ANNALES SCIENTIFIQUES DE L'É.N.S.

PIERRE DELIGNE
JEAN-PIERRE SERRE

Formes modulaires de poids 1

Annales scientifiques de l'É.N.S. 4^e série, tome 7, n° 4 (1974), p. 507-530.
<http://www.numdam.org/item?id=ASENS_1974_4_7_4_507_0>

Ann. scient. Éc. Norm. Sup.
4e série, t. 7, 1974, p. 507 à 530.

FORMES MODULAIRES DE POIDS 1

PAR PIERRE DELIGNE ET JEAN-PIERRE SERRE

A Henri Cartan,
à l'occasion de son
70e anniversaire

Introduction

La décomposition en produit eulérien, et l'équation fonctionnelle, des séries de Dirichlet associées par Hecke aux *formes modulaires de poids* 1 suggèrent que celles-ci correspondent à des *fonctions* L *d'Artin de degré* 2 *du corps* $\mathbf{Q}$, autrement dit à des *représentations de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *dans* $\mathbf{GL}_2(\mathbf{C})$. C'est une telle correspondance, conjecturée par Langlands, que nous établissons ici.

Les trois premiers paragraphes sont préliminaires. Le paragraphe 4 contient l'énoncé du théorème principal, et quelques compléments. La démonstration occupe les paragraphes 5 à 9. Son principe est le suivant : on commence par construire, pour tout nombre premier l, une représentation de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ en caractéristique l (*cf.* § 6); on montre ensuite que les images de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans ces diverses représentations sont « petites », ce qui permet de les relever en caractéristique 0, et d'obtenir la représentation complexe cherchée (§§ 7 et 8); la « petitesse » en question résulte elle-même d'une majoration en moyenne des valeurs propres des opérateurs de Hecke (Rankin, *cf.* § 5). Le paragraphe 9 contient une estimation des coefficients des formes modulaires de poids 1.

Signalons que nous avons utilisé en un point essentiel (§ 6, th. 6.1) des résultats démontrés par l'un de nous (P. Deligne), mais dont aucune démonstration complète n'a encore été publiée; en attendant une telle publication (ainsi que celle de SGA 5, dont ils dépendent), nous demandons au lecteur de bien vouloir les admettre.

§ 1. Rappels (analytiques) sur les formes modulaires

1.1. Soit N un entier $\geqq 1$. On associe à N les sous-groupes

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$$

de $\mathbf{SL}_2(\mathbf{Z})$ définis par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N) \quad \Leftrightarrow \quad a \equiv d \equiv 1 \pmod{N} \quad \text{et} \quad b \equiv c \equiv 0 \pmod{N},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \quad \Leftrightarrow \quad a \equiv d \equiv 1 \pmod{N} \quad \text{et} \quad c \equiv 0 \pmod{N},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \quad \Leftrightarrow \quad c \equiv 0 \pmod{N}.$$

1.2. Soit f une fonction sur le demi-plan $\mathrm{H} = \{ z \mid \mathrm{Im}(z) > 0 \}$. Si k est un entier, et si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un élément de $\mathbf{SL}_2(\mathbf{R})$, on pose

$$(f|_k \gamma)(z) = (cz+d)^{-k} f(\gamma z), \qquad \text{où} \quad \gamma z = \frac{az+b}{cz+d}.$$

Soit Γ un sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ contenant $\Gamma(N)$. On dit que f est *modulaire de poids k* sur Γ si :

(1.2.1) $f|_k \gamma = f$ pour tout $\gamma \in \Gamma$;

(1.2.2) f est holomorphe sur H;

(1.2.3) f est « holomorphe aux pointes », i. e., pour tout $\sigma \in \mathbf{SL}_2(\mathbf{Z})$, la fonction $f|_k \sigma$ a un développement en série de puissances de $e^{2\pi i z/N}$ à exposants $\geqq 0$.

Lorsque, dans (1.2.3), on remplace « exposants $\geqq 0$ » par « exposants > 0 », on obtient la notion de forme modulaire *parabolique*.

1.3. Soit f une forme modulaire de poids k sur $\Gamma(N)$. Pour que f soit une forme modulaire sur $\Gamma_1(N)$, il faut et il suffit que $f(z+1) = f(z)$, ou encore que f ait un développement de la forme

$$\sum_{n=0}^{\infty} a_n q^n, \qquad \text{où} \quad q = e^{2\pi i z}.$$

Dans ce qui suit, ce développement sera noté $f_\infty(q)$, ou simplement f.

1.4. Soit f une forme modulaire de poids k sur $\Gamma_1(N)$. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un élément de $\Gamma_0(N)$, la forme $f|_k \gamma$ ne dépend que de l'image de d dans $(\mathbf{Z}/N\mathbf{Z})^*$; on la note $f \mid \mathrm{R}_d$. On a $f \mid \mathrm{R}_{-1} = (-1)^k f$.

1.5. Soit ε un *caractère de Dirichlet* mod N, autrement dit un homomorphisme

$$\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*.$$

On dit que ε est *pair* (resp. *impair*) si $\varepsilon(-1) = 1$ (resp. si $\varepsilon(-1) = -1$).

Soit k un entier de même parité que ε [i. e. $\varepsilon(-1) = (-1)^k$]. On appelle *forme modulaire de type* (k, ε) *sur* $\Gamma_0(N)$ une forme modulaire f de poids k sur $\Gamma_1(N)$ telle que

$$f \mid R_d = \varepsilon(d) f$$

pour tout $d \in (\mathbf{Z}/N\mathbf{Z})^*$, i. e.

$$f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z) \quad \text{pour tout} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

(Noter que, si ε et k n'étaient pas de même parité, cette formule entraînerait $f = 0$.)

Toute forme modulaire de poids k sur $\Gamma_1(N)$ est combinaison linéaire de formes de types (k, ε_i) sur $\Gamma_0(N)$, où les ε_i sont les différents caractères de $(\mathbf{Z}/N\mathbf{Z})^*$ de même parité que k.

Cela se voit (*cf.* [16], p. IV-13) en remarquant que l'application

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod N$$

définit par passage au quotient un isomorphisme de $\Gamma_0(N)/\Gamma_1(N)$ sur $(\mathbf{Z}/N\mathbf{Z})^*$.

1.6. Opérateurs de Hecke. — Soit $f = \sum a_n q^n$ une forme modulaire de type (k, ε) sur $\Gamma_0(N)$, et soit p un nombre premier. On pose

$$f \mid T_p = \sum a_{pn} q^n + \varepsilon(p) p^{k-1} \sum a_n q^{pn} \quad \text{si} \quad p \nmid N, \tag{1.6.1}$$

$$f \mid U_p = \sum a_{pn} q^n \quad \text{si} \quad p \mid N. \tag{1.6.2}$$

On obtient ainsi une autre forme modulaire de type (k, ε) sur $\Gamma_0(N)$, qui est parabolique si f l'est.

1.7. Formes primitives. — On renvoie à [2] (dans le cas $\varepsilon = 1$) et à [6], [12], [13] (dans le cas général) pour la définition des formes paraboliques *primitives* (« newforms ») de type (k, ε) sur $\Gamma_0(N)$.

Si $f = \sum_{n=1}^{\infty} a_n q^n$ est une telle forme, on a $a_1 = 1$, et f est fonction propre des opérateurs de Hecke T_p et U_p, les valeurs propres correspondantes étant les a_p. Il en résulte que la série de Dirichlet

$$\Phi_f(s) = \sum a_n n^{-s} \tag{1.7.1}$$

admet le développement eulérien

$$\Phi_f(s) = \prod_{p \mid N} \frac{1}{(1 - a_p p^{-s})} \prod_{p \nmid N} \frac{1}{(1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s})}. \tag{1.7.2}$$

1.8. Si f est comme ci-dessus, et si $p \mid N$, la valeur absolue de a_p est donnée par la règle suivante ([12], [14]) :

$a_p = 0$ si $p^2 \mid N$ et si ε peut être défini mod N/p;

$|a_p| = p^{(k-1)/2}$ si ε ne peut pas être défini mod N/p;
$|a_p| = p^{k/2-1}$ si $p^2 \nmid N$ et si ε peut être défini mod N/p.

(Il résultera du théorème 4.6 ci-après que le dernier cas ne se présente pas pour $k = 1$.)

1.9. Toute forme f de type (k, ε) sur $\Gamma_0(N)$ peut s'écrire

$$f(z) = E(z) + \sum \lambda_i f_i(d_i z),$$

où E est une série d'Eisenstein, et où f_i est parabolique primitive de type (k, ε) sur $\Gamma_0(N_i)$, N_i étant un diviseur de N tel que ε puisse être défini mod N_i, et d_i un diviseur de N/N_i. De plus, cette décomposition est unique, en un sens évident.

§ 2. Rappels (géométriques) sur les formes modulaires

2.1. Soient k et N des entiers $\geqq 1$, et μ_N le schéma en groupes des racines N-ièmes de l'unité. Du point de vue géométrique, une forme modulaire de poids k sur $\Gamma_1(N)$ est une loi qui, à chaque courbe elliptique E munie d'un plongement $\alpha : \mu_N \to E$, associe une section de la puissance tensorielle k-ième $\omega_E^{\otimes k}$ de ω_E, où ω_E est le dual de l'algèbre de Lie de E.

Précisons :

(*a*) Une *courbe elliptique* sur un schéma S est un morphisme propre et lisse $E \to S$, muni d'une section $e : S \to E$, de fibres géométriques des courbes elliptiques. Lorsque S est le spectre d'un anneau commutatif A, on dit aussi que E est une courbe elliptique sur A. On pose $\omega_E = e^* \Omega^1_{E/S}$; pour S = Spec (A), ω_E s'identifie à un A-module inversible.

(*b*) Soit R un anneau commutatif dans lequel N est inversible. Une *forme modulaire* de poids k sur $\Gamma_1(N)$, méromorphe à l'infini, définie sur R, est une loi qui, à toute courbe elliptique E sur une R-algèbre A, munie d'un plongement $\alpha : \mu_N \to E$, associe un élément $f(E, \alpha)$ de $\omega_E^{\otimes k}$. On exige que cette loi soit compatible aux isomorphismes, et à l'extension des scalaires.

