation des deux facteurs de $V \times V$ induit un antiautomorphisme (de Rosati) $X \mapsto {}^tX$ de l'anneau des correspondances propres.

On note $d(X)$, $d'(X)$ les entiers tels que $pr_1(X) = d(X).V$, $pr_2(X) = d'(X).V$. Evidemment $d'(X) = d({}^tX)$. L'entier $d(X)$ est aussi le degré du cycle

$$X(u) = X.(u \times V) \qquad (u \in V).$$

4.2. Soit $a \in \Delta$. Posons $\Gamma(a) = \Gamma \cap a^{-1}.\Gamma.a$, et soit f_1 la projection canonique de $H/\Gamma(a)$ sur C. On a visiblement $a.\Gamma(a).z \subset \Gamma.a.z$ $(z \in H)$, d'où une application $f_2 : H/\Gamma(a) \to C$. Alors l'image de $H/\Gamma(a)$ dans $C \times C$ par (f_1,f_2) est une correspondance propre, ne dépendant que de $\Gamma.a.\Gamma$, appelée <u>correspondance modulaire</u>, qui sera notée $X(\Gamma.a.\Gamma)$. En fait, on ne s'intéressera qu'à $X_p = X(T(p))$, en notant que $X(T(p,p))$ est l'identité (p premier). L'application

$$\Gamma.a.\Gamma \mapsto X(\Gamma.a.\Gamma)$$

induit un homomorphisme de $R(\Gamma,\Delta)$ dans l'anneau des correspondances propres, rationnelles sur $\mathbb{Q}$, de C. Si $\Gamma.a.\Gamma = \cup\, \Gamma.a_i$, alors, en utilisant 1.4(1), on voit immédiatement que :

$$X(v(z)) = \Sigma\, v(a_i(z)),$$

v désignant la projection canonique de H sur C.

4.3. Le ième groupe de cohomologie à coefficients complexes $H^i(C)$ de C est de façon naturelle un espace de représentation pour $R(\Gamma,\Delta)$. Si l'on utilise l'isomorphisme canonique $H^i(H/\Gamma',\mathbb{C}) \cong H^i(\Gamma',\mathbb{C})$, où Γ' est un sous-groupe discret de G, et $H^i(\Gamma',\mathbb{C})$ le ième groupe de ième groupe de cohomologie de Γ' à coefficients dans le module trivial $\mathbb{C}$, on peut définir l'endomorphisme $X(\Gamma.a.\Gamma)^{(i)}$ de $H^i(C)$ associé à $\Gamma.a.\Gamma$ comme le composé des homomorphismes

(1) $\quad H^i(\Gamma;\mathbb{C}) \to H^i(a^{-1}.\Gamma.a;\mathbb{C}) \overset{res}{\to} H^i(\Gamma(a);\mathbb{C}) \overset{cores}{\to} H^i(\Gamma,\mathbb{C}),$

la première flèche étant l'isomorphisme associé à $\gamma \mapsto a^{-1}.\gamma.a$ $(\gamma\in\Gamma)$.

Pour $i = 0, 2$, $X(\Gamma.a.\Gamma)^i$ est l'homothétie de rapport $d(\Gamma.a.\Gamma)$. En effet, si $i = 0$ les espaces vectoriels de (1) s'identifient canoniquement à $\mathbb{C}$, les deux premiers homomorphismes sont l'identité, et le troisième est la multiplication par $[\Gamma : \Gamma(a)] = d(\Gamma.a.\Gamma)$, (cf. 1.4). Si $i = 2$, ces espaces s'identifient de nouveau à $\mathbb{C}$ via l'isomorphisme de $H^2(H/\Gamma', \mathbb{C})$ sur $\mathbb{C}$ qui applique la classe fondamentale de H/Γ' sur 1 $(\Gamma' = \Gamma,\Gamma(a), a^{-1}.\Gamma.a)$. On voit alors que le premier et le troisième homomorphisme sont l'identité, tandis que le deuxième est la multiplication par $[a^{-1}.\Gamma.a : \Gamma(a)]$. Or il est immédiat que cet indice est le nombre de classes à gauche contenues dans $\Gamma.a.\Gamma$; il est donc aussi égal à $d(\Gamma.a.\Gamma)$ (cf. 1.4).

4.4. Le formule de congruence. Elle s'écrit

$$p(X_p) = \pi + {}^t\pi ,$$

où p est un bon nombre premier ne divisant pas $d(L)$, $p(X_p)$ la réduction mod p du cycle X_p, vue comme correspondance sur $p(C)$, et π la correspondance de Frobenius de $p(C)$, (autrement dit le graphe de l'application qui associe au point x de coordonnées homogènes (x_i) le point x^p de coordonnées homogènes (x_i^p)).

Le principe de démonstration de cette égalité sera donné au § 5. Nous indiquons ici comment on en déduit 3.3(i).

