Cours DEA 2006, 2007 (Résumé)

Marie-France Vignéras

Institut de Mathématiques de Jussieu, Université de Paris 7-Denis Diderot

February 5, 2007

Un caractère de Dirichlet modulo N est un homomorphisme $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ vu comme une application de $\mathbf{Z}$ dans $\mathbf{C}$ nulle sur les entiers non premiers à N et égale à $\varepsilon(n + N\mathbf{Z})$ sinon. Le cours de Colmez a défini les fonctions L p-adiques des caractères de Dirichlet. Le but de ce cours est de définir les fonctions L p-adiques des formes modulaires. Passer de la dimension 1 à la dimension 2. Le cadre général (toute dimension $n \geq 1$) serait fourni par les formes automorphes. Application de la théorie analytique des caractères de Dirichlet à la théorie des nombres:

- Théorème des nombres premiers
- Théorème de la progression arithmétique

(et plus savant: la formule analytique du nombre de classes d'un corps de nombres, la conjecture de Birch et Swinnerton-Dyer d'une courbe elliptique définie sur $\mathbf{Q}$).

On expose le premier chapitre du texte de Mazur-Tate-Teitelbaum. Mais auparavant, il faut savoir ce qu'est une forme modulaire classique pour laquelle on construira une fonction L p-adique.

Formes modulaires au sens classique.

1. Formes holomorphes paraboliques modulaires pour $\Gamma_o(N)$ de caractère ε et de poids $k \geq 2$

2. Equation fonctionnelle de la fonction $L(f, s)$

3. Opérateur de Hecke $T(p)$ pour un nombre premier p

4. Formes primitives

5. Les opérateurs $|_k w_Q$

6. Torsion par un caractère de Dirichlet χ

7. Rationalité, intégralité (admis).

Livre conseillé: Miyake. On a besoin de la théorie des fonctions anaytiques sur $\mathbf{C}$, pour laquelle on conseille de livre de Vogel.

Articles originaux :
Atkin, A., Lehner, J. : Hecke operators on $\Gamma_o(m)$. Math. Ann. 185, 134-160 (1970).
Li W. Newforms and functional equations. Math. Ann. 212, 285-315 (1975).
Atkin A. and Lie W. Twists of Newforms and Pseudo-Eigenvalues of W-operators. Inv. math. 48. 221-243 (1978).

Autres références:
Lang S. Introduction to modular forms. Grundlehren 222. Springer-Verlag 1976 (qui a l'avantage de contenir des symboles modulaires).
Serre J.-P. Cours d'arithmétique. PUF 1970.(excellent pour $SL(2,\mathbf{Z})$ et pour les exemples).
Shimura G. Introduction to the arithmetic of automorphic functions. Iwanami Shoten et Princeton Univ. Press (1971) (la bible).
Diamond F., Shurman F. A first course in modular forms. GTM 228.

1. Formes holomorphes paraboliques modulaires pour $\Gamma_o(N)$ de caractère ε et de poids $k \geq 2$

Proposition 1. *Le demi-plan de Poincaré $\mathcal{H}$ est isomorphe analytiquement au disque unité ouvert D par $z \to w = \frac{z-i}{z+i}$ d'inverse $w \to i\frac{w+1}{-w+1}$.*

On utilise qu'une fonction holomorphe bijective entre deux ouverts de $\mathbf{C}$ a une inverse holomorphe.

Pour $A \in GL(2,\mathbf{R})_+$ et $z \in \mathcal{H}$ on définit l'homographie

$$Az = \frac{az+b}{cz+d}.$$

On a $(A_1A_2)z = A_1(A_2z)$ et

$$\operatorname{Im} Az = \frac{\det A}{|cz+d|^2} \operatorname{Im} z.$$

On pose

$$\rho(A) = \frac{(\det A)^{1/2}}{cz+d}.$$

Proposition 2. *a) Tout automorphisme de $\mathcal{H}$ est une homographie. b) Le groupe des automorphismes de $\mathcal{H}$ est isomorphe à $GL(2,\mathbf{R})_+/\mathbf{R}^* \simeq SL(2,\mathbf{R})/\pm id$.*

La démonstration de a) utilise le lemme de Schwarz (Vogel 89), après s'être ramené à D.

La métrique (hyperbolique) et la mesure

$$ds^2 = \frac{dx^2+dy^2}{y^2}, \quad dv(z) = \frac{dx\ dy}{y^2}$$

sont invariantes par $GL(2,\mathbf{R})_+$ (agissant par homographie).

Proposition 3. *1) Les géodésiques du demi-plan de Poincaré sont les demi-cercles centrés sur $\mathbf{R}$ et les droites perpendiculaires à $\mathbf{R}$.*

2) Entre deux points de $\mathcal{H}\cup\mathbf{R}\cup\infty$ passe une unique géodésique.

3) Soit D l'intérieur d'un triangle sur $\mathcal{H}\cup\infty\cup\mathbf{R}$ dont les cotés sont des géodésiques d'angle $\theta_1,\theta_2,\theta_3$. Alors l'aire de D pour la mesure hyperbolique $y^{-2}\ dx\ dy$ est $\pi-(\theta_1+\theta_2+\theta_3)$.

On renvoie a Miyake (page 13) pour la démonstration.

Soit $k\geq 2$ un entier. Pour $f:\mathcal{H}\to\mathbf{C}$, $A=\begin{pmatrix} a & b \\ c & d\end{pmatrix}$ dans $GL(2,\mathbf{R})_+$ et $z\in\mathcal{H}$, on pose

$$f|_k A(z) = \rho(A)^k f(Az) = (ad-bc)^{k/2}(cz+d)^{-k} f((az+b)/(cz+d)).$$

Si f est holomorphe, alors $f|_k A$ est homolomorphe. On a

$$f|_k(A_1A_2) = (f|_kA_1)|_kA_2,$$

c'est pourquoi A est à droite de f.

Proposition 4. *Soit $N>1$ un entier. La réduction modulo N définit un morphisme surjectif $SL(2,\mathbf{Z})\to SL(2,\mathbf{Z}/N\mathbf{Z})$.*

La démonstration utilise que que si $(c,d,N)=1$, il existe $c'\equiv c, d'\equiv d$ modulo N premiers entre eux.

On définit $\Gamma(N)$, $\Gamma_o(N)$, $\Gamma_1(N)$ comme le noyau de la réduction modulo N et les images inverses des groupes triangulaires supérieurs, strictement triangulaires supérieurs dans $SL(2,\mathbf{Z}/N\mathbf{Z})$. Pour $N=1$, on pose $\Gamma_o(1)=\Gamma_1(1)=SL(2,\mathbf{Z})$. L'application

$$A=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\to a$$

induit un homomorphisme surjectif de $\Gamma_o(N)$ sur $(\mathbf{Z}/N\mathbf{Z})^*$ de noyau $\Gamma_1(N)$. Tout caractère de Dirichlet modulo N, disons $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$, définit un caractère

$$\varepsilon(A) = \varepsilon(a)$$

de $\Gamma_o(N)$ trivial sur $\Gamma_1(N)$. On a $\varepsilon(A)^{-1} = \varepsilon(d)$.

Définition 1. *Soient N un entier ≥ 1, ε un caractère de Dirichlet modulo N, et k un entier ≥ 2. Une forme modulaire parabolique holomorphe de poids $k \geq 2$ et de caractère ε pour le groupe $\Gamma_o(N)$ est une fonction $f : \mathcal{H} \to \mathbf{C}$*

- holomorphe,

- parabolique: $f(z)\,\mathrm{Im}(z)^{k/2}$ est borné sur $\mathcal{H}$,

- modulaire : $f|_k A = \varepsilon(A)^{-1} f$ pour tout $A \in \Gamma_o(N)$.

On dit que N est le niveau de f. On note $\mathcal{C}(N, \varepsilon, k)$ l'espace vectoriel sur $\mathbf{C}$ formé par ces formes.