(*c*) On dit que f est *holomorphe à l'infini* si elle se prolonge en une loi $\tilde{f}$ définie pour les couples (E, α) où E est une *courbe elliptique généralisée* ([7], II.1.12) et α un plongement de μ_N dans E dont l'image rencontre chaque composante irréductible de chaque fibre géométrique ([7], IV.4.14). Si elle existe, la loi $\tilde{f}$ est unique.

Supposons que R soit un corps. On dit que f est *parabolique* si elle est holomorphe à l'infini et si $\tilde{f}(E, \alpha) = 0$ chaque fois que E est une courbe elliptique dégénérée (i. e. non lisse) sur une extension algébriquement close de R.

Ces notions pourraient aussi se définir en termes de développements de Laurent en q (*cf.* [7], VII, § 3).

2.2. Soit f comme ci-dessus. Si $d \in (\mathbf{Z}/N\mathbf{Z})^*$, on définit la forme modulaire $f \mid R_d$ par

$$(f \mid R_d)(E, \alpha) = f(E, d\alpha). \tag{2.2.1}$$

Si ε est un homomorphisme de $(\mathbf{Z}/N\mathbf{Z})^*$ dans R^*, on dit que f est *de type* (k, ε) *sur* $\Gamma_0(N)$ si $f \mid R_d = \varepsilon(d) f$ pour tout $d \in (\mathbf{Z}/N\mathbf{Z})^*$.

2.3. Soit p un nombre premier ne divisant pas N. L'opérateur de Hecke T_p est alors défini sur les espaces de formes modulaires. Si f est une telle forme, et si (E, α) est définie sur un corps algébriquement clos de caractéristique $\neq p$, on a

$$(f \mid T_p)(E, \alpha) = \frac{1}{p} \sum_{\varphi} \varphi^*(f(\varphi E, \varphi \circ \alpha)),$$

où φ parcourt les classes d'isogénies de degré p de source E (deux isogénies étant dans la même classe si leurs noyaux sont égaux).

Les T_p commutent entre eux, et commutent aux R_d.

2.4. Faisons $R = \mathbf{C}$. La donnée de $\alpha : \mu_N \to E$ équivaut alors à celle du point

$$\alpha(\exp(2\pi i/N)),$$

qui est d'ordre N. A une forme modulaire f comme ci-dessus, on associe une fonction (encore notée f) sur le demi-plan H par la règle

$$f(z) = f(E_z, 1/N)/(2\pi i du)^{\otimes k}, \tag{2.4.1}$$

où E_z désigne la courbe elliptique $\mathbf{C}/(\mathbf{Z} \oplus z\mathbf{Z})$.

Posons $f(z) = f_\infty(e^{2\pi i z})$. La formule (2.4.1) se récrit :

$$f_\infty(q) = f(\mathbf{C}^*/q^{\mathbf{Z}}, \mathrm{Id})/(dt/t)^{\otimes k} \qquad (0 < |q| < 1), \tag{2.4.2}$$

où Id est déduite de l'inclusion de μ_N dans $\mathbf{C}^*$.

Cette construction identifie les espaces de formes modulaires au sens de 2.1 et 2.2 aux espaces de même nom du § 1; même chose pour les opérateurs T_p et R_d.

2.5. Pour la définition de la *courbe de Tate* $\mathbf{G}_m/q^{\mathbf{Z}}$ sur l'anneau $\mathbf{Z}((q)) = \mathbf{Z}[[q]](q^{-1})$, nous renvoyons à [7], VII, § 1. Cette courbe est munie d'une forme différentielle invariante dt/t, et d'un plongement naturel $\mathrm{Id} : \mu_N \to \mathbf{G}_m/q^{\mathbf{Z}}$. Si f est une forme modulaire de poids k sur $\Gamma_1(N)$, méromorphe à l'infini, et définie sur un anneau R, on pose

$$f_\infty(q) = f(\mathbf{G}_m/q^{\mathbf{Z}}, \mathrm{Id})/(dt/t)^{\otimes k} \in \mathbf{Z}((q)) \otimes R \subset R((q)).$$

(Dans cette formule, $\mathbf{G}_m/q^{\mathbf{Z}}$ désigne la courbe sur $\mathbf{Z}((q)) \otimes R$ déduite de la courbe de Tate par extension des scalaires.)

Posons

$$f_\infty(q) = \sum a_n q^n \qquad \text{et} \qquad (f \mid R_d)_\infty(q) = \sum a_n(d) q^n, \quad d \in (\mathbf{Z}/N\mathbf{Z})^*;$$

si p est un nombre premier ne divisant pas N, on a

$$(f \mid T_p)_\infty(q) = \sum a_{pn} q^n + p^{k-1} \sum a_n(p) q^{np}. \tag{2.5.1}$$

En particulier, si f est de type (k, ε) sur $\Gamma_0(N)$, on a

$$(f \mid T_p)_\infty(q) = \sum a_{pn} q^n + \varepsilon(p) p^{k-1} \sum a_n q^{pn}. \tag{2.5.2}$$

Lorsque $R = \mathbf{C}$, $f_\infty(q)$ est le développement en série de (2.4.2); ceci est prouvé dans [7], VII, § 4 (au moins pour f holomorphe, le seul cas qui nous importe). La formule (2.5.2) redonne (1.6.1).

2.6. Si K est un corps de caractéristique 0, notons S_K l'espace vectoriel des formes modulaires paraboliques de poids k sur $\Gamma_1(N)$ qui sont définies sur K. On a

$$S_K = K \otimes_{\mathbf{Q}} S_{\mathbf{Q}}; \tag{2.6.1}$$

on le voit en interprétant S_K comme l'espace des sections d'un faisceau inversible sur le « champ algébrique » correspondant à $\Gamma_1(N)$ (*cf.* [7], VII, 3.2).

Si K′ est un sous-corps de K, une forme $f \in S_K$ appartient à $S_{K'}$ si et seulement si les coefficients de la série $f_\infty(q)$ appartiennent à K′. Cela se voit en se ramenant au cas où K est algébriquement clos, et en remarquant que, pour tout K′-automorphisme σ de K, les formes f et $\sigma(f)$ ont même développement en série, donc coïncident.

PROPOSITION 2.7. — *Soit* L *l'ensemble des* $f \in S_{\mathbf{C}}$ *telles que* $(f \mid R_d)_\infty(q) \in \mathbf{Z}[[q]]$ *pour tout* $d \in (\mathbf{Z}/N\mathbf{Z})^*$. *Alors* :

(2.7.1) L *est un* $\mathbf{Z}$*-module libre de type fini, stable par les opérateurs* T_p *et* R_d.

(2.7.2) *Pour tout corps* K *de caractéristique* 0, *on a* $S_K = K \otimes L$.

(2.7.3) *Les valeurs propres des* T_p *dans* $S_{\mathbf{C}}$ *sont des entiers d'une extension finie de* $\mathbf{Q}$.

(2.7.4) *Si* $f \in S_{\mathbf{C}} = \mathbf{C} \otimes L$ *est telle que* $f \mid T_p = a_p f$, *alors, pour tout automorphisme* σ *de* $\mathbf{C}$, *la forme* $\sigma(f)$ *est telle que* $\sigma(f) \mid T_p = \sigma(a_p)\sigma(f)$. *Si* f *est de type* (k, ε) *sur* $\Gamma_0(N)$, *alors* $\sigma(f)$ *est de type* $(k, \sigma(\varepsilon))$ *sur* $\Gamma_0(N)$.

Si $f \in S_{\mathbf{Q}}$, on a $f \mid R_d \in S_{\mathbf{Q}}$ pour tout $d \in (\mathbf{Z}/N\mathbf{Z})^*$ et les séries $(f \mid R_d)_\infty(q)$ appartiennent à $\mathbf{Z}[[q]] \otimes \mathbf{Q}$, donc ont des dénominateurs bornés. Il en résulte qu'un multiple non nul de f appartient à L, d'où $\mathbf{Q} \otimes L = S_{\mathbf{Q}}$ et d'après (2.6.1) $K \otimes L = S_K$ pour tout corps K de caractéristique 0. Que L soit de type fini provient de ce que les formes linéaires « n-ièmes coefficients des $(f \mid R_d)_\infty(q)$ » séparent les éléments de $S_{\mathbf{Q}}$.

Le fait que L soit stable par les R_d (resp. les T_p) est évident (resp. résulte de (2.5.1)). Les assertions (2.7.3) et (2.7.4) en résultent.

REMARQUE 2.8. — Le fait que la série $f_\infty(q)$, $f \in S_{\mathbf{Q}}$, soit à dénominateurs bornés a été ici déduit du fait que la courbe de Tate est définie sur $\mathbf{Z}((q)) \otimes \mathbf{Q}$. On aurait également pu utiliser le théorème 3.5.2 de Shimura [24], valable lorsque $k \geqq 2$, et ramener le poids 1 au poids 13 par multiplication par Δ.

§ 3. Rappels sur les représentations galoisiennes

3.1. Soient $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$, et $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Nous aurons à considérer des *représentations linéaires* de G, autrement dit des homomorphismes continus

$$\rho : G \to \mathbf{GL}_n(k),$$

où k est de l'un des types suivants :

(a) le corps $\mathbf{C}$ (avec la topologie discrète);

(b) un corps fini (avec la topologie discrète);

(c) une extension finie d'un corps l-adique $\mathbf{Q}_l$ (avec sa topologie naturelle).

Dans les deux premiers cas, l'image de ρ est *finie*.

Si p est un nombre premier, on dit que ρ est *non ramifiée en p* si elle est triviale sur le groupe d'inertie d'une place de $\overline{\mathbf{Q}}$ prolongeant p. On note alors $F_{\rho,p}$ l'image par ρ de la substitution de Frobenius ([1]) relative à p; c'est un élément de $\mathbf{GL}_n(k)$, défini à conjugaison près. On pose

$$P_{\rho,p}(T) = \det(1 - F_{\rho,p}T) = 1 - \mathrm{Tr}(F_{\rho,p})T + \ldots + (-1)^n \det(F_{\rho,p})T^n. \tag{3.1.1}$$

La connaissance des polynômes $P_{\rho,p}(T)$ permet presque de reconstituer ρ. De façon plus précise :

LEMME 3.2. — *Soit* X *un ensemble de nombres premiers de densité* 1 *et soient* ρ *et* ρ' *deux représentations linéaires semi-simples de* G. *Supposons que, pour tout* $p \in X$, ρ *et* ρ' *soient non ramifiées, et que* $P_{\rho,p}(T) = P_{\rho',p}(T)$ (*resp. que* $\mathrm{Tr}(F_{\rho,p}) = \mathrm{Tr}(F_{\rho',p})$ *lorsque k est de caractéristique* 0). *Alors* ρ *et* ρ' *sont isomorphes.*

Cela résulte du théorème de densité de Čebotarev, combiné avec le fait qu'une représentation linéaire semi-simple d'un groupe est déterminée, à isomorphisme près, par les polynômes caractéristiques (resp. les traces, si la caractéristique du corps est 0) correspondants ([3], § 30.16).