4.5. Démonstration de 3.3(i). Nous en donnons tout d'abord une version plus longue que celle de [11], mais qui est utilisée dans le cas des variétés fibrées [6]. Etant donné une correspondance propre X de C (ou de $p(C)$), on note $I_o(X)$ le degré de $X.D$, où D est la diagonale. Si X est une correspondance sur Q de C et si p est bon, alors

(1) $$I_o(X) = I_o(p(X)).$$

N_m étant comme dans 3.1, on a

$$I_o(\pi^m) = I_o({}^t\pi^m) = N_m \qquad (m \in \mathbb{Z},\ m \geqslant 1).$$

D'autre part, $\pi.{}^t\pi = p.\mathrm{Id}.$, donc si l'on pose $X = \pi + {}^t\pi$ et $Y = p.\mathrm{Id}.$ dans 4.0(1), on obtient

$$\pi^m + {}^t\pi^m = f_m(\pi + {}^t\pi,\ p.\mathrm{Id}), \qquad (m \geqslant 1),$$

d'où

$$2.\frac{d}{du} \log Z(u;p(C)) = \sum_{m \geqslant 1} I_o(f_m(\pi + {}^t\pi,\ p.\mathrm{Id})).u^{m-1}\ .$$

En vertu de 4.4 et de (1), cela s'écrit

$$2.\frac{d}{du} \log Z(u;p(C)) = \sum_{m \geqslant 1} I_o(f_m(X_p, p.\mathrm{Id})).u^{m-1}.$$

Mais la formule des points fixes de Lefschetz entraîne

$$I_o(f_m(X_p, p.\mathrm{Id})) = \sum_{i=0,1,2} (-1)^i \operatorname{tr} f_m(X_p^{(i)}, p.\mathrm{Id}),$$

d'où, vu 4.0(2) :

$$(2) \qquad Z(u;p(C))^2 = \prod_{0 \leqslant i \leqslant 2} \det(1 - X_p^{(i)}u + p.u^2)^{(-1)^{i+1}}\ .$$

Comme $d(X_p) = p + 1$, les endomorphismes $X_p^{(o)}$ et $X_p^{(2)}$ sont la multiplication par $p + 1$ (cf. 4.3), donc

$$(3) \qquad \det(1 - X_p^{(i)}.u + p.u^2) = (1 - p.u)(1 - u) \qquad (i = 0,\ 2).$$

On a $H^1(C) = H^{1,o}(C) + H^{o,1}(C)$. L'espace $H^{1,o}(C)$ des différentielles holomorphes de degré 1 sur C s'identifie canoniquement à $S_2(\Gamma)$, et la conjugaison complexe induit un $\mathbb{R}$-isomorphisme de $H^{1,o}$ sur $H^{o,1}$. On vérifie que ces isomorphismes commutent à $R(\Gamma,\Delta)$, opérant dans S_2 par les opérateurs de Hecke (cf. § 2) et dans $H^1(C)$ par les $X(\Gamma.a.\Gamma)^{(1)}$. Comme les valeurs propres des opérateurs de

Hecke sont réelles, et que $T(p,p)_2$ est l'identité, on en déduit

$$(4) \qquad \det(1-X_p^{(1)}.u + p.u^2) = (\det(1-T_{p,2}.u + p.u^2))^2 = \det H(u;p,2)^2,$$

ce qui, joint à (2), (3), démontre 3.3(i).

4.6. Démonstration de 3.3(i), (2ème version). Il suffit de prouver :

$$(1) \qquad \det(1 - T_{p,2}.u + p.u^2) = \det(1 - M_\ell(\hat{\pi}).u),$$

où $\hat{\pi}$ est l'endomorphisme de Frobenius de la jacobienne $J(p(C))$ de $p(C)$, (cf. 3.1). Le membre de droite est aussi égal à $\det(1 - M_\ell({}^t\hat{\pi}).u)$, donc vu $\hat{\pi}.{}^t\hat{\pi} = p.\mathrm{Id}$,

$$(2) \qquad (\det(1 - M_\ell(\hat{\pi}).u))^2 = \det(1 - M_\ell(\hat{\pi} + {}^t\hat{\pi}).u + p.u^2).$$

Soit $p(X_p)\hat{}$ la correspondance de $J(p(C))$ canoniquement associée à $p(X_p)$. La formule de congruence implique

$$p(X_p)\hat{} = \hat{\pi} + {}^t\hat{\pi}$$

d'autre part $J(p(C)) = p(J(C))$ et $p(X_p)\hat{}$ est la réduction mod p de l'endomorphisme $\hat{X}_p$ de $J(C)$ associée à X_p. On sait que l'on a alors

$$M_\ell(X_p) = M_\ell(p(X_p)\hat{})$$

pour un choix convenable de coordonnées ℓ-adiques, d'où

$$(3) \qquad (\det(1 - M_\ell(\pi).u))^2 = \det(1 - M_\ell(X_p).u + p.u^2).$$

Il est bien connu que $M_\ell(X_p)$ est équivalente à la somme $M^d(X_p) + \bar{M}^d(X_p)$, où $M^d(X_p)$ est l'endomorphisme de l'espace des différentielles de première espèce sur C induit par X_p. En utilisant l'isomorphisme canonique de ce dernier espace sur $S_2(\Gamma)$ on voit que le membre de droite de (3) est égal à $\det(1 - T_{p,2}.u + p.u^2)^2$, d'où le résultat.

§ 5. Familles de variétés abéliennes. Formule de congruence.