Remarque 1. Le groupe $GL(2, \mathbf{R})_+$ opère à droite sur l'espace $\mathcal{C}$ des formes holomorphes paraboliques $f : \mathcal{H} \to \mathbf{C}$ de poids k. Pour toute matrice $A \in GL(2, \mathbf{R})_+$, l'holomorphie est respectée par $|_k A$. De même la parabolicité car

$$f|_k A(z)(\mathrm{Im}\, z)^{k/2} = f(Az)(\mathrm{Im}\, Az)^{k/2}.$$

Poour tout caractère de Dirichlet ε modulo N, le groupe $\Gamma_o(N)$ agit à droite sur $\mathcal{C}$ par

$$f|_{\varepsilon,k} A = \varepsilon(A) f|_k A.$$

Noter que $\varepsilon^{-1}(?) = \overline{\varepsilon(?)}$. L'espace des fonctions de $\mathcal{C}$ invariantes par $\Gamma_o(N)$ est $\mathcal{C}(N, \varepsilon, k)$.

Remarque 2. La modularité implique $\varepsilon(-1) = (-1)^k$ si $f \neq 0$. Elle implique aussi

$$f(z+1) = f(z)$$

car $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_o(N)$. Posons

$$q = e^{2i\pi z}$$

L'application $z \to q$ est holomorphe, l'image de $\mathcal{H}$ est le disque unité ouvert privé de l'origine D^*. Il existe une unique fonction holomorphe $g : D^* \to \mathbf{C}$ telle que $g(q) = f(z)$ (Vogel). Son développement de Laurent en $q = 0$ est $g(q) = \sum_{n \in \mathbf{Z}} a_n q^n$ pour des constantes $a_n \in \mathbf{C}$. La fonction g se prolonge en 0 si $a_n = 0$ pour $n < 0$. Alors $g(0) = a_o$ et g est holomorphe sur D. La parabolicité implique $a_o = 0$. Donc

$$f(q) = \sum_{n \geq 1} a_n q^n.$$

Lorsque f est parabolique, $f(q) = O(q)$ lorsque $q \to 0$. Comme $|q| = e^{-2\pi y}$, il existe une constante $C > 0$ telle que

$$|f(x+iy)| \leq e^{-2\pi y} C$$

lorsque y est assez grand.

Proposition 5. *Soit $f = \sum_{n\geq 1} a_n q^n \in \mathcal{C}(N, \varepsilon, k)$. Alors il existe une constante $M > 0$ telle que $|a_n| \leq M n^{k/2}$ pour tout entier $n \geq 1$.*

La démonstration utilise la parabolicité et et la formule

$$a_n = \int_{z_o}^{z_o+1} f(z) e^{-2\pi n z} dz$$

pour $\operatorname{Im} z_o = 1/n$.

Ce n'est pas la meilleure majoration possible. Par Eichler si $k = 2$ et Deligne si $k > 2$, on peut remplacer k par $k-1$ dans la proposition (conséquence des conjectures de Weil sur les variétés algébriques sur les corps finis). Mais elle suffit pour voir que la série de Dirichlet associée à f converge quelque part.

Corollaire 1. *La fonction $L(f, s) = \sum_{n\geq 1} a_n n^{-s}$ converge absolument pour $\Re s > k/2 + 1$.*

On définit de façon analogue la notion de forme modulaire parabolique holomorphe de poids $k \geq 2$ pour le groupe $\Gamma_1(N)$ (pas de caractère). On note $\mathcal{C}(N, k)$ l'espace vectoriel de ces formes.

Théorème 1. *La dimension de $\mathcal{C}(N, k)$ sur $\mathbf{C}$ est finie.*

On l'admet. Cela nous emmenerait trop loin, on n'a pas le temps. Je connais deux preuves, l'une utilisant le théorème de Riemann-Roch pour les surfaces de Riemann, l'autre la formule des traces des opérateurs de Hecke. Elles se trouvent dans Miyake. Pour $SL(2, \mathbf{Z})$, voir Serre, cours d'arithmétique, la preuve utilise Riemann-Roch. Le résultat est pour le poids $k = 4, 6, 8, \ldots$ pair (sinon l'espace est nul),

$$\dim \mathcal{C}(1, k) = [k/12] \text{ sauf si } k \equiv 2 \bmod 12 \text{ ou c'est } [k/12] - 1$$

Pour $k \leq 11$ il n'y a pas de formes paraboliques. Pour $k = 12$, l'espace est de dimension 1. On montrera $a_1 \neq 0$ si $f \neq 0$ est de poids 12 pour $SL(2, \mathbf{Z})$. Le générateur normalisé par $a_1 = 1$ est (Serre, cours d'arithmétique, ch.VII, prop.14):

$$\Delta(z) = (2\pi)^{12} q \prod_{n\geq 1} (1 - q^n)^{24} = \sum_{n\geq 1} \tau(n) q^n = q - 24q^2 + 252q^3 - \ldots$$

La fonction $\tau(n)$ est la fonction de Ramanujan. Ses valeurs sont des entiers et la fonction $\Delta(z)$ ne s'annule pas. Voir Serre cours d'arithmétique (et aussi pour d'autres exemples de formes modulaires, séries d'Eisenstein, séries theta). La question $\tau(n) \neq 0$? est ouverte.

Proposition 6. $\mathcal{C}(N,k) = \oplus_\varepsilon \mathcal{C}(N,\varepsilon,k)$.

La somme est sur les caractères de Dirichlet modulo N. La preuve utilise que $\Gamma_o(N)$ normalise $\Gamma_1(N)$ et la propriété générale:

Proposition 7. *Si un groupe fini commutatif G opère à droite sur un espace vectoriel complexe de dimension finie V, alors*

$$V = \oplus_{\varepsilon:G\to\mathbf{C}^*} V^\varepsilon$$

où $V^\varepsilon = \{v \in V \ vg = \varepsilon(g)v\}$ pour tous les caractères $\varepsilon : G \to \mathbf{C}^*$.

2. Equation fonctionnelle de la fonction $L(f,s)$

On pose

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

On a

$$w_N \begin{pmatrix} a & b \\ c & d \end{pmatrix} w_N^{-1} = \begin{pmatrix} d & -cN^{-1} \\ -bN & a \end{pmatrix},$$

$$(f|_k w_N)(z) = N^{-k/2} z^{-k} f(-1/Nz).$$

Lemme 1. $f \to f|_k w_N$ *est un isomorphisme* $\mathcal{C}(N,\varepsilon,k) \simeq \mathcal{C}(N,\varepsilon^{-1},k)$.

La modularité utilise que w_N normalise $\Gamma_o(N)$. La bijection utilise que $f|_k a\,\mathrm{id} = \mathrm{sign}(a)^k f$ pour une matrice scalaire $a\,\mathrm{id}$ avec $a \in \mathbf{R}^*$, Comme $w_N^2 = -N\,\mathrm{id}$,

$$f|_k w_N|_k w_N = (-1)^k f.$$

La fonction Gamma (à ne pas confondre avec $\Gamma_o(N)$). L'intégrale

$$\int_0^\infty e^{-t} t^{s-1} dt$$

converge absolument pour $s \in \mathbf{C}$ de partie réelle > 0 et définit une fonction holomorphe $\Gamma(s)$ sur cet ouvert. Une intégration par parties

$$\int_0^\infty t^s d(-e^{-t}) = -\int_0^\infty s t^{s-1}(-e^{-t})dt$$

montre

$$\Gamma(s+1) = s\Gamma(s)$$

pour $\Re s > 0$. Un calcul direct montre $\Gamma(1) = 1$, ce qui implique que $\Gamma(n+1) = n!$ pour tout entier $n > 0$.

La formule permet de prolonger la fonction en une fonction méromorphe $\Gamma(s)$ sur $\mathbf{C}$, de pôles simples aux points $s = 0, -1, -2, \ldots$ de résidus

$$\lim_{s\to -n}(s+n)\Gamma(s) = \lim_{s\to -n}\frac{\Gamma(s+n+1)}{s(s+1)\ldots(s+n-1)} = \frac{(-1)^n}{n!}.$$

Proposition 8. *La fonction $\Gamma(s)$ ne s'annule pas.*

On l'admet. Cela se déduit de Vogel 43 exo 9 e) ou de la formule

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

Voir aussi Dieudonné Calcul infinitésimal.