REMARQUES

3.3. Dans la suite, on appliquera le lemme 3.2 au cas particulier où X est l'ensemble des nombres premiers qui ne divisent pas un entier N donné; on dira alors que ρ et ρ' sont *non ramifiées en dehors de* N.

3.4. Lorsque $k = \mathbf{C}$, la condition de semi-simplicité est automatiquement satisfaite, puisque $\rho(G)$ et $\rho'(G)$ sont finis.

§ 4. Résultats

(a) ÉNONCÉ DU THÉORÈME PRINCIPAL

THÉORÈME 4.1. — *Soient* N *un entier* $\geqq 1$, ε *un caractère de Dirichlet* mod N *tel que* $\varepsilon(-1) = -1$, *et f une forme modulaire de type* $(1, \varepsilon)$ *sur* $\Gamma_0(N)$, *non identiquement nulle. On suppose que f est fonction propre des* T_p, $p \nmid N$, *avec pour valeurs propres* a_p.

([1]) Nous adoptons ici les conventions d'Artin [1]. Notre « substitution de Frobenius » est donc l'élément noté φ dans [5]; son inverse est le « Frobenius géométrique ».

Il existe alors une représentation linéaire

$$\rho : G \to \mathbf{GL}_2(\mathbf{C}), \qquad où \quad G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}),$$

qui est non ramifiée en dehors de N *et telle que*

$$(4.1.1) \qquad \mathrm{Tr}(F_{\rho,p}) = a_p \qquad et \qquad \det(F_{\rho,p}) = \varepsilon(p) \quad pour\ tout\ p \nmid N.$$

Cette représentation est irréductible si et seulement si f est parabolique.

La démonstration sera donnée au § 8.

COROLLAIRE 4.2. — *Les valeurs propres a_p sont sommes de deux racines de l'unité; en particulier on a $|a_p| \leqq 2$.*

En d'autres termes, la « conjecture de Ramanujan-Petersson » est vraie en poids 1; on sait d'ailleurs qu'elle est également vraie en poids $\geqq 2$, *cf.* [5], 8.2.

REMARQUES

4.3. D'après le lemme 3.2, la représentation ρ associée à f par 4.1 est unique, à isomorphisme près.

4.4. La formule $\det(F_{\rho,p}) = \varepsilon(p)$ montre que l'on a

$$\det(\rho) = \varepsilon,$$

en convenant d'identifier ε au caractère $G \to \mathbf{C}^*$ qui lui correspond par la théorie du corps de classes (c'est simplement le composé de ε et de l'homomorphisme $G \to (\mathbf{Z}/N\mathbf{Z})^*$ fourni par l'action de G sur les racines N-ièmes de l'unité).

4.5. Notons c l'élément de G correspondant à la conjugaison complexe (pour un plongement de $\overline{\mathbf{Q}}$ dans $\mathbf{C}$). Du fait que ε est impair, 4.4 montre que $\det(\rho(c)) = -1$; comme c est d'ordre 2, cela signifie que $\rho(c)$ *est conjuguée de la matrice* $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(b) CONDUCTEUR D'ARTIN ET FACTEURS LOCAUX. — On conserve les hypothèses et notations du théorème 4.1.

THÉORÈME 4.6. — *Supposons f parabolique primitive, de coefficients a_n, $n \geqq 1$. Soit ρ la représentation de* G *correspondante. Alors* :

a. Le conducteur d'Artin de ρ est égal à N;

b. La fonction L *d'Artin* $L(s, \rho)$ *est égale à* $\Phi_f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$.

(Pour la définition de la série L, et du conducteur, d'une représentation, *voir* [1].)

COROLLAIRE 4.7. — *La représentation ρ est ramifiée en tous les diviseurs premiers de* N.

Cela résulte de (*a*).

COROLLAIRE 4.8. — *La fonction* $L(s, \rho)$ *est une fonction entière.*

[Autrement dit, la « conjecture d'Artin » est vraie pour ρ, *cf.* (c) ci-dessous.]

En effet, la théorie de Hecke montre que $\Phi_f(s)$ est entière.

Démonstration de 4.6. — Elle utilise les *équations fonctionnelles* satisfaites par $\Phi_f(s)$ et $L(s, \rho)$ (comparer avec [9], p. 172-177).

(i) Posons $\tilde{f} = \sum \bar{a}_n q^n$. Du fait que f est primitive, il existe une constante $\lambda \neq 0$ telle que $f(-1/Nz) = \lambda z\tilde{f}(z)$, *cf.* [12] et [13]. Par transformation de Mellin, on en déduit que

$$\Psi_f(1-s) = \mu\tilde{\Psi}_f(s) \qquad \text{avec} \quad \mu = i\lambda/N^{1/2},$$

où

$$\Psi_f(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)\Phi_f(s) \qquad \text{et} \qquad \tilde{\Psi}_f(s) = \Psi_{\tilde{f}}(s).$$

(ii) D'après 4.5, le « facteur à l'infini » de $L(s, \rho)$ est égal à $(2\pi)^{-s}\Gamma(s)$. Si M est le conducteur de ρ, et si l'on pose

$$\xi(s, \rho) = M^{s/2}(2\pi)^{-s}\Gamma(s)L(s, \rho),$$

on a donc

$$\xi(1-s, \rho) = \nu.\xi(s, \bar{\rho}) \qquad \text{avec} \quad \nu \in \mathbf{C}^*.$$

(iii) Posons

$$F(s) = (N/M)^{s/2}\Psi_f(s)/\xi(s, \rho) \qquad \text{et} \qquad \tilde{F}(s) = (N/M)^{s/2}\tilde{\Psi}_f(s)/\xi(s, \bar{\rho}).$$

Les formules ci-dessus montrent que

$$F(1-s) = \omega.\tilde{F}(s) \qquad \text{avec} \quad \omega = \mu/\nu.$$

Mais, si p est un nombre premier ne divisant pas N, les p-facteurs de $\Psi_f(s)$ et de $\xi(s, \rho)$ coïncident d'après 4.1. On a donc

$$F(s) = A^s \prod_{p \mid N} F_p(s),$$

avec

$$A = (N/M)^{1/2} \qquad \text{et} \qquad F_p(s) = (1-a_p p^{-s})/(1-b_p p^{-s})(1-c_p p^{-s}),$$

où $1-a_p p^{-s}$ est le p-facteur de $\Psi_f(s)$ et $(1-b_p p^{-s})(1-c_p p^{-s})$ celui de $\xi(s, \rho)$ (noter que b_p et c_p peuvent être nuls). Tout revient à montrer que A et les F_p sont égaux à 1. On utilise pour cela le lemme élémentaire suivant :

LEMME 4.9. — *Soient* $G(s) = A^s \prod_p G_p(s)$, $H(s) = A^s \prod_p H_p(s)$, *deux produits eulériens finis. Supposons que* :

(4.9.1) $\qquad G(1-s) = \omega.H(s) \qquad$ *avec* $\quad \omega \in \mathbf{C}^*$;

(4.9.2) *Chacun des* G_p *et des* H_p *est produit fini de termes de la forme* $(1-\alpha_p^{(i)} p^{-s})^{\pm 1}$, *avec* $|\alpha_p^{(i)}| < p^{1/2}$.

On a alors $A = 1$ *et* $G_p = H_p = 1$ *pour tout* p.

Si H_p n'est pas égal à 1, la fonction H a une infinité de zéros (ou de pôles) de la forme

$$(\log(\alpha_p^{(i)}) + 2\pi i n)/\log p, \qquad n \in \mathbf{Z},$$

et l'on voit facilement que ceux-ci ne peuvent pas être tous des zéros (ou des pôles) de $G(1-s)$; l'hypothèse $|\alpha_p^{(i)}| < p^{1/2}$ assure en effet qu'aucun des $\alpha_p^{(i)}$ ne peut être égal à un $p/\alpha_p^{(j)}$.

(iv) Il reste encore à vérifier que a_p, b_p, c_p et leurs conjugués satisfont à (4.9.2), i. e. sont $< p^{1/2}$ en valeur absolue. C'est clair pour b_p et c_p qui sont, soit 0, soit des racines de l'unité. Pour a_p, on peut invoquer 1.8 qui montre que $|a_p| \leqq 1$; on peut aussi, si l'on préfère, utiliser l'inégalité de Rankin :

$$|a_n| = O(n^{1/2-1/5}), \quad cf.\ [18];$$

en l'appliquant à $n = p^m$, et en remarquant que $a_n = (a_p)^m$, on en déduit bien

$$|a_p| \leqq p^{1/2-1/5} < p^{1/2}.$$

Cela achève la démonstration de 4.6.

(c) CARACTÉRISATION DES REPRÉSENTATIONS ATTACHÉES AUX FORMES DE POIDS 1. — Reprenons les notations de (*a*), en supposant que la forme f considérée soit parabolique. La représentation

$$\rho : G \to \mathbf{GL}_2(\mathbf{C})$$

correspondante a alors les propriétés suivantes :

(i) ρ est irréductible (4.1);

(ii) $\det \rho$ est un caractère impair (4.4);

(iii) Pour tout caractère continu $\chi : G \to \mathbf{C}^*$, la fonction L d'Artin $L(s, \rho \otimes \chi)$ est une fonction entière [cela résulte de 4.8 appliqué à la forme parabolique

$$f_\chi = \sum \chi(n)\, a_n\, q^n].$$

Réciproquement :

THÉORÈME 4.10. (Weil-Langlands). — *Soit* $\rho : G \to \mathbf{GL}_2(\mathbf{C})$ *une représentation continue du groupe* $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *satisfaisant aux conditions* (i), (ii), (iii) *ci-dessus. Posons*

$$L(s, \rho) = \sum a_n n^{-s}, \qquad f = \sum a_n q^n, \qquad \varepsilon = \det \rho, \qquad N = \text{conduct. } \rho.$$

Alors f *est une forme parabolique primitive de type* $(1, \varepsilon)$ *sur* $\Gamma_0(N)$, *et* ρ *est la représentation attachée à* f.