5.1. (Pour le contenu de ce n°, cf. [10]). Pour $z \in C$, on note $e(z)$ le vecteur $(z,1)$ de $\mathbb{C}^2$. Etant donné $z \in H$, l'ensemble $\underline{o}.e(z) = D_z$ est un réseau de $\mathbb{C}^2$. Soit $c \in \underline{o}$ tel que c^2 soit rationnel et < 0. On montre qu'un multiple de la forme $\mathbb{R}$-bilinéaire E sur $\mathbb{C}^2$ définie par

$$E(a.e(z),\ b.e(z)) = \mathrm{tr}(c.a.b'), \quad (a,\ b \in L \otimes \mathbb{R}),$$

est une forme de Riemann sur D_z, d'où une structure de variété abélienne et une polarisation C_z sur le quotient $A_z = \mathbb{C}^2/D_z$. La transformation linéaire de $\mathbb{C}^2$ définie par $a \in \underline{o}$ laisse D_z stable, donc définit un endomorphisme de A_z, d'où un monomorphisme θ_z de $\underline{o}$ dans l'anneau $A(A_z)$ des endomorphismes de A_z, (compatible avec la polarisation en ce sens que

$$E(\theta_z(a).x,y) = E(x,\theta_z(c^{-1}.a'.c).y) \quad (a \in \underline{o},\ x,\ y \in \mathbb{C}^2).$$

On a ainsi obtenu une famille analytique de variétés abéliennes polarisées $P_z = (A_z, C_z, \theta_z)$ de type $\underline{o}$, paramétrée par H. Un homomorphisme de P_x sur P_y $(x,\ y \in H)$ est une isogénie $f : A_x \to A_y$ commutant à $\underline{o}$ et telle que $f^{-1}(C_y) = C_x$. On montre que P_x est isomorphe à P_y si et seulement si $x \in \Gamma.y$. La courbe C paramètre donc les classes d'isomorphisme de tels systèmes. On peut préciser cela en construisant dans un espace projectif une famille F de sous-variétés F_z $(z \in H)$ ayant notamment les propriétés suivantes : $F(x) = F(y)$ si et seulement si $x \in \Gamma.y$ $(x,\ y \in H)$. Le point de Chow $c(F_z)$ de F_z décrit une courbe C' définie sur $\mathbb{Q}$ et $\mathbb{Q}(c(F_z))$ est le "corps des modules" de P_z (i.e. le plus petit sous-corps k de $\mathbb{C}$ ayant la propriété suivante : si K est un corps de définition pour $A_z, C_z, \theta_z(a)$ $(a \in \underline{o})$ et σ est un monomorphisme de K dans $\mathbb{C}$, alors $K \supset k$ et P_z est isomorphe à $(A_z^\sigma, C_z^\sigma, \theta_z^\sigma)$ si et seulement si σ est l'identité sur k.) Il existe un nombre fini de fonctions f_i sur H automorphes

pour Γ, définies en dehors de la réunion W d'un nombre fini d'orbites de Γ, qui engendrent sur $\mathbb{C}$ le corps $K(\Gamma)$ des fonctions automorphes pour Γ, telles que pour $z \in H-W$, les coordonnées de $c(F_z)$ soient $(1, f_1(z), \ldots, f_m(z))$.

Le corps $L = \mathbb{Q}(u)$, (u générique sur $\mathbb{Q}$) s'identifie donc à un sous-corps de $K(\Gamma)$ tel que $K(\Gamma) = \mathbb{C}.L$. La courbe C du théorème est un modèle lisse sur $\mathbb{Q}$ de L. Elle est analytiquement isomorphe à H/Γ. Dans la suite, on n'aura à considérer que des points génériques, aussi ne distinguerons-nous pas entre C et C'.

[Pour donner une idée de la construction de F, indiquons comment on obtient un système de représentants des classes d'isomorphisme de variétés abéliennes polarisées (A_z, C_z) : on part d'une famille de plongements projectifs $\mu_z : A_z \to P = \mathbb{P}(n,\mathbb{C})$ dépendant holomorphiquement de $z \in H$, tels que C_z soit induite par les sections hyperplanes (ce qui se construit à l'aide de fonctions thêta, cf. [8]). En associant à $\varphi \in \mathrm{Aut}\, P$ le point de Chow $c(\varphi(\mu_z(A_z)))$ de $\varphi(\mu_z(A_z))$ on définit un morphisme ν_z de $\mathrm{Aut}\, P$ dans un espace projectif. Alors $F(A_z, C_z)$ est l'adhérence de Zariski de l'image de ν_z.]

5.2. La correspondance X_p définie dans 4.2 est de degré $p+1$. Ecrivons, pour $u \in C$ générique

$$X_p(u) = X_p \circ (u \times C) = u_o + \ldots + u_p .$$

Pour démontrer la formule de congruence (4.3), il suffit de faire voir que si k est un corps sur lequel u et les u_i sont rationnels et $\underline{p}$ est une place de k prolongeant p, alors on a, $\bar{}$ dénotant la réduction mod $\underline{p}$:

$$(1) \qquad \bar{u}_o = \bar{u}^p , \quad \bar{u}_i^p = \bar{u}_o .$$

En effet, on a $\pi(\bar{u}) = \bar{u}^p$ et ${}^t\pi(\bar{u}) = p \circ \bar{u}^{1/p}$; la réduction commutant à l'intersection de cycles positifs, (1) entraîne que $p(X_p) - (\pi + {}^t\pi)$ est un diviseur de la forme

$\underline{a} \times C$, où $\underline{a}$ est un diviseur de C ; comme $\pi + {}^t\pi$ n'a pas de composante de ce type, $\underline{a}$ doit être positif, mais d'autre part il est de degré zéro, puisque $d(p(X_p)) = d(\pi + {}^t\pi) = p + 1$.