On pose pour $f \in \mathcal{C}(N, \varepsilon, k)$ et pour $s \in \mathbf{C}$ de partie réelle $\Re s > k/2 + 1$,

$$\Lambda(f, s) = (2\pi/\sqrt{N})^{-s}\Gamma(s)L(f, s).$$

Elle admet la représentation intégrale

$$\Lambda(f, s) = \int_0^\infty f(it/\sqrt{N})t^{s-1}dt$$

en utilisant $a^{-s}\Gamma(s) = \int_0^\infty e^{-t}(t/a)^s dt/t = \int_0^\infty e^{-at}t^{s-1}dt$ pour $a > 0$ et

$$f(it/\sqrt{N}) = \sum_{n\geq 1} a_n e^{-2\pi nt/\sqrt{N}}.$$

Théorème 2. *La fonction $\Lambda(f, s)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$ vérifiant l'équation fonctionnelle*

$$\Lambda(f, s) = i^k\Lambda(f|_k w_N, k - s)$$

On coupe l'intégrale en deux parties de 0 à 1 et de 1 à ∞. Comme $e^{-2\pi t/\sqrt{N}}$, l'intégrale de $f(it/\sqrt{N})t^{s-1}$ de 1 à ∞ définit une fonction homolorphe en $s \in \mathbf{C}$. Utilisant la relation

$$i^k(f|_k w_N)(i/t\sqrt{N}) = t^k f(it/\sqrt{N})$$

l'intégrale de 0 à 1 se ramène en une intégrale absolument convergente de 1 à ∞,

$$i^k\int_0^1 f|_k w_N)(i/t\sqrt{N})t^{s-k}dt/t = i^k\int_1^\infty (f|_k w_N)(it/\sqrt{N})t^{k-s}dt/t$$

Sur l'expression

$$\Lambda(f, s) = \int_1^\infty (f(it/\sqrt{N})t^s + i^k(f|_k w_N)(it/\sqrt{N})t^{k-s})dt/t$$

on voit que $\Lambda(f, s)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$, et l' équation fonctionnelle s'obtient avec $f|_k w_N|_k w_N = (-1)^k f$. Comme $\Gamma(s)$ ne s'annule pas, on déduit:

Corollaire 2. *$L(f,s)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$ égale à*

$$L(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^{s-1} dt$$

pour tout $s \in \mathbf{C}$, vérifiant l'équation fonctionnelle

$$(2\pi/\sqrt{N})^{-s}\Gamma(s)L(f,s) = i^k(2\pi/\sqrt{N})^{-k+s}\Gamma(k-s)L(f|_k w_N, k-s).$$

Voir Miyake 4.3 et Diamond page 204, ce qui se passe pour la fonction L d'une forme holomorphe, faiblement modulaire de poids k pour $\Gamma_1(N)$, et $f|_k A$ est holomorphe à l'infini pour tout $A \in SL(2,\mathbf{Z})$, non parabolique.

3. Opérateur de Hecke $T(p)$

Soit p un nombre premier. Pour $f \in \mathcal{C}(N,\varepsilon,k)$, on pose

$$fT(p) = p^{(k/2)-1}[(\sum_{u=0}^{p-1} f|_k \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}) \ + \ \varepsilon(p) f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}].$$

Rappelons que $\varepsilon(p) = 0$ pour $p|N$,

$$f|_k \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix})(z) = f(\frac{z+u}{p}) p^{-k/2}, \quad f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}(z) = f(pz) p^{k/2}.$$

Donc

$$fT(p)(z) = (p^{-1} \sum_{u=0}^{p-1} f(\frac{z+u}{p})) \ + \ \varepsilon(p) p^{k-1} f(pz).$$

Proposition 9. *Soit $f \in \mathcal{C}(N,\varepsilon,k)$. Alors $fT(p)$ appartient à $\mathcal{C}(N,\varepsilon,k)$.*

La preuve repose sur la remarque 1 et un argument général:

Proposition 10. *Si un monoide G (on ne suppose pas qu'il y ait d'inverse) opère sur un espace vectoriel complexe V, si H est un sous-groupe de G et si $g \in G$ a un double classe HgH égale à une union finie disjointe de classes Hg_i pour $1 \leq i \leq n$. Alors pour v fixe par H,*

$$\sum_{i=1}^{n} v g_i$$

ne dépend pas du choix des g_i et est fixe par H.

Les matrices $A \in GL(2,\mathbf{R})_+$ avec $a,b,c,d \in \mathbf{Z}$ et $c|N$ forment un monoide multiplicatif G et $\varepsilon(A) := \varepsilon(a)$ est un homomorphisme de monoides car

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}\begin{pmatrix} a' & b' \\ Nc' & d' \end{pmatrix} = \begin{pmatrix} aa'+Nbc' & * \\ N(ca'+ac') & * \end{pmatrix}.$$

Le monoide G agit sur l'espace $\mathcal{C}$ des fonctions holomorphes paraboliques de poids k sur $\mathcal{H}$ par

$$f|_{\varepsilon,k}A = \det A^{k/2-1}\varepsilon(A)f|_k A = (ad-bc)^{k-1}\varepsilon(a)(cz+d)^{-k}f(\frac{az+b}{cz+d}).$$

On a $f|_{\varepsilon,k}AA' = (f|_{\varepsilon,k}A)|_{\varepsilon,k}A'$. On applique la proposition

La double classe $\Gamma_o(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_o(N)$ est contenue dans G et

$$fT(p) = \sum_{A\in\Gamma_o(N)\backslash\Gamma_o(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_o(N)} f|_{\varepsilon,k}A$$

par la proposition suivante, puisque $\varepsilon(A) = \varepsilon(a)$.

Proposition 11. *La double classe $\Gamma_o(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_o(N)$ est l'union disjointe des classes $\Gamma_o(N)\begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}$ pour $0 \le u \le p-1$ si p divise N; si p ne divise pas n il faut rajouter la classe $\Gamma_o(N)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.*

Pour la disjonction des classes $\Gamma_o(N)$?, on remarquera que les matrices ? sont triangulaires supérieures.

Exhaustivité. Une matrice $A = \begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ dans la double classe appartient à G et $ad - Nbc = p$. On a deux cas:

1) $(a, cN) = 1$, on choisit $B \in \Gamma_o(N)$ de seconde ligne $(-cN, a)$ telle que $BA = \begin{pmatrix} 1 & b' \\ 0 & p \end{pmatrix}$ pour un entier b'. Si $b' + yp = u$ avec $0 \le u \le p-1$, on multiplie à gauche par $C = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in \Gamma_o(N)$, et $CBA = \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}$.

Si $p|N$, on a fini car alors $(a,p) = 1$ donc $(a, cN)\neq p$. On est dans le cas 1).

2) p ne divise pas N et $(a, cN) = p$ alors $(a, c) = p$; on choisit $B \in \Gamma_o(N)$ de seconde ligne $(-cN/p, a/p)$. On a $BA = \begin{pmatrix} p & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. La proposition est démontrée.

Proposition 12. *Soient p un nombre premier et $f \in \mathcal{C}(N, \varepsilon, k)$. Les coefficients de Fourier de $fT(p) = \sum_{n\geq 1} b_n q^n$ sont reliés à ceux de $f(z) = \sum_{n\geq 1} a_n q^n$ par la relation*

$$b_n = a_{np} + \varepsilon(p)p^{k-1}a_{n/p}$$

avec la convention $a_{n/p} = 0$ si p ne divise pas n.