D'après Langlands (*cf.* [27], p. 152 et 160) les constantes des équations fonctionnelles des séries $\sum a_n \chi(n) n^{-s}$ vérifient l'identité nécessaire pour que l'on puisse appliquer la caractérisation des formes modulaires due à Hecke-Weil ([12], [26]). Il s'ensuit que f est modulaire de type $(1, \varepsilon)$ sur $\Gamma_0(N)$; il est clair que f est fonction propre des T_p et des U_p, et que la représentation qui lui est associée est isomorphe à ρ. D'après 4.1, f est parabolique. Soit f' l'unique forme parabolique primitive (sur un $\Gamma_0(N')$, où N' est un diviseur convenable de N) telle que $f' \mid T_p = a_p f'$ pour $p \nmid N$. Vu 4.6, la série de Dirichlet associée à f' est $L(s, \rho) = \sum a_n n^{-s}$. Il en résulte que $f' = f$, ce qui montre que f est primitive.

REMARQUES

4.11. On trouvera dans [27], p. 163, une généralisation du théorème 4.10 à tous les corps globaux.

4.12. La condition (iii) (conjecture d'Artin pour les $\rho \otimes \chi$) peut être remplacée par la condition plus faible :

(iii') Il existe un entier $M \geqq 1$ tel que, pour tout caractère χ de conducteur premier à M, la fonction $L(s, \rho \otimes \chi)$ soit une fonction entière.

Cela résulte de [26] (*voir* aussi [12]).

4.13. Si la conjecture d'Artin est vraie, les théorèmes ci-dessus fournissent une *bijection* entre « classes de représentations irréductibles de degré 2 de Gal $(\overline{\mathbf{Q}}/\mathbf{Q})$ à déterminant impair » et « formes paraboliques primitives de poids 1 ».

4.14. Le théorème 4.6 donne même un moyen de *vérifier* la conjecture d'Artin dans des cas particuliers. Si l'on se donne une représentation ρ satisfaisant à (i) et (ii), de conducteur N et de déterminant ε, on peut déterminer numériquement les coefficients a_n de la série $L(s, \rho) = \sum a_n n^{-s}$ pour n inférieur à un entier A donné, et l'on peut chercher à construire une forme parabolique primitive f de type $(1, \varepsilon)$ sur $\Gamma_0(N)$ dont le développement commence par $\sum_{n \leqq A} a_n q^n$. Si A est assez grand,

$$\text{par exemple} \quad A \geqq (N/12) \prod_{p \mid N} (1 + p^{-1}),$$

une telle forme est unique, si elle existe (si elle n'existe pas, la conjecture d'Artin est fausse). Une fois f obtenue, il lui correspond une représentation ρ_f; si l'on peut prouver que ρ_f est isomorphe à ρ, il en résulte bien que ρ satisfait à (iii).

EXEMPLES. — Si ρ est comme ci-dessus, l'image de ρ dans le groupe

$$\mathbf{PGL}_2(\mathbf{C}) = \mathbf{GL}_2(\mathbf{C})/\mathbf{C}^*$$

est, soit un groupe diédral, soit l'un des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$ ([22], prop. 16). Dans le cas *diédral*, ρ est induite par une représentation de degré 1 de Gal $(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{d}))$, où $\mathbf{Q}(\sqrt{d})$ est une extension quadratique de $\mathbf{Q}$. La condition (iii) est alors vérifiée, et ρ cor-

respond bien à une forme parabolique; celle-ci est une combinaison linéaire de *séries thêta* pour des formes binaires de discriminant d, *cf.* [9], p. 428-460. Des exemples *non diédraux* ont été construits récemment par Tate (pour N = 133, 229, 283, 331, ...).

Pour l'un de ces exemples (celui où N = 133, qui correspond à un groupe $\mathfrak{A}_4$), Tate, aidé par Atkin *et al.*, a pu mener à bien la méthode esquissée dans 4.14, et prouver l'existence d'une forme modulaire correspondante – donc aussi la conjecture d'Artin pour la représentation en question.

§ 5. Exploitation d'un résultat de Rankin

PROPOSITION 5.1. – *Soit f une forme modulaire parabolique de type (k, ε) sur $\Gamma_0(N)$, non identiquement nulle. On suppose que f est fonction propre des T_p, $p \nmid N$, avec pour valeurs propres a_p. Alors la série $\sum_{p \nmid N} |a_p|^2 p^{-s}$ converge pour s réel $> k$, et l'on a*

$$\sum_{p \nmid N} |a_p|^2 p^{-s} \leqq \log(1/(s-k)) + O(1) \qquad \text{pour} \quad s \to k. \tag{5.1.1}$$

Démonstration 5.2. – On se ramène aussitôt au cas où f est une forme primitive $\sum_{n=1}^{\infty} a_n q^n$. Pour tout $p \nmid N$, soit $\varphi_p \in \mathbf{GL}_2(\mathbf{C})$ tel que $\mathrm{Tr}(\varphi_p) = a_p$ et $\det(\varphi_p) = \varepsilon(p) p^{k-1}$. La série de Dirichlet

$$\Phi_f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

s'écrit alors :

$$\Phi_f(s) = \prod_{p \mid N} (1 - a_p p^{-s})^{-1} \prod_{p \nmid N} \det(1 - \varphi_p p^{-s})^{-1}, \quad \textit{cf.} \ (1.7.2).$$

Posons

$$L(s) = \prod_{p \nmid N} \det(1 - \varphi_p \otimes \bar{\varphi}_p p^{-s})^{-1}.$$

C'est un produit eulérien à quatre facteurs : si l'on note λ_p, μ_p les valeurs propres de φ_p, on a

$$L(s) = \prod_{p \nmid N} [(1 - \lambda_p \bar{\lambda}_p p^{-s})(1 - \lambda_p \bar{\mu}_p p^{-s})(1 - \mu_p \bar{\lambda}_p p^{-s})(1 - \mu_p \bar{\mu}_p p^{-s})]^{-1}.$$

Utilisant la formule $\lambda_p \bar{\lambda}_p \mu_p \bar{\mu}_p = |\varepsilon(p) p^{k-1}|^2 = p^{2k-2}$, on démontre (*cf.* par exemple [10], p. 33, ou [12], [15]) que

$$L(s) = H(s) \zeta(2s - 2k + 2) \left(\sum_{n=1}^{\infty} |a_n|^2 n^{-s} \right),$$

avec

$$H(s) = \prod_{p \mid N} (1 - p^{-2s+2k-2})(1 - |a_p|^2 p^{-s}).$$

D'après [18] (*cf.* aussi [12], [13] et [15]), la série $\sum |a_n|^2 n^{-s}$ converge pour $\mathscr{R}(s) > k$ et son produit par $\zeta(2s - 2k + 2)$ se prolonge en une fonction méromorphe dans tout le

plan complexe, avec pour unique pôle le point $s = k$. Comme $|a_p| < p^{k/2}$ si $p \mid N$ (*cf.* 1.8) la fonction $H(s)$ est holomorphe $\neq 0$ dans $\mathscr{R}(s) \geqq k$. Il résulte de ceci que $L(s)$ est méromorphe dans tout le plan complexe, et holomorphe pour $\mathscr{R}(s) \geqq k$, à la seule exception de $s = k$ qui en est un pôle simple; on a de plus $L(s) \neq 0$ pour s réel $> k$ puisqu'il en est ainsi de $H(s)$, $\zeta(2s-2k+2)$, et $\sum |a_n|^2 n^{-s}$.

Posons

$$g_m(s) = \sum_{p \nmid N} |\mathrm{Tr}(\varphi_p^m)|^2 p^{-ms}/m \qquad \text{et} \qquad g(s) = \sum_{m=1}^{\infty} g_m(s).$$

La série $g(s)$ est une série de Dirichlet à coefficients $\geqq 0$. Pour s assez grand, un calcul immédiat montre qu'elle est égale à $\log L(s)$. Comme $L(s)$ est holomorphe et $\neq 0$ pour s réel $> k$, il résulte d'un lemme classique de Landau ([21], p. 112) que $g(s)$ converge pour $\mathscr{R}(s) > k$. Du fait que $L(s)$ a un pôle simple en $s = k$, on a

$$g(s) = \log(1/(s-k)) + O(1) \qquad \text{pour} \quad s \to k.$$

Mais $g_1(s) = \sum |a_p|^2 p^{-s}$ est évidemment $\leqq g(s)$. On en conclut bien

$$\sum |a_p|^2 p^{-s} \leqq \log(1/(s-k)) + O(1) \qquad \text{pour} \quad s \to k.$$

REMARQUES 5.3. — On peut renforcer la proposition 5.1 de diverses manières. D'abord une fois que l'on dispose de la conjecture de Petersson, une majoration facile montre que la série

$$\sum_{p \nmid N} \sum_{m \geqq 2} |\mathrm{Tr}(\varphi_p^m)|^2 p^{-ms}/m = g_2(s) + g_3(s) + \ldots$$

converge pour $\mathscr{R}(s) \geqq k$, et cela permet de remplacer l'inégalité (5.1.1) par l'égalité :

$$\sum |a_p|^2 p^{-s} = \log(1/(s-k)) + O(1) \qquad \text{pour} \quad s \to k. \tag{5.3.1}$$

D'autre part, un argument à la Hadamard-de la Vallée Poussin montre que $L(s) \neq 0$ pour tout s tel que $\mathscr{R}(s) \geqq k$ (y compris la droite critique $\mathscr{R}(s) = k$), et en appliquant le théorème de Wiener-Ikehara à $L'(s)/L(s)$ on obtient

$$\sum_{p \leqq x} |a_p|^2 p^{-(k-1)} \sim x \qquad \text{pour} \quad x \to \infty, \tag{5.3.2}$$

cf. Rankin [19].

5.4. APPLICATION AUX FORMES DE POIDS 1. — Soient P l'ensemble des nombres premiers et X une partie de P. On pose

$$\text{dens. sup } X = \lim_{s \to 1,\, s > 1} \sup \Big(\sum_{p \in X} p^{-s} \Big) / \log(1/(s-1)). \tag{5.4.1}$$

C'est la *densité supérieure* de X; elle est comprise entre 0 et 1.