La démonstration de (1) se fera en établissant des relations similaires pour les réductions mod $\underline{p}$ des variétés abéliennes polarisées de type $\underline{o}$ représentées par les points de C.

5.3. Soit v la projection de H sur C. On fixe un point $u \in C$ "suffisamment général", et $y \in v^{-1}(u)$. Soit p un bon nombre premier ne divisant pas $d(L)$. Soient $\underline{o}.a_i$ $(0 \leqslant i \leqslant p)$ les idéaux de norme p et $y_i = a_i(y)$. On a donc $T(p) = \cup\, \Gamma.a_i$ et le cycle $X_p(u)$ est la somme des $v(y_i)$. En accord avec 5.2, on pose $u_i = v(y_i)$. On écrira $A_i, C_i, \theta_i, P_i, F_i, D_i$ pour A_{y_i}, C_{y_i}, θ_{y_i}, P_{y_i}, F_{y_i}, D_{y_i}. Admettons que P_i et F_i soient rationnels sur k et se réduisent bien mod $\underline{p}$. Alors (1) équivaut à

$$\overline{c(F_o)} = \overline{c(F_u)}^p,\ \overline{c(F_i)}^p = \overline{c(F_u)} \qquad (1 \leqslant i \leqslant p). \tag{2}$$

Vu les propriétés de la famille F, cela revient à

$$\bar{A}_o = (\bar{A}_y)^p,\ (\bar{A}_i)^p = \bar{A}_y \qquad (1 \leqslant i \leqslant p), \tag{3}$$

et à des relations semblables pour les C_i et θ_i. On se bornera ici à démontrer (3), le reste se prouvant de la même manière.

5.4. Le groupe $g(p, A_y)$ des éléments d'ordre p de A_y est d'ordre p^4 et s'identifie canoniquement, comme $\underline{o}$-module, à $\underline{o}/p.\underline{o} = M(2, \mathbb{Z}/2\mathbb{Z})$. C'est le noyau de l'isogénie $p.\mathrm{Id}$. Il possède $p+1$ sous-$\underline{o}$-modules g_i d'ordre p^2, dont les images inverses sont, dans $\underline{o}$ les idéaux $\underline{o}.a_i$ et dans $\mathbb{C}^2$ les réseaux $p^{-1}.\underline{o}.a_i(e(y))$, $(0 \leqslant i \leqslant p)$. On a évidemment, dans les notations du § 2,

$$a_i.e(y) = j(a_i, y).e(y_i),$$

ce qui entraîne que l'homothétie de $\mathbb{C}^2$ de rapport $p.j(a_i, y)^{-1}$ envoie

$p^{-1}.\underline{o}a_i(e(y))$ sur D_i. Elle induit donc une isogénie $\lambda_i : A_y \to A_i$ de noyau g_i, qui visiblement, commute à $\underline{o}$ et est compatible avec les polarisations ; c'est donc en fait une isogénie de P_y sur P_i. Comme $\operatorname{Ker} \lambda_i \subset g(p,A_y)$, on a une factorisation $p.\mathrm{Id} = \mu_i.\lambda_i$, où μ_i est une isogénie de P_i sur P_y. Quitte à passer à une extension de k, on peut supposer les éléments de $g(p,A_y)$ rationnels sur k, donc λ_i, μ_i définis sur k. Supposons que P_y, P_i, F_y, F_i $(0 \leqslant i \leqslant p)$ se réduisent bien mod $\underline{p}$. La réduction mod $\underline{p}$ définit un homomorphisme r de $g(p,A_y)$ dans le groupe $g(\bar{A}_y)$ des éléments d'ordre p de $\bar{A}_y$, qui est surjectif [16, Prop. 16, p.98]. On montre d'autre part que $g(p,\bar{A}_y)$ est d'ordre p^2 [6, 5.11, p. 516]. Le noyau de r est donc l'un des g_i, que l'on supposera être $\underline{g}_o$. Sous les hypothèses faites $r(\ker \bar{\lambda}_i) = \ker \bar{\lambda}_i$ $(0 \leqslant i \leqslant p)$ [16, Prop. 13, p. 96]. D'autre part, g_i et g_j sont supplémentaires si $i \neq j$, donc