En utilisant que $\sum_u e^{2i\pi n/p} = 0$ si p ne divise pas n et $= p$ sinon, on voit que

$$fT(p)(z) = \sum_{n\geq 1} a_{np} q^n + \varepsilon(p)p^{k-1} \sum_{n\geq 1} a_n q^{pn}.$$

Corollaire 3. *Les opérateurs de Hecke commutent.*

Il suffit de calculer les coefficients de Fourier de $fT(p)T(q)$ et de $fT_qT(p)$ pour deux nombres premiers distincts et de voir que la formule est symétrique en p, q.

Lemme 2. *Une série formelle dans l'anneau $\mathbf{C}[[X]]$ des séries formelles est inversible si et seulement si son coefficient constant est non nul.*

Preuve. (Bourbaki A IV.28 §4 prop.6). On l'écrit $a(1 - f(X))$ avec $f(X)$ une série formelle divisible par X. Clairement $1 - X$ est inversible d'inverse $1 + X + X^2 + \ldots$ et il existe un $\mathbf{C}$-endomorphisme continu de $\mathbf{C}[[X]]$ tel que $X \to f(X)$. Donc $a(1 - X) \to a(1 + f(X))$ et

$$a^{-1}(1 + f(X) + f(X)^2 + \ldots)$$

est l'inverse de $a(1 + f(X))$.

Soit p un nombre premier et soit $\lambda(p) \in \mathbf{C}$. Le polynôme

$$1 - \lambda(p)X + \varepsilon(p)p^{k-1}X^2$$

est inversible dans l'anneau $\mathbf{C}[[X]]$ des séries formelles, car le coefficient constant est non nul. On note son inverse

$$1 + \lambda(p)X + \lambda(p^2)X^2 + \lambda(p^3)X^3 + \ldots,$$

et $\lambda(1) = 1$. Par identification,

$$(1 - \lambda(p)X + \varepsilon(p)p^{k-1}X^2)(1 + \lambda(p)X + \lambda(p^2)X^2 + \lambda(p^3)X^3 + \ldots) = 1,$$

les coefficients $\lambda(p^n)$ pour $n \geq 2$ vérifient la relation

$$0 = \lambda(p^n) - \lambda(p)\lambda(p^{n-1}) + \varepsilon(p)p^{k-1}\lambda(p^{n+2}).$$

Corollaire 4. *Si f est propre pour $T(p)$ de valeur propre $\lambda(p) \in \mathbf{C}$, alors*

$$a_n = a_m \lambda(p^r)$$

pour tout entier $n = mp^r \geq 1$ avec $(m, p) = 1$

Corollaire 5. *Si f est propre pour $T(p)$ de valeur propre $\lambda(p) \in \mathbf{C}$ pour tout nombre premier p, alors pour tout entier $n = \prod_p p^r \geq 1$, on a*

$$a_n = a_1 \prod_p \lambda(p^r)$$

En particulier $f \neq 0$ si et seulement si $a_1 \neq 0$.

Une fonction $f \in \mathcal{C}(N, \varepsilon, k)$ propre pour $T(p)$ pour tout nombre premier p est dite normalisée si $a_1 = 1$. Alors

$$a(p) = \lambda(p)$$

pour tout nombre premier p, et pour tout entier $r \geq 2$,

$$a_{p^{r+1}} = a_p a_{p^r} - \varepsilon(p) p^{k-1} a_{p^{r-1}}, \text{ et } a_{mn} = a_m a_n \text{ si } (n, m) = 1.$$

Lorsque la dimension de $\mathcal{C}(N, \varepsilon, k)$ est 1, toute fonction non nulle est propre pour tous les opérateurs de Hecke, et son premier coefficient de Fourier est non nul. La fonction normalisée est un générateur canonique. Comme la dimension des formes modulaires paraboliques holomorphes de poids 12 pour $SL(2, \mathbf{Z})$ est 1, on démontre ainsi les relations de Ramanujan

$$\tau(nm) = \tau(n)\tau(m) \text{ si } (n, m) = 1 \text{ et } \tau(p^r) = \tau(p)\tau(p^{r-1}) - p^{11}\tau(p^{r-2})$$

pour tout nombre premier p et tout entier $r \geq 2$.

Proposition 13. *Soit $f \in \mathcal{C}(N, \varepsilon, k)$ propre pour $T(p)$ pour tout nombre premier p et normalisée. Alors pour $s \in \mathbf{C}, \Re s > k/2 + 1$,*

$$L(f, s) = \prod_p (1 - a(p)p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1}.$$

On dit que $L(f, s)$ a un produit Eulérien.

Rappel: $\varepsilon(p) = 0$ si $p|N$.

4. Le produit scalaire de Petersson

On cherche à diagonaliser les opérateurs de Hecke $T(p)$ agissant dans l'espace vectoriel complexe $\mathcal{C}(N, \varepsilon, k)$ de dimension finie. On y arrive pour les $T(p)$ avec p ne divisant par N car on peut munir l'espace d'un produit scalaire hermitien défini positif, pour lesquels ils commutent avec leur adjoints.

5. Produit scalaire de Petersson

Proposition 14. *Le triangle hyperbolique D de sommets $\infty, e^{i\pi/3}, e^{2i\pi/3}$ a la propriété suivante:*

1) Pour tout $z \in \mathcal{H}$ il existe $g \in SL(2,\mathbf{Z})$ tel que $gz \in D$.

2) Soit $z \neq z'$ deux points de D congrus modulo $SL(2,\mathbf{Z})$. On a alors soit $\Re z = \pm 1/2$ et $z' = z \mp 1$, soit $|z| = 1$ et $z' = -1/z$.

3) Le groupe $SL(2,\mathbf{Z})/\pm \mathrm{id}$ est engendré par les images de

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Faire un dessin. Le coté entre $e^{i\pi/3}, e^{2i\pi/3}$ est l'arc du cercle centre 0 de rayon 1, au dessus du segment les joignant. On fait la preuve comme dans Serre. Pour obtenir 3), on montre 1) avec le sous-groupe engendré par les matrices de 3). On en déduit que $SL(2,\mathbf{Z})$ est engendré par les deux matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ car le groupe qu'elles engendrent contient $-\mathrm{id}$. Le triangle hyperbolique D est appelé un domaine fondamental de $SL(2,\mathbf{Z})$ dans $\mathcal{H}$.

Remarque 3. Donc une fonction $f = \sum_n a_n e^{2i\pi n/z}$ holomorphe parabolique sur $\mathcal{H}$ vérifiant $f(z+1) = f(z)$ est modulaire de poids k pour $SL(2,\mathbf{Z})$ si et seulement si elle vérifie $f(-i/t) = i^k y^k f(it)$ pour tout $t > 0$.

L'intégrale de $y^{-2}dxdy$ sur D est finie (elle est majorée par celle sur le demi-cylindre qui est évidemment finie). On peut faire mieux, l'intégrale est l'aire du triangle hyperbolique qui est $\pi/3$ par la proposition 3. C'est le volume de l'espace quotient $SL(2,\mathbf{Z})\backslash\mathcal{H}$. On reste flou sur la notion "d'espace quotient".

Corollaire 6. *Le volume de l'espace quotient $\Gamma\backslash\mathcal{H}$ pour la mesure hyperbolique y^{-2} dx dy est fini pour tout sous-groupe d'indice fini Γ de $SL(2,\mathbf{Z})$.*

On a

$$\mathrm{vol}(\Gamma_o(N)\backslash\mathcal{H}) = [SL(2,\mathbf{Z}) : \Gamma_o(N)]\,\mathrm{vol}(SL(2,\mathbf{Z})\backslash\mathcal{H})$$

(car $-\mathrm{id}$ appartient à $\Gamma_o(N)$). Mieux,

$$\mathrm{vol}(\Gamma_o(N)\backslash\mathcal{H}) = (\pi/3)N\prod_{p|N}(1+p^{-1}).$$

Proposition 15. *Pour $f, g \in \mathcal{C}(N, \varepsilon, k)$, et Γ un sous-groupe d'indice fini de $\Gamma_o(N)$, l'intégrale*

$$(f, g) = \mathrm{vol}(\Gamma\backslash\mathcal{H})^{-1} \int_{\Gamma\backslash\mathcal{H}} f(z)\overline{g(z)}\, y^k\, \frac{dx\, dy}{y^2}$$

est absolument convergente et définit un produit scalaire hermitien défini positif sur l'espace vectoriel complexe $\mathcal{C}(N, \varepsilon, k)$ de dimension finie, indépendant du choix de Γ, appelé le produit scalaire de Petersson.