PROPOSITION 5.5. — *On conserve les hypothèses de* 5.1, *et l'on suppose en outre que le poids k de f est égal à* 1. *Alors, pour tout* $\eta > 0$, *il existe un ensemble* X_η *de nombres*

premiers et une partie finie Y_η *de* $\mathbf{C}$ *tels que*

$$\text{dens. sup}\, X_\eta \leqq \eta \qquad \textit{et} \qquad a_p \in Y_\eta \quad \textit{pour tout} \quad p \notin X_\eta.$$

D'après 2.7, les a_p sont des entiers d'une extension finie K de $\mathbf{Q}$. Si c est une constante $\geqq 0$, notons $Y(c)$ l'ensemble des entiers a de K tels que $|\sigma(a)|^2 \leqq c$ pour tout plongement σ de K dans $\mathbf{C}$; c'est un ensemble fini. Notons $X(c)$ l'ensemble des p tels que $a_p \notin Y(c)$; il nous suffit de prouver que $\text{dens. sup}\, X(c) \leqq \eta$ si c est assez grand.

Or on sait (2.7) que les $\sigma(a_p)$ sont également valeurs propres des T_p en poids 1. Vu (5.1.1), on a donc

$$\sum_\sigma \sum_p |\sigma(a_p)|^2 p^{-s} \leqq r \log(1/(s-1)) + O(1) \qquad \text{pour} \quad s \to 1,$$

où $r = [K : \mathbf{Q}]$. Comme $\sum_\sigma |\sigma(a_p)|^2 \geqq c$ si $p \in X(c)$, on en conclut que

$$c \sum_{p \in X(c)} p^{-s} \leqq r \log(1/(s-1)) + O(1) \qquad \text{pour} \quad s \to 1,$$

d'où

$$\text{dens. sup}\, X(c) \leqq r/c,$$

et il suffit donc de prendre $c \geqq r/\eta$.

REMARQUE 5.6. — En utilisant (5.3.2) au lieu de (5.1.1) dans la démonstration ci-dessus, on aurait pu remplacer la densité « analytique » (5.4.1) par la densité « naturelle » (*cf.* [21], VI, n° 4.5). De toute façon, 5.5 n'a qu'un intérêt provisoire : une fois le théorème 4.1 démontré, on saura que l'ensemble des a_p est *fini*.

§ 6. **Représentation** *l*-**adiques et réduction** mod *l*

(a) REPRÉSENTATIONS *l*-ADIQUES. — Nous utiliserons le résultat suivant :

THÉORÈME 6.1. — *Soit f une forme modulaire de type* (k, ε) *sur* $\Gamma_0(N)$, *non identiquement nulle. On suppose que* $k \geqq 2$ *et que f est fonction propre des* T_p, $p \nmid N$, *avec pour valeurs propres* a_p. *Soit* K *une extension finie de* $\mathbf{Q}$ *contenant les* a_p *et les* $\varepsilon(p)$, cf. (2.7.3). *Soit* λ *une place finie de* K, *de caractéristique résiduelle l, et soit* K_λ *le complété de* K *en* λ. *Il existe alors une représentation linéaire semi-simple continue*

$$\rho_\lambda : G \to \mathbf{GL}_2(K_\lambda), \qquad \textit{où} \quad G = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}),$$

qui est non ramifiée en dehors de Nl *et telle que*

$$(6.1.1) \qquad \text{Tr}(F_{\rho_\lambda, p}) = a_p \qquad \textit{et} \qquad \det(F_{\rho_\lambda, p}) = \varepsilon(p) p^{k-1} \quad \textit{si} \quad p \nmid Nl.$$

D'après 3.2, la condition (6.1.1) détermine ρ_λ de manière unique, à isomorphisme près.

REMARQUE 6.2. — Si f est une série d'Eisenstein, l'énoncé ci-dessus se déduit immédiatement des résultats de Hecke ([9], p. 690) en prenant pour ρ_λ la somme directe de deux représentations de degré 1. Lorsque f est parabolique, 6.1 est démontré dans un cas particulier dans [4]. Le cas général n'est pas beaucoup plus difficile. Il est traité, par une autre méthode (inspirée de Ihara) et dans un autre langage, par Langlands [11] (où est toutefois admise sans démonstration une « formule des traces » qui semble accessible mais que personne n'a démontrée). Dans un travail futur de l'un de nous, 6.2 sera redémontré par une méthode due à Piateckii-Shapiro [17].

COROLLAIRE 6.3. — *Soient* $(f, N, k, \varepsilon, (a_p))$ *et* $(f', N', k', \varepsilon', (a'_p))$ *comme dans le théorème* 6.1. *Si l'ensemble des nombres premiers* p *tels que* $a_p = a'_p$ *est de densité* 1, *alors* $k = k'$, $\varepsilon = \varepsilon'$ *et* $a_p = a'_p$ *pour tout* $p \nmid NN'$.

En effet, les représentations attachées à f et f' (pour un même choix de K et de λ) sont isomorphes d'après 3.2.

REMARQUES

6.4. L'image de G par ρ_λ est un sous-groupe compact de $\mathbf{GL}_2(K_\lambda)$, donc un *groupe de Lie l-adique*; ce n'est pas un groupe fini.

6.5. Une fois le théorème 4.1 démontré, on voit facilement ([2]) que 6.1 *et* 6.3 *restent valables en poids* 1; toutefois, dans ce cas, l'image du groupe G est un groupe fini.

(b) RÉDUCTION mod l

6.6. Soient $K \subset \mathbf{C}$ un corps de nombres algébriques, λ une place finie de K, $\mathfrak{O}_\lambda$ l'anneau de valuation correspondant, $\mathfrak{m}_\lambda$ son idéal maximal, $k_\lambda = \mathfrak{O}_\lambda/\mathfrak{m}_\lambda$ son corps résiduel, et l la caractéristique de k_λ. Dans ce qui suit, nous écrirons « mod λ » pour « mod $\mathfrak{m}_\lambda$ ».

Soit f une forme modulaire de type (k, ε) sur $\Gamma_0(N)$. On dit que f est λ-*entière* (resp. que $f \equiv 0$ (mod. λ)) si les coefficients de la série $f_\infty(q)$ appartiennent à $\mathfrak{O}_\lambda$ (resp. à $\mathfrak{m}_\lambda$). Supposons f λ-entière; on dit que f est *vecteur propre de* T_p mod λ, *de valeur propre* $a_p \in k_\lambda$, si l'on a

$$f \mid T_p - a_p f \equiv 0 \pmod{\lambda}. \tag{6.6.1}$$

THÉORÈME 6.7. — *Avec les notations précédentes, soit* f *une forme modulaire de type* (k, ε) *sur* $\Gamma_0(N)$, $k \geqq 1$, *à coefficients dans* K. *On suppose que* f *est* λ-*entière*, $f \not\equiv 0$ (mod λ), *et que* f *est vecteur propre des* T_p mod λ, *pour* $p \nmid Nl$, *de valeurs propres* $a_p \in k_\lambda$. *Soit* k_f *le sous-corps de* k_λ *engendré par les* a_p *et les réductions* mod λ *des* $\varepsilon(p)$. *Il existe alors une représentation semi-simple*

$$\rho : G \to \mathbf{GL}_2(k_f)$$

([2]) Cela résulte du fait que la représentation ρ du théorème 4.1 est *réalisable sur* K : son image contient un élément à valeurs propres rationnelles et distinctes (l'élément $\rho(c)$ de 4.5) et cela entraîne que son indice de Schur est 1 (*cf.* [20], IX *a*); elle est donc réalisable sur le corps des valeurs de son caractère.

qui est non ramifiée en dehors de Nl *et telle que, pour tout* $p \nmid Nl$, *on ait*

$$(6.7.1) \qquad \mathrm{Tr}(F_{\rho,p}) = a_p \qquad et \qquad \det(F_{\rho,p}) \equiv \varepsilon(p)\, p^{k-1} \pmod{\lambda}.$$

Démonstration du théorème 6.7

6.8. Soient $(K', \lambda', f', k', \varepsilon', (a'_p))$ comme dans le théorème 6.7, où K' contient K et λ' prolonge λ. Si $a_p \equiv a'_p \pmod{\lambda'}$ et $\varepsilon(p)\, p^{k-1} \equiv \varepsilon'(p)\, p^{k'-1} \pmod{\lambda'}$ pour tout $p \nmid Nl$, le théorème pour f équivaut au théorème pour f'. La seconde condition est vérifiée dès que $\varepsilon = \varepsilon'$ et $k \equiv k' \pmod{(l-1)}$, et elle entraîne la première pourvu que $f \equiv f' \pmod{\lambda'}$.

6.9. RÉDUCTION AU CAS OÙ $k \geqq 2$. — Pour n pair > 2, soit E_n la série d'Eisenstein de poids n sur $\mathbf{SL}_2(\mathbf{Z})$ normalisée pour que son terme constant soit 1. Si l'on choisit n divisible par $l-1$, le développement en série de E_n est l-entier, et $E_n \equiv 1 \pmod{l}$, *cf.* [25]. Le produit $f.E_n$ est donc congru à f mod λ; son poids $k+n$ est congru à k mod $(l-1)$. Vu 6.8, le théorème pour f équivaut au théorème pour $f.E_n$, qui est de poids > 2.