$$r(g_i) = g(p,\bar{A}_y) \qquad (1 \leqslant i \leqslant p).$$

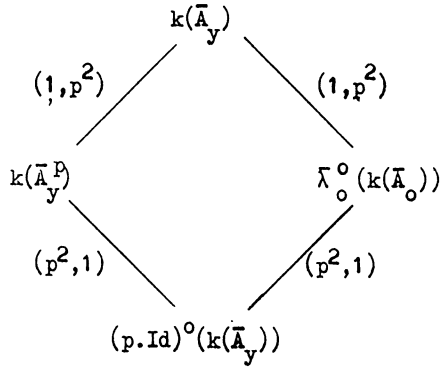
On a donc

$$\ker \bar{\lambda}_o = (0)$$

$$\ker \bar{\lambda}_i = g(p,\bar{A}_y) \qquad (1 \leqslant i \leqslant p)$$

Mais $\mu_i.\lambda_i = p.\mathrm{Id}$ entraîne $\bar{\mu}_i.\bar{\lambda}_i = p.\mathrm{Id}$. Comme le degré d'une isogénie se conserve par réduction et que celui de $p.\mathrm{Id}$ est p^4, on a un diagramme d'extensions de corps (voir page suivante) ; dans ce diagramme, $k(A)$ est le corps des fonctions rationnelles sur k de la k-variété A, f^o le morphisme de fonctions associé à un k-morphisme f de variétés, et (a,b) = (degré séparable, degré inséparable).

(4)



Cela entraîne que $k(\bar{A}_y^p) = \bar{\lambda}_o^o(k(\bar{A}_o)) \simeq k(\bar{A}_o)$, et par suite que $\bar{A}_y^p$ et $\bar{A}_o$ sont birationnellement k-isomorphes, donc k-isomorphes. C'est la première égalité de (3). En remplaçant dans ce qui précède $\bar{A}_y$, $\bar{A}_o$ et $\bar{\lambda}_o$ par $\bar{A}_i$, $\bar{A}_y$ et $\bar{\mu}_i$ $(i \geqslant 1)$, on démontre exactement de la même manière la deuxième partie de (3). (Pour cette démonstration, dans le cas plus général de 6.1, voir [11, § 5].)

5.5. Remarque. Il y a quelques précautions à prendre avec les conditions de bonne réduction mod $\underline{p}$, car d'une part tout doit marcher en dehors d'un ensemble fini de nombres premiers, et d'autre part les P_i, y_i dépendent de p. Ayant fixé u, on commence par choisir une extension k_o de type fini de $\mathbb{Q}$, sur laquelle P_y est défini et, pour tout bon p, une place $\underline{p}_o$ de k_o prolongeant p. Pour presque tout p, P_y et F_y se réduisent bien mod $\underline{p}_o$. Choisissons un tel p. Soit k une extension algébrique de k_o sur laquelle les éléments de $g(p,A_y)$ sont rationnels, et soit $\underline{p}$ une extension de $\underline{p}_o$ à k. Comme P_i est l'image de P_y par une k-isogénie, il résulte d'un théorème de Koizumi-Shimura [3] que l'on peut trouver un modèle $P_i^* = (A_i^*, C_i^*, \theta_i^*)$ de P_i tel que P_i^* et les isogénies λ_i^*, μ_i^* correspondant à λ_i, μ_i se réduisent bien mod $\underline{p}$. Au changement de modèle des P_i près, qui ne modifie pas substantiellement la démonstration, on est donc bien parvenu à la situation de 5.4 pour presque tout p.

§ 6. Généralisations.

Le théorème 3.3 a été généralisé dans trois directions, que nous allons passer brièvement en revue.

Dans ce paragraphe, $\underline{b} = \underline{o}.b$ est un $\underline{o}$.idéal entier bilatère de L, on note b_o l'entier rationnel > 0 tel que $\underline{b} \cap \mathbb{Z} = b_o.\mathbb{Z}$, et l'on pose

$$\Delta_{\underline{b}} = \{x \in \Delta,\ (\det x,\ b_o) = 1\} ,$$

$$\Gamma_{\underline{b}} = \{\gamma \in \Gamma,\ \gamma \equiv 1 \bmod \underline{b}\} .$$

L'application $\Gamma_{\underline{b}}.a.\Gamma_{\underline{b}} \longmapsto \Gamma.a.\Gamma$ induit un homomorphisme de l'anneau de Hecke $R(\Gamma_{\underline{b}},\Delta_{\underline{b}})$, qui n'est pas toujours commutatif, dans $R(\Gamma,\Delta)$.

6.1. Sous-groupes de congruence [11]. On suppose ici $\underline{b}$ premier à $\underline{o}.d(L)$. On peut alors prendre $b = b_o$. et il existe un isomorphisme $h_{\underline{b}}$ de $\underline{o}$-modules de $\underline{o}/\underline{b}$ sur $\mathbb{M}(2, \mathbb{Z}/b\mathbb{Z})$. On note $\Delta_{\underline{b}}^*$ l'ensemble des éléments de $\Delta_{\underline{b}}$ dont l'image par $h_{\underline{b}}$ est de la forme $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$. L'homomorphisme $R(\Gamma_{\underline{b}},\Delta_{\underline{b}}) \to R(\Gamma,\Delta)$ induit un isomorphisme de $R_{\underline{b}} = R(\Gamma_{\underline{b}},\Delta_{\underline{b}}^*)$ sur $R(\Gamma,\Delta_{\underline{b}})$ [11, Prop. 1.15]. On désigne par $T_{\underline{b}}(p)$ et $T_{\underline{b}}(p,p)$ les éléments correspondant par cet isomorphisme à $T(p)$ pour p premier à b et à $T(p,p)$ pour p premier à $b.d(L)$. On fait opérer $R_{\underline{b}}$ sur l'espace $S_k(\Gamma_{\underline{b}})$ des formes automorphes de poids k comme au § 2, et on en déduit une série de Dirichlet