$f(z)\overline{g(z)}\, y^k$ est invariante par $z \mapsto Az$ pour $A \in \Gamma_o(N)$ et $f(z)\overline{g(z)}\, y^k$ est borné par parabolicité. L'introduction du volume en facteur implique qu'on peut que le choix du sous-groupe d'indice fini Γ de $\Gamma_o(N)$ dans le membre de droite, ne change pas sa valeur.

Proposition 16. *Soit p un nombre premier ne divisant pas N. Alors, l'endomorphisme de $\mathcal{C}(N, \varepsilon, k)$ adjoint de l'opérateur de Hecke $T(p)$ est $\varepsilon(p)^{-1}T(p)$. On a donc pour tout $f, g \in \mathcal{C}(N, \varepsilon, k)$*

$$(fT(p), g) = \varepsilon(p)(f, T(p)g).$$

Si p ne divise pas N, les opérateurs de Hecke $T(p)$ commutent avec leurs adjoints, et commutent entre eux, ils sont normaux. Par le théorème de décomposition spectrale en algèbre linéaire :

Corollaire 7. *Il existe une base de $\mathcal{C}(N, \varepsilon, k)$ formée de vecteurs propres pour les opérateurs de Hecke $f|_k T(p)$ pour tout nombre premier p ne divisant pas n.*

En particulier, l'espace des formes holomorphes paraboliques modulaires pour $SL(2, \mathbf{Z})$ a une base canonique: les fonctions propres pour tous les opérateurs de Hecke $T(p)$ et normalisées.

Corollaire 8. *Soit p un nombre premier tel que $(p, N) = 1$. Si $\lambda(p)$ est une valeur propre de $T(p)$ dans $\mathcal{C}(N, \varepsilon, k)$, alors $\lambda(p) = \varepsilon(p)\overline{\lambda}(p)$.*

En particulier, les valeurs propres des opérateurs de Hecke $T(p)$ dans l'espace des formes holomorphes parabolique de poids k pour $SL(2, \mathbf{Z})$ sont réelles pour tout nombre premier p.

Pour montrer la proposition, on utilise l'anti-involution de $GL(2, \mathbf{R})_+$ (renverse l'ordre du produit),

$$A \mapsto A^* = (\det A)A^{-1}$$

telle que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Lemme 3. *On a pour $f, g : \mathcal{H} \to \mathbf{C}$ et $w = Az$, on a*

$$f|_k A(z)\ \overline{g(z)}\,\mathrm{Im}(z)^k = f(w)\ \overline{g|_k A^*(w)}\,\mathrm{Im}(w)^k. \qquad (1)$$

Preuve. En effet, $z = A^* w, \det A = \det A^*$.

Le membre de gauche est $f(Az)(cz+d)^{-k} \det A^{k/2}\ \overline{g(z)}\,\mathrm{Im}(z)^k$.

Celui de droite est $f(Az)\ \overline{g(z)}(-c\overline{w}+a)^{-k} \det A^{k/2}\,\mathrm{Im}(w)^k$.

Utiliser $\mathrm{Im}(w) = \mathrm{Im}(z) \det A/((cz+d)(c\overline{z}+d))$ et $(-c\overline{w}+a) = (ad-bc)/(c\overline{z}+d)$.

L'involution permute $\Gamma_o(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_o(N)$ et $\Gamma_o(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_o(N)$.

Lorsque p ne divise pas N, ces classes sont égales (faux pour $p|N$). Cela implique que le nombre (fini) de classes à gauche de la double classe est égal au nombre de classes à droite, donc il existe un même système de représentants pour les classes à droite et à gauche (Miyake lemma 2.7.7).

Argument: $HgH = \cup Hh_i = \cup k_i H$. Montrons $Hh_i \cap k_j H$ est impossible. Sinon $Hh_i \subset \cup_{t \neq j} k_t H$. Or $HgH = Hh_i H$ donc $HgH = \cup_{t \neq j} k_t H$ absurde. On choisit $u_i \in Hh_i \cap k_i H$. On a $Hh_i = Hu_i$ et $k_i H = u_i H$. Gagné.

On en déduit qu'il existe des matrices A telles que

$$\Gamma_o(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_o(N) = \cup_A \Gamma_o(N) A = \cup_A \Gamma_o(N) A^*.$$

Donc $fT(p) = \sum_A f|_{\varepsilon,k} A = \sum_A f|_{\varepsilon,k} A^*$. On a $\varepsilon(A)\varepsilon(A^*) = \varepsilon(p)$ et en multipliant le lemme 3 par $\varepsilon(A)$ on obtient

$$f|_{\varepsilon,k} A(z)\ \overline{g(z)}\,\mathrm{Im}(z)^k = \varepsilon(p) f(w)\ \overline{g|_{\varepsilon,k} A^*(w)}\,\mathrm{Im}(w)^k.$$

La fonction $f|_{\varepsilon,k} A(z)\ \overline{g(z)}\,\mathrm{Im}(z)^k$ est invariante par $\Gamma = \Gamma_o(N) \cap A^{-1}\Gamma_o(N)A$ et bornée sur $\mathcal{H}$. On pose

$$(f|_{\varepsilon,k} A, g)_\Gamma := \mathrm{vol}(\Gamma\backslash\mathcal{H})^{-1} \int_{\Gamma\backslash\mathcal{H}} f|_{\varepsilon,k} A(z)\ \overline{g(z)}\,\mathrm{Im}(z)^k\ dv(z).$$

De même

$$\varepsilon(p)(f, g|_{\varepsilon,k} A^*)_{\Gamma'} := \varepsilon(p)\,\mathrm{vol}(\Gamma'\backslash\mathcal{H})^{-1} \int_{\Gamma'\backslash\mathcal{H}} f(w)\ \overline{g|_{\varepsilon,k} A^*(w)}\,\mathrm{Im}(w)^k\ dv(w)$$

où $\Gamma' = \Gamma_o(N) \cap A^{*-1}\Gamma_o(N)A^* = A\Gamma A^{-1}$. Les volumes sont les mêmes car la mesure hyperbolique est invariante par homographie par $GL(2,\mathbf{R})_+$. On a donc

$$(f|_{\varepsilon,k} A, g)_\Gamma = \varepsilon(p)(f, g|_{\varepsilon,k} A^*)_{\Gamma'}.$$

Les groupes Γ, Γ' dépendent de A. Mais on peut les remplacer par un sous-groupe commun d'indice fini, contenu dans $\Gamma_o(N)$ (à vérifier en exercice).

En sommant sur A, on obtient la formule

$$(\sum_A f|_{\varepsilon,k}A, g) = \varepsilon(p)(f, \sum_A g|_{\varepsilon,k}A^*).$$

Remarque 4. Les opérateurs de Hecke $T(p)$ ne sont pas simultanément diagonalisables dans $\mathcal{C}(N, \varepsilon, k)$ lorsque le caractère de Dirichlet ε n'est pas primitif.

Remarque 5. Pour tout $A \in M(2, \mathbf{Z})$ de déterminant > 0, le sous-groupe $\Gamma := \Gamma_1(N) \cap A^{-1}\Gamma_1(N)A \cap A\Gamma_1(N)A^{-1}$ de $SL(2, \mathbf{Z})$ est d'indice fini. On a

$(f|_kA, g)_\Gamma = (f, g|_kA^*)_\Gamma$ pour $f, g \in C(N, k)$.

6. Formes primitives

Si H est un sous-groupe d'un groupe commutatif G, un caractère $\chi : G/H \to \mathbf{C}^*$ de G/H définit par inflation un caractère $\chi(g) = \chi(gH)$ de G trivial sur H.

Caractère de Dirichlet primitif.