6.10. RÉDUCTION AU CAS OÙ f EST VECTEUR PROPRE DES T_p. — Il suffit de vérifier qu'il existe f' comme en 6.8, avec $(k', \varepsilon') = (k, \varepsilon)$, et vecteur propre des T_p. Cela résulte du lemme suivant, appliqué aux T_p agissant sur le $\mathfrak{O}_\lambda$-module M des formes modulaires de type (k, ε) sur $\Gamma_0(N)$, à coefficients dans $\mathfrak{O}_\lambda$:

LEMME 6.11. — *Soit* M *un module libre de type fini sur un anneau de valuation discrète* $\mathfrak{O}$; *on note* $\mathfrak{m}$ *l'idéal maximal de* $\mathfrak{O}$, k *son corps résiduel,* K *son corps des fractions. Soit* $\mathscr{T}$ *un ensemble d'endomorphismes de* M *commutant deux à deux. Soit* $f \in M/\mathfrak{m}M$ *un vecteur propre commun* (non nul) *des* $T \in \mathscr{T}$, *et soient* $a_T \in k$ *les valeurs propres correspondantes. Il existe alors un anneau de valuation discrète* $\mathfrak{O}'$ *contenant* $\mathfrak{O}$, *d'idéal maximal* $\mathfrak{m}'$ *tel que* $\mathfrak{O} \cap \mathfrak{m}' = \mathfrak{m}$, *et de corps des fractions* K' *fini sur* K, *et un élément non nul* f' *de*

$$M' = \mathfrak{O}' \otimes_{\mathfrak{O}} M,$$

qui est vecteur propre des $T \in \mathscr{T}$, *de valeurs propres* a'_T *telles que* $a'_T \equiv a_T \pmod{\mathfrak{m}'}$. (Noter qu'on n'affirme pas que les *vecteurs propres* se relèvent, mais seulement les *valeurs propres.*)

Soit $\mathscr{H}$ la sous-algèbre de End (M) engendrée par $\mathscr{T}$. Quitte à faire une extension finie des scalaires, on peut supposer que $K \otimes \mathscr{H}$ est un produit d'anneaux artiniens de corps résiduel K. Soit $\chi : \mathscr{H} \to k$ l'homomorphisme tel que $h.f = \chi(h) f$ pour tout $h \in \mathscr{H}$. Puisque $\mathscr{H}$ est libre sur $\mathfrak{O}$, il existe un idéal premier $\mathfrak{p}$ de $\mathscr{H}$ contenu dans l'idéal maximal $\mathrm{Ker}(\chi)$ et tel que $\mathfrak{p} \cap \mathfrak{O} = 0$; c'est le noyau d'un homomorphisme $\chi' : \mathscr{H} \to \mathfrak{O}$ dont la réduction mod $\mathfrak{m}$ est χ. L'idéal de $K \otimes \mathscr{H}$ engendré par $\mathfrak{p}$ appartient au support du module $K \otimes M$; on en conclut qu'il existe un élément non nul f'' de $K \otimes M$ qui est annulé par cet idéal, i. e. tel que $hf'' = \chi'(h) f''$ pour tout $h \in \mathscr{H}$. On prend alors pour f' un multiple non nul de f'' appartenant à M.

Variante. — Se ramener au cas où M est $\mathscr{T}$-indécomposable, et où les valeurs propres des $T \in \mathscr{T}$ appartiennent à K. Montrer qu'il existe alors une base $(e_1, \ldots, e_n)$ de M par rapport à laquelle les éléments T de $\mathscr{T}$ se mettent sous forme de matrices triangulaires supérieures (T_{ij}); utiliser l'indécomposabilité de M pour prouver que l'on a alors $T_{ii} \equiv a_T \pmod{\mathfrak{m}}$ pour tout T et tout i. L'élément $f' = e_1$ répond alors à la question.

6.12. *Fin de la démonstration de* 6.7. — Vu 6.9 et 6.10, on peut supposer que $k \geqq 2$ et que f est vecteur propre des T_p, $p \nmid Nl$; comme T_l commute aux T_p, on peut aussi supposer que f est vecteur propre de T_l si $l \nmid N$. Soit alors

$$\rho_\lambda : G \to \mathbf{GL}_2(K_\lambda)$$

la représentation associée à f par le théorème 6.1. Quitte à remplacer ρ_λ par une représentation isomorphe, on peut supposer que $\rho_\lambda(G)$ est contenu dans $\mathbf{GL}_2(\hat{\mathfrak{O}}_\lambda)$, où $\hat{\mathfrak{O}}_\lambda$ est l'anneau des entiers de K_λ (i. e. le complété de $\mathfrak{O}_\lambda$). Par réduction mod λ on déduit de ρ_λ une représentation

$$\tilde{\rho}_\lambda : G \to \mathbf{GL}_2(k_\lambda).$$

Soit φ la semi-simplifiée de $\tilde{\rho}_\lambda$; c'est une représentation semi-simple, non ramifiée en dehors de Nl, et qui satisfait à (6.7.1). Le groupe $\varphi(G)$ est fini; d'après le théorème de Čebotarev, tout élément de $\varphi(G)$ est de la forme $F_{\varphi,p}$, avec $p \nmid Nl$. Vu la définition de k_f, on a donc :

(6.12.1) Pour tout $s \in \varphi(G)$, les coefficients du polynôme $\det(1 - sT)$ appartiennent à k_f.

L'existence de la représentation $\rho : G \to \mathbf{GL}_2(k_f)$ cherchée résulte alors du lemme suivant :

LEMME 6.13. — *Soit* $\varphi : \Phi \to \mathbf{GL}_n(k')$ *une représentation semi-simple d'un groupe* Φ *sur un corps fini* k'. *Soit* k *un sous-corps de* k' *contenant les coefficients des polynômes* $\det(1 - \varphi(s)T)$, $s \in \Phi$. *Alors* φ *est réalisable sur* k, *i. e. est isomorphe à une représentation* $\rho : \Phi \to \mathbf{GL}_n(k)$.

Pour que φ soit réalisable sur k, il suffit de vérifier que φ est isomorphe à $\sigma(\varphi)$ quel que soit le k-automorphisme σ de k' : cela provient de ce que le groupe de Brauer d'un corps fini est trivial, et qu'il n'y a donc pas « d'indice de Schur » à considérer. Or φ et $\sigma(\varphi)$ ont mêmes polynômes caractéristiques, et sont semi-simples; elles sont donc isomorphes d'après [3], th. 30.16.

§ 7. Majoration des ordres de certains sous-groupes de $\mathbf{GL}_2(\mathbf{F}_l)$

Si l est un nombre premier, on note $\mathbf{F}_l$ le corps $\mathbf{Z}/l\mathbf{Z}$ à l éléments.

7.1. Soient η et M deux nombres positifs. Nous aurons à considérer la propriété suivante d'un sous-groupe G de $\mathbf{GL}_2(\mathbf{F}_l)$:

C(η, M). — Il existe une partie H de Gt elle que $|H| \geqq (1-\eta)|G|$, et que l'ensemble des polynômes $\det(1 - hT)$, $h \in H$, ait au plus M éléments.

(Si X est un ensemble fini, on note $|X|$ son cardinal.)

Nous dirons que G est *semi-simple* si la représentation identique

$$G \to \mathbf{GL}_2(\mathbf{F}_l)$$

est semi-simple.

PROPOSITION 7.2. — *Soient* $\eta < 1/2$ *et* $M \geqq 0$. *Il existe une constante* $A = A(\eta, M)$ *telle que, pour tout nombre premier* l, *et tout sous-groupe semi-simple* G *de* $\mathbf{GL}_2(\mathbf{F}_l)$ *satisfaisant à* $C(\eta, M)$, *on ait* $|G| \leqq A$.

Démonstration. — Soit G un sous-groupe semi-simple de $\mathbf{GL}_2(\mathbf{F}_l)$. Rappelons (*cf.* [22] § 2, prop. 15 et 16) que l'une des conditions suivantes est satisfaite :

(*a*) G contient $\mathbf{SL}_2(\mathbf{F}_l)$;

(*b*) G est contenu dans un sous-groupe de Cartan T;

(*c*) G est contenu dans le normalisateur d'un sous-groupe de Cartan T, et n'est pas contenu dans T;

(*d*) l'image de G dans $\mathbf{PGL}_2(\mathbf{F}_l) = \mathbf{GL}_2(\mathbf{F}_l)/\mathbf{F}_l^*$ est isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.

Nous allons, dans chaque cas, majorer l'ordre de G.

Cas (*a*). — Posons $r = (G : \mathbf{SL}_2(\mathbf{F}_l))$. On a $|G| = rl(l^2-1)$. D'autre part, le nombre des éléments de $\mathbf{GL}_2(\mathbf{F}_l)$ de polynôme caractéristique donné est l^2+l, l^2 ou l^2-l suivant que le polynôme en question a 2, 1, ou 0 racines dans $\mathbf{F}_l$. Si G satisfait à $C(\eta, M)$, on a donc

$$(1-\eta)rl(l^2-1) = (1-\eta)|G| \leqq |H| \leqq M(l^2+l),$$

d'où

$$(1-\eta)r(l-1) \leqq M \qquad \text{et} \qquad l \leqq 1 + \frac{M}{(1-\eta)r} \leqq 1 + \frac{M}{1-\eta};$$

on obtient ainsi une majoration de l, d'où *a fortiori* une majoration de $|G|$.

Cas (*b*). — Au plus 2 éléments de T ont un polynôme caractéristique donné. L'hypothèse $C(\eta, M)$ (avec $\eta < 1$) entraîne donc

$$(1-\eta)|G| \leqq 2M,$$

d'où la majoration

$$|G| \leqq \frac{2M}{1-\eta}.$$

Cas (*c*). — Le groupe $G' = G \cap T$ est d'indice 2 dans G. Si G satisfait à $C(\eta, M)$, G′ satisfait à $C(2\eta, M)$. En appliquant (*b*) à G′, on obtient

$$|G| \leqq \frac{4M}{1-2\eta}.$$

Cas (*d*). — L'image de G dans $\mathbf{PGL}_2(\mathbf{F}_l)$ est d'ordre au plus 60. Le groupe

$$G \cap \mathbf{SL}_2(\mathbf{F}_l)$$

est donc d'ordre au plus 120, et il y a dans G au plus 120 éléments de déterminant donné, et *a fortiori* de polynôme caractéristique donné. Si G satisfait à $C(\eta, M)$, on a donc

$$(1-\eta)|G| \leqq 120M, \qquad \text{d'où} \quad |G| \leqq \frac{120M}{1-\eta}.$$

§ 8. **Démonstration du théorème** 4.1

On peut supposer que la forme modulaire f considérée est, soit une série d'Eisenstein, soit une forme parabolique.

8.1. Si f est une *série d'Eisenstein*, il existe des caractères χ_1 et χ_2 de $(\mathbf{Z}/N\mathbf{Z})^*$ tels que $\chi_1 \cdot \chi_2 = \varepsilon$ et que $a_p = \chi_1(p) + \chi_2(p)$ pour $p \nmid N$ (*cf.* [9], p. 690). On prend alors pour ρ la représentation réductible

$$\rho = \chi_1 \oplus \chi_2,$$

où les χ_i sont identifiés à des représentations de degré 1 de G, *cf.* 4.4.