$$D_{\underline{b}}(s,k) = \Sigma\ (\Gamma_{\underline{b}}.a.\Gamma_{\underline{b}})_k.(\det a)^{-s} = \prod_{\substack{p \text{ premier} \\ (p,\underline{b}) = 1}} H_{\underline{b}}(p^{-s};p,k)$$

où $H_{\underline{b}}(u;p,k)$ est le polynôme obtenu à partir du polynôme $H(u;p,k)$ du § 2 en remplaçant $T(p)_k$ et $T(p,p)_k$ par les endomorphismes $T_{\underline{b}}(p)_k$ et $T_{\underline{b}}(p,p)_k$ de $S_k(\Gamma_{\underline{b}})$ définis par $T_{\underline{b}}(p)$ et $T_{\underline{b}}(p,p)$; cette série se prolonge en une fonction entière avec équation fonctionnelle [11, § 1].

On reprend les notations du § 5. Pour $z \in H$, soit t_z l'image dans A_z du point $b^{-1}.e(z)$. On vérifie que $x \mapsto \theta_z(x).t_z$ induit un isomorphisme de $\underline{o}$-modules de $\underline{o}/\underline{b}$ sur le groupe $g(b,A_z) = \{t \in A_z, \theta_z(\underline{b}).t = 0\}$ des points d'ordre b de A_z. On associe alors à z le système $Q_z = (P_z, t_z)$ formé de P_z, avec les points d'ordre b de A_z marqués (dans un ordre déterminé). On montre que $Q_x \cong Q_y$ $(x,y \in H)$ si et seulement si $x \in \Gamma_{\underline{b}}.y$ [14, Prop. 4.4]. Le système Q_z admet un corps de modules; les résultats de 5.1. s'étendent et conduisent à un modèle projectif lisse $C_{\underline{b}}$ sur $\mathbb{Q}$ de $H/\Gamma_{\underline{b}}$ pour lequel 3.3 est valable, pour presque tout p ne divisant pas $b.d(L)$, une fois $H(u;p,2)$ et $D(s,2)$ remplacés par $H_{\underline{b}}(u;p,2)$ et $D_{\underline{b}}(s,2)$.

La démonstration est semblable en principe à celle de 3.3(i), mais présente quelques complications techniques, en particulier à propos de la formule de congruence. En effet, l'isogénie $\lambda_i : P_y \to P_{y_i}$ de 5.4 applique t_y sur $\pm p.t_{y_i}$ pour $i \geq 1$, et n'est donc pas une isogénie de Q_y sur Q_{y_i}. En introduisant un automorphisme convenable $Y_{\underline{b}}$ de $C_{\underline{b}}$, laissant stables les fibres de $C_{\underline{b}} \to C$, et induisant la bijection

$$\{\pm t\} \mapsto \{\pm p.t\}$$

de $g(\underline{b},A_y)/\{\pm 1\}$, on est conduit à une formule de congruence de la forme

$$\bar{X}_p = \pi + {}^t\pi \circ \bar{Y}_p \tag{1}$$

où $\bar{}$ est la réduction mod p, qui se complète par

$${}^t\pi \circ \bar{Y}_p = {}^t\bar{Z} \circ {}^t\pi \circ \bar{Z}\ , \tag{2}$$

où Z est un automorphisme défini sur $\mathbb{Q}$ de $C_{\underline{b}}$ [11, theorems 4,5]. La partie de la démonstration résumée au § 4 subsiste avec peu de changements.

6.2. Variétés fibrées [6]. On suppose jusqu'à la fin de cet exposé que $\Gamma_{\underline{b}}$ opère librement sur H, (ce qui a lieu notamment si $b_o \geq 3$). Soit $W_{\underline{b}}$ le quo-

tient de $H \times (L_R/o)$ par Γ_b, opérant via $\gamma(z,u) = (\gamma.z, \gamma.u)$. C'est une variété fibrée sur C_b, de fibre type le tore $T = L_R/o$, de groupe structural Γ_b. On munit W_b d'une structure de variété analytique complexe telle que la projection $\varphi_b : W_b \to C_b$ soit un morphisme, que les zéros des fibres forment une section holomorphe ψ_b, et que la fibre sur un point $v_b(z)$ soit isomorphe à $A_z(z \in H; v_b$ projection de H sur $H/\Gamma_b)$. Soit $W_{m,b}$ ou W_m le produit fibré sur C_b de m copies de W_b, φ_{mb} la projection de $W_{m,b}$ sur C_b et ψ_{mb} la section zéro de W_{mb}. Il existe des modèles projectifs lisses de W_m, C_b définis sur le corps cyclotomique $K_b = \mathbb{Q}(\exp. 2\pi i.b_o^{-1})$ tels que ψ_{mb} et φ_{mb} soient définis sur K_b [14, §§ 5,6].