Un caractère de Dirichlet ε modulo N est appelé non primitif s'il est trivial sur le noyau de l'homomorphisme surjectif canonique

$$(\mathbf{Z}/N\mathbf{Z})^* \to (\mathbf{Z}/M\mathbf{Z})^*$$

pour un $M|N, M \neq N$ (lorsque $M = 1$ la convention est que $(\mathbf{Z}/M\mathbf{Z})^*$ est le groupe trivial). Sinon, il est appelé primitif.

Si $N = p^r$ les noyaux des homomorphismes possibles non triviaux forment une suite finie croissante $(1 + p^{r'}\mathbf{Z})/p^r\mathbf{Z}$ modulo p^r pour $r' < r$. On voit que ε est l'inflation d'un unique caractère primitif modulo p^s avec $s \geq p$. On dit que p^s est le conducteur de ε.

Par le lemme chinois, un caractère de Dirichlet ε est un produit $\varepsilon = \prod_p \varepsilon_p$ de caractères de Dirichlet ε_p modulo une puissance d'un nombre premier p. Le caractère ε est primitif si et seulement si chaque ε_p est primitif.

Proposition 17. *Tout caractère de Dirichlet ε modulo N est l'inflation d'un unique caractère de Dirichlet primitif modulo $N'|N$. On dit que N' est le conducteur de ε.*

Le conducteur de ε est le produit des conducteurs des ε_p.

A un caractère de Dirichlet primitif modulo N, on associe la famille de ses inflatés. On dit que N est le conducteur de la famille. Il est

pratique de noter la famille et les caractères de la famille par la même lettre ε. Un caractère de la famille est précisé par son niveau qui est un multiple du conducteur. Un caractère de Dirichlet primitif a moins de zéros qu'un inflaté lorsqu'il est étendu à $\mathbf{Z}$ puisque qu'un inflaté s'annulera sur les nombres premiers divisant son niveau.

Les caractères de Dirichlet arrivent en familles, paramétrées par les caractères de Dirichlet primitifs.

La généralisation de la notion de caractère de Dirichlet primitif est la notion de forme modulaire primitive.

On commence par étendre la notion d'"inflation" aux formes modulaires. Soit ε une famille de caractères de Dirichlet. Soit $N'|N$ multiple du conducteur de ε. Posons pour $M \geq 1$,

$$\delta_M = \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}.$$

Soit ε un caractère de Dirichlet modulo N'.

Proposition 18. *Pour tout entier $M \geq 1$ tel que $N'M|N$,*

$$f \mapsto f|_k\delta_M$$

définit une application linéaire $\mathcal{C}(N', \varepsilon, k) \to \mathcal{C}(N, \varepsilon, k)$ commutant avec les opérateurs de Hecke $T(p)$ pour tout nombre premier p ne divisant pas N.

Rappelons que $f|_k\delta_M = M^{k/2}f(Mz)$. Evidement $f|_k\delta_M$ est holomorphe et parabolique $f|_k\delta_M(z)(\operatorname{Im} z)^{k/2} = f(Mz)(\operatorname{Im} Mz)^{k/2}$ est borné sur $\mathcal{H}$. On a $\mathcal{C}(N'M, \varepsilon, k) \subset \mathcal{C}(N, \varepsilon, k)$ et $f|_k\delta_M \in \mathcal{C}(N'M, \varepsilon, k)$ car

$$\delta_M^{-1}A'\delta_M = \begin{pmatrix} a & M^{-1}b \\ MN'c & d \end{pmatrix} = A, \quad A' = \begin{pmatrix} a & b \\ N'c & d \end{pmatrix} \in \Gamma_o(N'). \tag{2}$$

Donc $\Gamma_o(N'M)$ est contenu dans $\delta_M^{-1}\Gamma_o(N')\delta_M$ et $\varepsilon(A) = \varepsilon(A')$, ce qui implique $f|_k\delta_M|_kA = f|_kA'|_k\delta_M = \varepsilon^{-1}(A')f|_k\delta_M$, i.e. $f|_k\delta_M|_{k,\varepsilon}A = f|_k\delta_M$. L'équivariance par $T(p)$ provient de la formule

$$\delta_M \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix} = \begin{pmatrix} 1 & Mu \\ 0 & p \end{pmatrix} \delta_M$$

et du fait que si p ne divise pas N, lorsque u parcourt les entiers modulo p, il en est de même de Mu.

Définition 2. *Le sous-espace de $\mathcal{C}(N,\varepsilon,k)$ engendré par les formes construites par le lemme pour des niveaux N' divisant strictement N et les entiers $M \geq 1$ tels que $N'M|N$, via la proposition, s'appelle l'espace des formes anciennes. L'orthogonal des formes anciennes de $\mathcal{C}(N,\varepsilon,k)$ pour le produit scalaire de Petersson est l'espace des formes nouvelles. On le note $\mathcal{C}(N,\varepsilon,k)^{nouv}$.*

Lorsque le caractère de Dirichlet ε est primitif, toute forme $f \in \mathcal{C}(N,\varepsilon,k)$ est nouvelle. Toute forme holomorphe parabolique modulaire pour $SL(2,\mathbf{Z})$ est nouvelle. Il existe une caractérisation algébrique des formes nouvelles utilisant la trace, n'utilisant pas le produit scalaire de Petersson.

Posons pour $f \in \mathcal{C}(N,\varepsilon,k)$

$$\mathrm{tr}^N_{N'} f := \sum_A f|_{k,\varepsilon} A$$

où A parcourt un système de représentants de $\Gamma_o(N)\backslash\Gamma_o(N')$.

Exercice 1. 1) On vérifie que $\mathrm{tr}_{N/N'} f$ appartient à $\mathcal{C}(N',\varepsilon,k)$. L'application linéaire $\mathrm{tr}_{N/N'} : \mathcal{C}(N,\varepsilon,k) \to \mathcal{C}(N',\varepsilon,k)$ s'appelle la trace de $\mathcal{C}(N,\varepsilon,k)$ dans $\mathcal{C}(N',\varepsilon,k)$.

2) f est nouvelle si et seulement si $\mathrm{tr}^N_{N/p} f = \mathrm{tr}^N_{N/p} f|_k w_N = 0$ pour tout nombre premier p divisant N tel que N/p est un multiple du conducteur de ε.

(Li, theorem 4 page 298).

Définition 3. *Une forme modulaire parabolique de poids k et de caractère ε pour $\Gamma_o(N)$ est dite primitive si elle est*
- *nouvelle,*
- *propre pour les $T(p)$ pour tout nombre premier p,*
- *normalisée.*

On note $\mathcal{C}(N,\varepsilon,k)^{prim}$ l'ensemble des formes primitives de $\mathcal{C}(N,\varepsilon,k)$.

Corollaire 9. *L'espace des formes anciennes dans $\mathcal{C}(N,\varepsilon,k)$ et l'espace des formes nouvelles sont stables par les opérateurs de Hecke $T(p)$ pour $(p,N)=1$. Ils ont une base formée de vecteurs propres pour les $T(p)$ pour $(p,N)=1$.*

Et même si $p|N$, voir Diamond et Shurman 5.6.2. Si $(p,N)=1$, la proposition implique que les formes anciennes sont stables par $T(p)$. L'adjoint de $T(p)$ pour le produit scalaire de Petersson est $\varepsilon(p)^{-1}T(p)$, donc les formes nouvelles le sont aussi.

Théorème 3. *Multiplicité 1. Soient $f,g \in \mathcal{C}(N,\varepsilon,k)$ propres pour $T(p)$ de même valeurs propres pour tout nombre premier $p \neq p_1,\ldots,p_r$. Si f est nouvelle, alors $g = \lambda f$ pour une constante $\lambda \in \mathbf{C}$.*

Faute de temps la preuve n'a pas été donnee en cours. Elle utilise les lemmes suivants (non donnés en cours). Il est conseillé de les faire à titre d'exercice ou de sauter jusqu'au corollaire 10.