8.2. A partir de maintenant, on suppose que f est *parabolique*. D'après 2.7, les a_p et les $\varepsilon(p)$ appartiennent à l'anneau des entiers $\mathfrak{O}_K$ d'un corps de nombres K, que l'on peut supposer galoisien sur $\mathbf{Q}$. Soit L l'ensemble des nombres premiers l qui se décomposent complètement dans K. Pour tout $l \in L$, on choisit une place λ_l de K qui prolonge l; le corps résiduel correspondant est égal à $\mathbf{F}_l$. D'après le théorème 6.7, il existe une représentation semi-simple continue

$$\rho_l : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_l),$$

qui est non ramifiée en dehors de Nl, et telle que

$$\det(1 - F_{\rho_l, p} T) \equiv 1 - a_p T + \varepsilon(p) T^2 \pmod{\lambda_l} \quad \text{si} \quad p \nmid Nl.$$

Soit G_l le sous-groupe de $\mathbf{GL}_2(\mathbf{F}_l)$ image de ρ_l.

LEMME 8.3. — *Pour tout* $\eta > 0$, *il existe une constante* M *telle que* G_l *satisfasse à la condition* C(η, M) *de* 7.1 *pour tout* $l \in L$.

D'après la proposition 5.5, il existe une partie X_η de l'ensemble P des nombres premiers telle que dens. sup $X_\eta \leqq \eta$ et que les a_p, pour $p \notin X_\eta$, forment un ensemble fini. Notons $\mathscr{M}$ l'ensemble (fini) des polynômes $1 - a_p T + \varepsilon(p) T^2$, pour $p \notin X_\eta$, et soit $M = |\mathscr{M}|$. *Le groupe* G_l *satisfait à* C(η, M) *pour tout* $l \in L$. En effet, soit H_l le sous-ensemble de G_l formé des éléments de Frobenius $F_{\rho_l, p}$ $p \notin X_\eta$, et de leurs conjugués. D'après le théorème de densité de Čebotarev, on a $|H_l| \geqq (1-\eta)|G_l|$. D'autre part, si $h \in H_l$, le polynôme $\det(1 - hT)$ est la réduction (mod λ_l) d'un élément de $\mathscr{M}$, donc appartient à un ensemble à au plus M éléments. La condition C(η, M) est donc bien satisfaite.

LEMME 8.4. — *Il existe une constante* A *telle que* $|G_l| \leqq A$ *pour tout* $l \in L$.

Cela résulte du lemme précédent, et de la proposition 7.2.

8.5. Choisissons une constante A satisfaisant à 8.4. Quitte à agrandir le corps K (ce qui diminue L), on peut supposer qu'il contient toutes les racines n-ièmes de l'unité, pour $n \leqq A$. Soit Y l'ensemble des polynômes $(1 - \alpha T)(1 - \beta T)$, où α et β sont des racines de l'unité d'ordre $\leqq A$. Si $p \nmid N$, pour tout $l \in L$ avec $l \neq p$ il existe $R(T) \in Y$ tel que

$$1 - a_p T + \varepsilon(p) T^2 \equiv R(T) \pmod{\lambda_l}.$$

Comme Y est fini, il existe un R tel que la congruence ci-dessus soit satisfaite pour une infinité de l, et l'on a donc l'égalité

$$1-a_p T+\varepsilon(p)T^2 = R(T),$$

autrement dit *les polynômes* $1-a_p T+\varepsilon(p)T^2$ *appartiennent à* Y.

8.6. Soit L' l'ensemble des $l \in L$ tels que $l > A$ et que R, S $\in$ Y, R $\neq$ S entraîne R $\not\equiv$ S (mod λ_l); l'ensemble L—L' est fini, donc L' est infini. Soit $l \in L'$. L'ordre du groupe G_l est premier à l. Il en résulte, par un argument standard, que la représentation identique $G_l \to \mathbf{GL}_2(\mathbf{F}_l)$ est la réduction mod λ_l d'une représentation $G_l \to \mathbf{GL}_2(\mathfrak{O}_{\lambda_l})$, où $\mathfrak{O}_{\lambda_l}$ est l'anneau de la valuation λ_l. En composant cette dernière avec l'application canonique $G \to G_l$, on obtient une représentation

$$\rho : G \to \mathbf{GL}_2(\mathfrak{O}_{\lambda_l}).$$

Par construction, ρ est non ramifiée en dehors de Nl. Si $p \nmid Nl$, les valeurs propres de l'élément de Frobenius $F_{\rho,p}$ sont des racines de l'unité d'ordre $\leqq A$ (puisque l'image de ρ est isomorphe à G_l, donc d'ordre $\leqq A$); d'où $\det(1-F_{\rho,p}T) \in Y$. D'autre part, puisque la réduction de ρ mod λ_l est ρ_l, on a

$$\det(1-F_{\rho,p}T) \equiv 1-a_p T+\varepsilon(p)T^2 \pmod{\lambda_l}.$$

Mais les deux polynômes $\det(1-F_{\rho,p}T)$ et $1-a_p T+\varepsilon(p)T^2$ appartiennent à Y. Comme ils sont congrus (mod λ_l), ils sont égaux, et l'on a

$$\det(1-F_{\rho,p}T) = 1-a_p T+\varepsilon(p)T^2 \quad \text{pour tout } p \nmid Nl.$$

Remplaçons maintenant l par un autre nombre premier l' de L'. On obtient une représentation $\rho' : G \to \mathbf{GL}_2(\mathfrak{O}_{\lambda_{l'}})$ ayant la même propriété que ci-dessus, mais pour $p \nmid Nl'$. En particulier, on a

$$\det(1-F_{\rho,p}T) = \det(1-F_{\rho',p}T) \qquad \text{pour} \quad p \nmid Nll'.$$

D'après le lemme 3.2, ceci entraîne que ρ et ρ' sont isomorphes en tant que représentations dans $\mathbf{GL}_2(K)$, et *a fortiori* en tant que représentations complexes. Il en résulte que ρ est non ramifiée en dehors de N, et que

$$\det(1-F_{\rho,p}T) = 1-a_p T+\varepsilon(p)T^2 \quad \text{pour tout } p \nmid N.$$

8.7. Il reste à montrer que ρ est *irréductible*. Si elle ne l'était pas, elle serait somme de deux représentations de degré 1; celles-ci correspondraient à des caractères χ_1 et χ_2, non ramifiés en dehors de N, tels que $\chi_1 \chi_2 = \varepsilon$ et que

$$a_p = \chi_1(p)+\chi_2(p) \qquad \text{pour} \quad p \nmid N.$$

On aurait alors

$$\sum |a_p|^2 p^{-s} = 2\sum p^{-s} + \sum \chi_1(p)\bar{\chi}_2(p)p^{-s} + \sum \chi_2(p)\bar{\chi}_1(p)p^{-s}.$$

Lorsque s tend vers 1, on a $\sum p^{-s} = \log(1/(s-1))+O(1)$. D'autre part, le caractère $\chi_1\bar{\chi}_2$ est $\neq 1$ (sinon, on aurait $\varepsilon = (\chi_1)^2$ et $\varepsilon(-1) = 1$); il en résulte (*cf.* par exemple [21], VI.4.2) que

$$\sum \chi_1(p)\bar{\chi}_2(p)p^{-s} = O(1) \qquad \text{et} \qquad \sum \chi_2(p)\bar{\chi}_1(p)p^{-s} = O(1).$$

On en tire

$$\sum |a_p|^2 p^{-s} = 2\log(1/(s-1)) + O(1) \qquad \text{pour } s \to 1,$$

ce qui contredit la proposition 5.1, et achève la démonstration.

§ 9. Application aux coefficients des formes modulaires de poids 1

Soit $f = \sum_{n=0}^{\infty} a_n e^{2\pi i n z/M}$, $M \geqq 1$, une forme modulaire de poids 1 sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$.

(a) MAJORATION DES $|a_n|$

THÉORÈME 9.1. — *On a* $|a_n| = O(d(n))$ *pour* $n \to \infty$.

(Rappelons que $d(n)$ désigne le nombre de diviseurs $\geqq 1$ de n.)

COROLLAIRE 9.2. — *On a* $|a_n| = O(n^{\delta})$ *pour tout* $\delta > 0$.

En effet, on sait que $d(n)$ jouit de cette propriété ([8], th. 315).

Démonstration de 9.1. — Si n_0 est un entier $\geqq 1$, $d(n_0 n)/d(n)$ est compris entre 1 et $d(n_0)$. Il revient donc au même de démontrer l'estimation (9.1) pour $f(z)$ ou $f(n_0 z)$, et cela permet de supposer que $M = 1$, i. e. que $f(z+1) = f(z)$. Utilisant 1.5 et 1.9, on est ramené aux deux cas particuliers suivants :

(i) f est une série d'Eisenstein, auquel cas (9.1) résulte de la formule donnant les a_n ([9], p. 475);

(ii) f est une forme parabolique primitive de type $(1, \varepsilon)$ sur $\Gamma_0(N)$, pour N et ε convenables. Dans ce cas, on a même le résultat plus précis :

$$|a_n| \leqq d_N(n) \leqq d(n), \tag{9.3}$$

où $d_N(n)$ est le nombre de diviseurs positifs de n premiers à N. En effet, vu la multiplicativité de a_n et de $d_N(n)$, il suffit de vérifier (9.3) lorsque n est une puissance p^m d'un nombre premier p. Distinguons alors deux cas :

(ii_1) $p \mid N$.

On a $a_n = (a_p)^m$, et le théorème 4.6 montre que a_p est, soit 0, soit une racine de l'unité. On a donc bien

$$|a_n| \leqq 1 = d_N(n).$$

(ii_2) $p \nmid N$.