Dans la suite de ce n°, on suppose b premier à $d(L)$. On peut alors remplacer K_b par $\mathbb{Q}$ dans l'assertion précédente [6, Prop. 7.4]. Le théorème 3.3(i) se généralise de la manière suivante [6, 7.7] :

6.3. THÉORÈME. *On conserve les notations précédentes. Il existe des entiers* $a(m,i,q) \geqslant 0$ $(0 \leqslant i \leqslant 4m\ ;\ 0 \leqslant q \leqslant i)$ *tels que l'on ait,*

$$Z(u,p(W_{m,b})) = \prod_{0 \leqslant j \leqslant 2m} ((1-p^j.u).(1-p^{j+1}.u))^{-a(m,2j,0)} \times$$

(1)

$$\times \prod_{0 \leqslant i \leqslant 4m} \prod_{0 \leqslant q \leqslant i} \det (H_b(p^{(i-q)/2}.u;p,q+2))^{(-1)^i a(m,i,q)}$$

pour presque tout nombre premier p *ne divisant pas* $b.d(L)$.

Il en résulte en particulier que la fonction zêta globale $Z(s,W_{m,b}/\mathbb{Q})$ est le produit d'une fonction élémentaire de s, de translatées de $\zeta(s)$, et de

$$(2) \qquad \prod_{0 \leqslant i \leqslant 4m} \cdot \prod_{0 \leqslant q \leqslant i} \det D_b(s-(i-q)/2,\ q+2)^{(-1)^{i+1} a(m,i,q)}\ ,$$

donc que $Z(s,W_{m,b})$ se prolonge en une fonction méromorphe sur le plan complexe.

Pour la démonstration de 6.3 on définit un homomorphisme $\Gamma.a.\Gamma \mapsto X_m(\Gamma.a.\Gamma)$ de $R_{\underline{b}}$ dans l'anneau des correspondances propres de W_m rationnelles sur $\mathbb{Q}$, commutant à $\varphi_{m\underline{b}}$, et on montre [6,7.5] que la réduction mod p de $X_m(T_{\underline{b}}(p))$ vérifie des formules de congruence qui s'écrivent comme 6.1(1), (2), sauf que ${}^t\pi$ est remplacé par une correspondance π^* qui induit ${}^t\pi$ sur C_b et l'isogénie $u \mapsto p.u$ sur chaque fibre, (i.e. dont le diviseur est le lieu des points $(x^p, p.x)$). Des calculs presque identiques à ceux de 4.5 mènent alors à

$$(3) \qquad Z(u,p(W_m))^2 = \prod_{0 \leqslant i \leqslant 4m+2} \det(1 - X_{mp}^{(i)}.u + p.U_{mp}^{(i)}.u^2)^{(-1)^{i+1}} ,$$

où $X_{mp}^{(i)}$ et $U_{mp}^{(i)}$ désignent les endomorphismes de $H^i(W_m;\mathbb{C})$ induits par les correspondances $X_m(T_{\underline{b}}(p))$ et $X_m(T_{\underline{b}}(p,p))$. La détermination de ceux-ci est faite dans [4]. On établit tout d'abord un isomorphisme d'espaces vectoriels, où la cohomologie est à coefficients complexes :

$$(4) \qquad H^i(W_m) = \sum_{c+d=i} H^c(\Gamma_{\underline{b}}; H^d(T^m)), \qquad (T = L_{\mathbb{R}}/o) ,$$

les termes de droite étant nuls pour $c \geqslant 3$; on montre que $H^d(T^m)$ s'identifie, comme $\Gamma_{\underline{b}}$-module, au dual de $\bigwedge^d(L_{\mathbb{C}} + \ldots + L_{\mathbb{C}})$, (m copies), sur lequel $\Gamma_{\underline{b}}$ agit par la représentation congragrédiente de $\bigwedge^d \circ \rho^{(m)}$, où $\rho^{(m)}$ est la somme directe de m copies de la représentation de G dans $L_{\mathbb{C}}$ définie par multiplication à gauche [4, Chap. I-II]. On décompose ensuite ces espaces en sommes directes de G-modules irréductibles. On parvient ainsi à une somme de termes de la forme $H^c(\Gamma_{\underline{b}}; M_q)$, où M_q est l'espace des polynômes homogènes de degré q sur $\mathbb{C}^2$, muni de sa structure usuelle de $\Gamma_{\underline{b}}$-module. Pour $c = 0,2$, on montre que $X_m(\Gamma.a.\Gamma)^{(c+d)}$ opère sur $H^c(\Gamma_{\underline{b}}; H^d(T^m))$ par homothétie de rapport $(\det a)^{d/2}.d(\Gamma.a.\Gamma)$, [4, Thm IV-2-3]. Pour $i = 1$, on utilise l'isomorphisme de Eichler-Shimura [12, 17] :

$$(5) \qquad H^1(\Gamma_{\underline{b}};M_q) \cong S_{q+2}(\Gamma_{\underline{b}}) + \overline{S_{q+2}(\Gamma_{\underline{b}})} .$$

On en déduit alors une décomposition de $X_{mp}^{(i)}$ et $U_{mp}^{(i)}$ en somme d'opérateurs de Hecke et d'opérateurs scalaires [4, Chap. IV, 2], qui conduit au résultat.

L'opérateur $T_{\underline{b}}(p,p)_k$ est la multiplication par p^{k-2}. On tire alors de 6.3 et des conjectures de Weil (cf. 3.1) que les valeurs propres de $T_{\underline{b}}(p)_k$ sont $\leqslant 2.p^{(k-1)/2}$, (cf. [6], 6.12, 6.14).