Soit Q un entier ≥ 1 et $\Gamma_o(N,Q)$ le sous-groupe de $\Gamma_o(N)$ formé des matrices $A=\begin{pmatrix} a & bQ \\ cN & d\end{pmatrix}$ avec $a,b,c,d\in\mathbf{Z}, ad-bcQN=1$.

Lemme 4. *Si p est un nombre premier, le groupe $\Gamma_o(N)$ est engendré par $\Gamma_o(N,p)$ et $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ ainsi que par $\Gamma_o(Np)$ et $\begin{pmatrix}1&0\\N&1\end{pmatrix}$.*

L'indice de $\Gamma_o(N,p)$ dans le groupe engendré est au moins p. On vérifie que l'indice de $\Gamma_o(N,p)$ dans $\Gamma_o(N)$ est p si $p|N$ et $p+1$ sinon. Même raisonnement pour $\Gamma_o(Np)$.

Lemme 5. *Soit p est nombre premier tel que $(p,N)=1$. Alors il existe $A,A'\in\Gamma_o(N)$ tel que $\begin{pmatrix}p&1\\0&p\end{pmatrix}=A\begin{pmatrix}1&0\\0&p^2\end{pmatrix}A'$.*

C'est un exercice sur les diviseurs élémentaires. On considère la suite

$$L_1=\begin{pmatrix}p&1\\0&p\end{pmatrix}L_o\subset L_o=\mathbf{Z}\begin{pmatrix}1\\0\end{pmatrix}\oplus N\begin{pmatrix}0\\1\end{pmatrix}\mathbf{Z}\subset L=\mathbf{Z}\begin{pmatrix}1\\0\end{pmatrix}\oplus\mathbf{Z}\begin{pmatrix}0\\1\end{pmatrix}$$

de $\mathbf{Z}$-modules libres. Soient $a|b$ les diviseurs élémentaires de L_1 dans L. Il existe une base (w_1,w_2) de L telleque aw_1,bw_2 est une base de L_1. Comme L_1 n'est contenu ni dans pL ni dans ML pour tout diviseur M de N, et que l'indice $[L:L_1]=Np^2$, on a $a=1,b=Np^2$. On en déduit que pour tout diviseur t de Np^2, le module de base (w_1,tw_2) est l'unique sous-module de L contenant L_1 d'indice t dans L. Donc $\begin{pmatrix}p&1\\0&p\end{pmatrix}L$ a pour base w_1,p^2w_2 et L_o a pour base w_1,Nw_2. On choisit $A,A'\in GL(2,\mathbf{Z})$ tel que $(w_1,w_2)=A,\begin{pmatrix}p&1\\0&p\end{pmatrix}=(w_1,p^2w_2)A'$. On a alors $\begin{pmatrix}p&1\\0&p\end{pmatrix}=A\begin{pmatrix}1&0\\0&p^2\end{pmatrix}A'$. Comme $\det AA'=1$, quitte à remplacer w_2 par $-w_2$ on peut supposer que $A,A'\in SL(2,\mathbf{Z})$. Comme $w_1\in L_o$ on a $A,A'\in\Gamma_o(N)$.

Proposition 19. *Soit p un nombre premier. Si les coefficients de Fourier a_n de $f\in\mathcal{C}(N,\varepsilon,k)$ sont nuls pour tout entier n premier à p, alors f est ancienne ou nulle.*

La condition est $f=g|_k\delta_p$ pour $g=p^{-k/2}\sum_{n\geq 1}a_{np}q^n\in\mathcal{C}$. Pour $A\in\Gamma_o(N,p)$ on a $g|_kA=\varepsilon(A)^{-1}g$ car $\delta_p^{-1}A\delta_p\in\Gamma_o(N)$ et $\varepsilon(A)=\varepsilon(\delta_p^{-1}A\delta_p)$. Par le lemme 4, g appartient aussi à $\mathcal{C}(N,\varepsilon,k)$.

Si $(p,N)=1$ cela implique $f=g=0$. L'argument repose :

$$p\delta_p^{-1}\begin{pmatrix}1&1\\0&1\end{pmatrix}\delta_p=\begin{pmatrix}p&1\\0&p\end{pmatrix}\in\Gamma_o(N)\begin{pmatrix}1&0\\0&p^2\end{pmatrix}\Gamma_o(N)$$

déduit du lemme 5. Agissant par $|_k$ sur g on obtient $g(z)=Cg(z/p^2)$ pour une constante non nulle. On voit sur le développement de Fourier de g que ceci implique $g=0$.

Supposons $p|N$. On a $f|_k\begin{pmatrix}1&0\\N/p&1\end{pmatrix}=f$ car $\begin{pmatrix}1&0\\N/p&1\end{pmatrix}=\delta_p\begin{pmatrix}1&0\\N&1\end{pmatrix}\delta_p^{-1}$. Le lemme 4 implique que $f\in\mathcal{C}(N/p,\varepsilon,k)$ si N/p est multiple du conducteur de e, et $f=0$ sinon. En effet, le lemme implique que $f|_kA=c(A)f$ pour un caractère $c:\Gamma_o(N/p)\to\mathbf{C}^*$ trivial sur $\begin{pmatrix}1&0\\N/p&1\end{pmatrix}$ est égal à ε sur $\Gamma_o(N)$. On vérifie que $c(A)=c(a)$ si $A=\begin{pmatrix}a&pb\\N/pc&d\end{pmatrix}$. Cela implique que c est un caractère de Dirichlet c modulo N/p tel que ε est l'inflaté de c, si $f\neq0$.

On peut remplacer p par un ensemble fini $p_1,\dots,p_r$ de nombres premiers dans la proposition précédente. Autrement dit,

Proposition 20. *Soit $f=\sum_{n\geq1}a_nq^n\in\mathcal{C}(N,\varepsilon,k)$. Si $a_n=0$ pour tout n premier à $p_1\dots p_r$ alors f est ancienne ou nulle.*

Non démontré en cours. Li Corollary 1 page 293, ou Miyake (4.6.8), ou Lang Ch.VIII, §4.

Corollaire 10. *Si $f=\sum_{n\geq1}a_nq^n\in\mathcal{C}(N,\varepsilon,k)^{nouv}$ est propre pour $T(p)$ pour tout nombre premier $p\neq p_1,\dots,p_r$, et si son premier coefficient de Fourier est nul, alors f est ancienne ou nulle.*

Car $a_1=0$ implique $a_n=0$ pour tout n premier à $p_1\dots p_r$.

Le théorème multiplicité 1 peut se montrer ainsi. Soit $\lambda=(\lambda(p)$ la valeur propre de commune de f,g pour $T=(T(p))$ pour $p\neq p_1,\dots,p_r$. On suppose que l'ensemble $p_1,\dots,p_r$ contient les diviseurs premiers de N, que $f=q+\sum_{n\geq2}a_nq^n$. Les espaces propres dans $\mathcal{C}(N,\varepsilon,k)$ pour T sont en somme directe. Les composantes de g dans l'espace ancien et l'espace nouveau sont propres pour T de valeur propre λ. On est ramené à g nouvelle et à g ancienne.

Si $g=\sum_{n\geq1}b_nq^n$ est nouvelle, alors $g-b_1f$ est nouvelle propre pour T et son premier coefficient de Fourier est nul, donc $g-b_1f=0$, par la proposition.

Si g est ancienne, c'est une somme finie $g(z) = \sum h_i(n_i z)$ ou $h_i \in \mathcal{C}(N_i, \varepsilon, k)^{nouv}$ est propre pour T de valeur propre λ, avec $n_i N_i$ divisant N et multiple du conducteur de ε. On peut supposer les h_i propres pour T de valeur propre λ_i car $\mathcal{C}(N_i, \varepsilon, k)^{nouv}$ a une base propre pour T. On sait que $h_i(n_i z)$ reste propre pour T de même valeur propre. Le théorème d'indépendance linéaire des vecteurs propres pour T de valeur propres différentes, montre que l'on peut supposer que $\lambda_i = \lambda$ pour tout i.