Si l'on écrit le polynôme $1 - a_p T + \varepsilon(p) T^2$ sous la forme $(1-\lambda T)(1-\mu T)$, on a

$$a_n = \lambda^m + \lambda^{m-1}\mu + \ldots + \lambda\mu^{m-1} + \mu^m.$$

Or, d'après le théorème 4.1, λ et μ sont des racines de l'unité. On a donc bien

$$|a_n| \leqq m+1 = d_N(n).$$

REMARQUE 9.4. — Si $f = \sum b_n e^{2\pi inz/M}$, $M \geqq 1$, est une forme modulaire *parabolique* de poids $k \geqq 2$ sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$, le même argument que ci-dessus (utilisant [5], 8.2) montre que

$$|b_n| = O(n^{(k-1)/2} d(n)) \qquad \text{pour} \quad n \to \infty.$$

(b) ORDRE DE GRANDEUR MAXIMAL DES $|a_n|$. — On sait ([8]), th. 317) que l'ordre de grandeur « maximal » de $d(n)$ est $2^{\log n/\log\log n}$, en ce sens que

$$\limsup \frac{\log d(n) \log\log n}{\log n} = \log 2.$$

Le même résultat vaut pour les $|a_n|$:

PROPOSITION 9.5. — *Si* $f \neq 0$, *on a*

$$\limsup \frac{\log |a_n| \log\log n}{\log n} = \log 2.$$

LEMME 9.6. — *Soit* N *un entier* $\geqq 1$. *Il existe des ensembles* X_N *et* Y_N *de nombres premiers, de densités* > 0, *tels que* :

(*x*) *Pour tout* $p \in X_N$, *on a* $p \equiv 1 \pmod N$ *et* $g | T_p = 2g$ *pour toute forme modulaire* g *de poids* 1 *sur* $\Gamma_1(N)$;

(*y*) *Pour tout* $p \in Y_N$, *on a* $p \equiv -1 \pmod N$ *et* $g | T_p = 0$ *pour toute forme modulaire* g *de poids* 1 *sur* $\Gamma_1(N)$.

Soient $\rho_1, \ldots, \rho_h$ les représentations de G associées aux différents systèmes de valeurs propres des T_p agissant sur les formes de type $(1, \varepsilon)$ sur $\Gamma_0(N)$, où ε parcourt les caractères impairs de $(\mathbf{Z}/N\mathbf{Z})^*$. Soit X_N l'ensemble des $p \equiv 1 \pmod N$ tels que $F_{\rho_i,p} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ pour $i = 1, \ldots, h$, et soit Y_N l'ensemble des $p \equiv -1 \pmod N$ tels que $F_{\rho_i,p}$ soit conjugué de $\rho_i(c)$, *cf.* 4.5. D'après le théorème de densité de Čebotarev, X_N et Y_N ont des densités > 0. Si $p \in X_N$, 2 est la seule valeur propre de T_p; comme T_p est semi-simple, on a bien $g | T_p = 2g$ pour tout g. Le même argument montre que $g | T_p = 0$ si $p \in Y_N$ puisque la trace de la matrice $\rho_i(c)$ est 0.

Démonstration de 9.5. — On se ramène comme dans (a) au cas où f est une forme modulaire de poids 1 sur $\Gamma_1(N)$. Soit X_N comme dans le lemme 9.6, et choisissons un entier m tel que $a_m \neq 0$. Si x est un entier $\geqq 1$, notons $p_1, \ldots, p_{i(x)}$ les différents nombres premiers $p \in X_N$ qui sont $\leqq x$ et ne divisent pas m. Posons $n(x) = m p_1 p_2 \ldots p_{i(x)}$. Puisque les p_i appartiennent à X_N, on a $f | T_{p_i} = 2f$ et $f | R_{p_i} = f$; vu (2.5.1), cela entraîne

$$a_{n(x)} = 2^{i(x)} a_m,$$

d'où

$$\log |a_{n(x)}| \sim i(x) \log 2 \qquad \text{pour} \quad x \to \infty.$$

Si c est la densité de X_N, on a $i(x) \sim cx/\log x$, et $\sum_{i \leqq i(x)} \log p_i \sim cx$. On en déduit

$$\log |a_{n(x)}| \sim cx \log 2/\log x,$$
$$\log n(x) \sim cx,$$
$$\log \log n(x) \sim \log x,$$

d'où l'inégalité

$$\limsup \frac{\log |a_n| \log \log n}{\log n} \geqq \log 2.$$

L'inégalité opposée résulte de ce que $|a_n| = O(d(n))$.

(c) ORDRE DE GRANDEUR NORMAL DE $|a_n|$. — L'ordre de grandeur « normal » (i.e. le plus fréquent) de $d(n)$ est $2^{\log\log n}$ (*cf.* [8], th. 432). Celui de $|a_n|$ est plus petit :

PROPOSITION 9.7. — *L'ensemble des n tels que $a_n = 0$ a pour densité* 1.

(Une partie S de N est dite de densité c si le nombre d'éléments de S qui sont $\leqq x$ est égal à $cx + o(x)$ pour $x \to \infty$.)

Ici encore, on peut supposer que f est une forme modulaire de poids 1 sur $\Gamma_1(N)$. Soit Y_N comme dans le lemme 9.6. Si $p \in Y_N$, on a $f|T_p = 0$ et $f|R_p = -f$. Vu (2.5.1), il en résulte que, si n est un entier divisible par p mais pas par p^2, on a $a_n = 0$. Or, si Y est un ensemble fini de nombres premiers, l'ensemble S_Y des entiers n ayant la propriété ci-dessus (pour au moins un $p \in Y$) a pour densité

$$1 - \prod_{p \in Y} \left(1 - \frac{p-1}{p^2}\right).$$

Du fait que Y_N a une densité > 0, la série $\sum_{p \in Y_N} 1/p$ diverge, et le produit

$$\prod_{p \in Y_N} \left(1 - \frac{p-1}{p^2}\right)$$

a pour valeur 0. On en conclut que la réunion des S_Y, $Y \subset Y_N$, est de densité 1, ce qui démontre la proposition.

REMARQUE 9.8. — Pour tout x, notons $M(x)$ le nombre des $n \leqq x$ tels que $a_n \neq 0$. La proposition 9.7 revient à dire que

$$M(x) = o(x) \qquad \text{pour} \quad x \to \infty.$$

En utilisant le théorème 2 de [23], on peut prouver le résultat plus précis suivant : il existe $\alpha > 0$ tel que

$$M(x) = O(x/\log^{\alpha} x) \qquad \text{pour} \quad x \to \infty.$$

BIBLIOGRAPHIE

[1] E. ARTIN, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren* (*Hamb. Abh.*, vol. 8, 1930, p. 292-306 (Collected Works, p. 165-179)).

[2] A. O. L. ATKIN et J. LEHNER, *Hecke operators on $\Gamma_0(m)$* (*Math. Ann.*, vol. 185, 1970, p. 134-160).

[3] C. CURTIS et I. REINER, *Representation theory of finite groups and associative algebras*, Intersc. Publ., New York, 1962.

[4] P. DELIGNE, *Formes modulaires et représentations l-adiques* (*Séminaire Bourbaki*, vol. 1968/1969, exposé n° 355, *Lect. Notes* 179, Springer, 1971, p. 139-172).
[5] P. DELIGNE, *La conjecture de Weil. I.* (*Publ. Math. I.H.E.S.*, vol. 43, 1974, p. 273-307).
[6] P. DELIGNE, *Formes modulaires et représentations de* **GL**(2) (*Lecture Notes*, n° 349, Springer, 1973, p. 55-105).
[7] P. DELIGNE et M. RAPOPORT, *Les schémas de modules de courbes elliptiques* (*Lecture Notes*, n° 349, Springer, 1973, p. 143-316).
[8] G. H. HARDY et E. M. WRIGHT, *An introduction to the theory of numbers*, 3rd edit., Oxford, 1954.
[9] E. HECKE, *Mathematische Werke* (zw. Aufl.). Vandenhoeck und Ruprecht, Göttingen, 1970.
[10] H. JACQUET, *Automorphic Forms on* **GL**(2), *Part II* (*Lecture Notes*, n° 278, Springer, 1972).
[11] R. P. LANGLANDS, *Modular forms and l-adic representations* (*Lecture Notes*, n° 349, Springer, 1973, p. 361-500).
[12] W. LI, *Newforms and Functional Equations*, Dept. of Maths., Berkeley, 1974 (à paraître aux *Math. Ann.*).
[13] T. MIYAKE, *On automorphic forms on* $\mathbf{GL}_2$ *and Hecke operators* (*Ann. of Maths.*, vol. 94, 1971, p. 174-189).
[14] A. P. OGG, *On the eigenvalues of Hecke operators* (*Math. Ann.*, vol. 179, 1969, p. 101-108).
[15] A. P. OGG, *On a convolution of L-series* (*Invent. Math.*, vol. 7, 1969, p. 297-312).
[16] A. P. OGG, *Modular forms and Dirichlet series*, W. A. Benjamin Publ., New York, 1969.
[17] I. I. PIATECKII-SHAPIRO, *Zeta functions of modular curves* (*Lecture Notes*, n° 349, Springer, 1973, p. 317-360).
[18] R. A. RANKIN, *Contributions to the theory of Ramanujan's function* $\tau(n)$ *and similar arithmetical functions.* I, II (*Proc. Cambridge Phil. Soc.*, vol. 35, 1939, p. 351-372).
[19] R. A. RANKIN, *An* Ω*-result for the coefficients of cusp forms* (*Math. Ann.*, vol. 203, 1973, p. 239-250).
[20] I. SCHUR, *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen* (*Sitz. Pr. Akad. Wiss.*, 1906, p. 164-184 (*Gesam. Abhl.*, I, p. 177-197, Springer, 1973)).
[21] J.-P. SERRE, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970.
[22] J.-P. SERRE, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (*Invent. Math.*, vol. 15, 1972, p. 259-331).
[23] J.-P. SERRE, *Divisibilité des coefficients des formes modulaires de poids entier* (*C. R. Acad. Sci. Paris*, t. 279, série A, 1974, p. 679-682).
[24] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions* (*Publ. Math. Soc. Japan*, vol. 11, Princeton Univ. Press., 1971).
[25] H. P. F. SWINNERTON-DYER, *On l-adic representations and congruences for coefficients of modular forms* (*Lecture Notes*, n° 350, Springer, 1973, p. 1-55).
[26] A. WEIL, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen* (*Math. Ann.*, vol. 168, 1967, p. 149-156).
[27] A. WEIL, *Dirichlet Series and Automorphic Forms* (Lezioni Fermiane). (*Lecture Notes*, n° 189, Springer, 1971).

(Manuscrit reçu le 9 août 1974.)

Pierre DELIGNE,
I.H.E.S.,
91440 Bures-sur-Yvette
et
Jean-Pierre SERRE,
Collège de France,
75231 Paris-Cedex 05