6.4. Variétés fibrées et fonctions L [6]. Soient $G_{\underline{b}}$ le groupe des éléments inversibles de $\underline{o}/\underline{b}$ et $S_{\underline{b}}$ le sous-groupe de $G_{\underline{b}}$ formé des classes de restes contenant un élément a de déterminant $\equiv 1 \bmod \underline{b}$. La projection de $\underline{o}$ sur $\underline{o}/\underline{b}$ induit un isomorphisme de $\Gamma/\Gamma_{\underline{b}}$ sur $S_{\underline{b}}$ [6, Prop. 1.8]. On définit d'autre part un homomorphisme $s \mapsto Y(s)$ de $S_{\underline{b}}$ sur un groupe d'automorphismes de W_m définis sur $K_{\underline{b}}$, injectif si $m \geqslant 1$, de noyau ± 1 si $m = 0$ [6, 6.7].

Soit π une représentation de $G_{\underline{b}}$ dans un espace vectoriel complexe U de dimension finie. On note $S_k(\Gamma,\pi)$ l'espace vectoriel des applications holomorphes $f : H \to U$ vérifiant $f(\gamma(z)) = j(\gamma,z)^k.\pi(\gamma).f(z)$ $(z \in H; \gamma \in \Gamma)$.

Les résultats mentionnés plus haut sont en fait des cas particuliers des théorèmes principaux de [6]. Ces derniers établissent des relations semblables entre opérateurs de Hecke opérant sur certains espaces $S_k(\Gamma,\pi)$ et séries L de $\underline{p}(W_{m,\underline{b}})$, ($\underline{p}$ idéal premier de $K_{\underline{b}}$), définies par rapport au groupe d'automorphismes $\underline{p}(Y(s))$ $(s \in S_{\underline{b}})$ et à certains caractères de $S_{\underline{b}}$. On renvoie à [6], pour les énoncés (Thms 6.8, 6.11) et les démonstrations.

BIBLIOGRAPHIE

Outre les mémoires cités dans le texte, elle comprend quelques articles d'exposition ([5], [9], [13], [15]).

[1] M. EICHLER - Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Archiv der Math., 5 (1954), 355-366.

[2] A. GROTHENDIECK - Formule de Lefschetz et rationalité des fonctions L. Sém. Bourbaki, 17e année, 1964-65, Exp. 279.

[3] S. KOIZUMI and G. SHIMURA - On specializations of abelian varieties. Sci. Papers Coll. Gen. Ed. Univ. Tokyo 9 (1959), 187-211.

[4] M. KUGA - Fibre varieties over a symmetric space whose fibres are abelian varieties. Lecture Notes, Univ. of Chicago, 1963-64.

[5] M. KUGA - Fibre varieties over a symmetric space whose fibres are abelian varieties. Proc. Symp. Pure Math. 9, A.M.S., Providence R.I., 1966.

[6] M. KUGA and G. SHIMURA - On the zeta function of a fibre variety whose fibres are abelian varieties. Annals of Math.(2) 82 (1965), 478-539.

[7] G. SHIMURA - Correspondances modulaires et les fonctions ζ des courbes algébriques. J. Math. Soc. Japan 10(1958), 1-28.

[8] G. SHIMURA - Modules de variétés abéliennes polarisées et fonctions modulaires III. Sém. E.N.S. 1957-58, Exp. 20.

[9] G. SHIMURA - Fonctions automorphes et corrèspondances modulaires. Proc. Int. Congress Math. Edimburgh 1958, Cambridge Univ. Press, p. 330-338.

[10] G. SHIMURA - On the theory of automorphic functions. Annals of Math. (2) 70(1959), 101-144.

[11] G. SHIMURA - On the zeta-functions of curves uniformized by certain automorphic functions. J. Math. Soc. Japan 13(1961), 275-331.

[12] G. SHIMURA - On Dirichlet series and abelian varieties attached to automorphic forms. Annals of Math. (2) 76(1962), 237-294.

[13] G. SHIMURA - The zeta-function of an algebraic variety and automorphic functions. Summer Institute on algebraic geometry, Woodshole 1964, (Notes)

[14] G. SHIMURA - On the field of definition for a field of automorphic functions II. Annals of Math. (2) 81(1965), 124-165.

[15] G. SHIMURA - Moduli of abelian varieties and number theory. Proc. Symp. pur. Math. 9, A.M.S. Providence R.I. 1966.

[16] G. SHIMURA and Y. TANIYAMA - Complex multiplication of abelian varieties and its applicationsto number theory. Publ. Math. Soc. Japan 6 (1961).

[17] J.-L. VERDIER - Sur les intégrales attachées aux formes automorphes. Sém. Bourbaki 13e année, 1960-1961, Exp. 216.

[18] A. WEIL - Variétés abéliennes et courbes algébriques. Act. Sci. Ind. 1064, Hermann éd., Paris 1948.

ERRATA

Page 307-06 - Lignes 2 et 3, insérer "inverses" après "racines" et remplacer " $p^{-i/2}$ " par " $p^{i/2}$ ".

Page 307-21 - Ligne 5, insérer : "en valeur absolue" après " $\leq 2.p^{(k-1)/2}$ ".