Soit $h = \sum_{n\geq 1} c_n T^n \in \mathcal{C}(N', \varepsilon, k)^{nouv}$ propre pour T de valeur propre λ. Si $h \neq 0$ alors $c_1 \neq 0$, le premier coefficient de Fourier de $h - b_1 f$ est donc $h - b_1 f$ est ancienne dans $\mathcal{C}(N, \varepsilon, k)$. Comme h est ancienne, f est ancienne ce qui est absurde.

Corollaire 11. *$\mathcal{C}(N, \varepsilon, k)^{prim}$ est une base de $\mathcal{C}(N, \varepsilon, k)^{nouv}$.*

On suppose que $p_1, \ldots, p_r$ est l'ensemble des diviseurs de N. Il existe une base de $\mathcal{C}(N, \varepsilon, k)^{nouv}$ formée de vecteurs propres pour T. Chaque espace propre pour T est de dimension 1 par le théorème de multiplicité 1. La commutativité des opérateurs de Hecke montre que les vecteurs sont propres pour $T(p)$ pour tout p.

Corollaire 12. *Si ε est primitif, $\mathcal{C}(N, \varepsilon, k)^{prim}$ est une base de $\mathcal{C}(N, \varepsilon, k)$.*

On trouve une base canonique de $\mathcal{C}(N, \varepsilon, k)$ comme conséquence d'un théorème de multiplicité 1 un peu plus fort (Li Corollary 3 page 300).

Théorème 4. *Multiplicité 1. Soient $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$ et $g \in \mathcal{C}(M, \varepsilon, k)^{prim}$ deux formes primitives de même poids et de caractère dans la même famille, propres pour $T(p)$ de même valeur propre pour tout nombre premier $p \neq p_1, \ldots, p_r$ donnés. Alors $g = f$.*

Miyake prouve un résultat un peu plus fort 4.6.19, la preuve utilise les séries de Dirichlet (ce qui est naturel) mais aussi l'estimation de Ramanujan-Petersson (cas 4), c'est tricher ! Diamond et Shurman l'admettent. Le premier cas à considérer est N, M deux nombres premiers distincts, le même caractère ε trivial et le même poids k.

Corollaire 13. *$\mathcal{C}(N, \varepsilon, k)$ a une base canonique: les formes primitives $f \in \mathcal{C}(N', \varepsilon, k)^{prim}$ et leurs inflatées $f(Mz)$ pour tout N', M tel que N' est un multiple du conducteur de ε et MN' divise N.*

Par induction croissante sur N, ces éléments engendrent $\mathcal{C}(N, \varepsilon, k)$. Soit $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$. Les formes $f(Mz)$ sont linéairement indépendantes lorsque $M \in N$ non nul; cela se voit sur les coefficients de Fourier en utilisant que $f(Mz) = q^M + \ldots$. Si fT est propre de valeur propre λ_f pour $T = (T(p))$ avec p ne divisant pas N, alors les espaces propres $\mathcal{C}(N, \varepsilon, k)^{T=\lambda_f}$ pour toute forme primitive de niveau $N'|N$ (de caractère ε et de poids k) sont en somme directe par le théorème de multiplicité un plus fort.

Remarque 6. Le bon théorème de multiplicité 1 serait (dans ce cours): Si f, g sont deux formes holomorphes paraboliques primitives (de niveau, caractère, poids quelconques), propres et de même valeurs propres pour les opérateurs de Hecke $T(p)$ pour tout nombre premier p n'appartenant pas à un ensemble de densité 0 de nombres premiers, alors $f = g$. Cela utilise un théorème de Deligne profond (encore un) reliant les formes modulaires aux représentations des groupes de Galois et le théorème de Cebotarev.

7. Les opérateurs $|_k w_Q$

La référence est Atkin-Li.

Si $f = \sum_{n\geq 1} a_n q^n \in \mathcal{C}(N, \varepsilon, k)$, on pose

$$f_\rho = \sum_{n\geq 1} \overline{a}_n q^n.$$

On a $-\overline{z} = -x + iy \in \mathcal{H}$ et $f_\rho(z) = \overline{f(-\overline{z})}$.

Proposition 21. *Soit $f \in \mathcal{C}(N, \varepsilon, k)$. Alors*
1) $f_\rho \in \mathcal{C}(N, \overline{\varepsilon}, k)$ et $(f_\rho)_\rho = f$.
2) $(fT(p))_\rho = f_\rho T(p)$ pour tout nombre premier p.
3) $(f|_k\delta_M)_\rho = f_\rho|_k\delta_M$ pour tout entier $M \geq 1$.
4) $(f_\rho, g_\rho) = \overline{(g, f)}$.
5) Si f est ancienne, resp. nouvelle, resp. primitive, alors f_ρ est ancienne, resp. nouvelle, resp. primitive.

1) $f_\rho|_k A = (f|_k\delta_{-1}A\delta_{-1}^{-1})_\rho$ pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbf{R})_+$, car $f_\rho|_k A(z) = \overline{f(-\overline{Az})} \det A^{k/2}(-c(-\overline{z}) + d)^{-k}$, $\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \delta_{-1}A\delta_{-1}^{-1}$ a même déterminant que A, et $-\overline{Az} = (a(-\overline{z}) - b)/(-c(-\overline{z}) + d) = \delta_{-1}A\delta_{-1}^{-1}(-\overline{z})$.

On a $\delta_{-1}\Gamma_o(N)\delta_{-1}^{-1} = \Gamma_o(N)$.

2) Rappel: les matrices $A \in GL(2, \mathbf{R})_+$ avec $a, b, c, d \in \mathbf{Z}$ et $c|N$ forment un monoide multiplicatif G et $\varepsilon(A) := \varepsilon(a)$ est un homomorphisme de monoides car

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \begin{pmatrix} a' & b' \\ Nc' & d' \end{pmatrix} = \begin{pmatrix} aa' + Nbc' & * \\ N(ca' + ac') & * \end{pmatrix}.$$

Le monoide G agit sur l'espace $\mathcal{C}$ des fonctions holomorphes paraboliques de poids k sur $\mathcal{H}$ par $f|_{\varepsilon,k}A = \det A^{k/2-1}\varepsilon(A)f|_k A$. Pour $A \in G$, on a $f_\rho|_{k,\overline{\varepsilon}}A = (f|_{k,\varepsilon}\delta_{-1}A\delta_{-1}^{-1})_\rho$.

On a $fT(p) = \sum_A f|_{k,\varepsilon}A$ pour A dans un système de représentants de $\Gamma_o(N)\backslash\Gamma_o(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_o(N)$. Les $\delta_{-1}A\delta_{-1}^{-1}$ forment un autre système de représentants car $\begin{pmatrix}1&0\\0&p\end{pmatrix}$ est fixe par conjugaison par δ_{-1}.

3) δ_M est fixe par conjugaison par δ_{-1} et la formule de 1).

4) Il faut montrer que l'intégrale de $\phi(x,y)dv(z)$ sur $\gamma\backslash\mathcal{H}$, si elle est définie ne change pas si l'on remplace (x,y) par $(-x,y)$. Cela nécessite des arguments subtils de mesure positive, de mesure quotient .... Une mesure positive sur un espace compact est simplement une forme linéaire sur les fonctions continues qui est positive sur les fonctions positives.

5) se déduit de ce qui précède.

On considère maintenant l'isomorphisme $|_k w_N : \mathcal{C}(N,\varepsilon,k) \to \mathcal{C}(N,\overline{\varepsilon},k)$ (lemme 1), qui a joué un rôle dans l'équation fonctionnelle de $L(f,s)$,

$$w_N = \begin{pmatrix}0&-1\\N&0\end{pmatrix}.$$

Rappelons que $(f|_k w_N)(z) = N^{-k/2}z^{-k}f(-1/Nz)$ et w_N normalise $\Gamma_o(N)$ car

$$w_N\begin{pmatrix}a&b\\c&d\end{pmatrix}w_N^{-1} = \begin{pmatrix}d&-cN^{-1}\\-bN&a\end{pmatrix}.$$

On a $w_N^2 = -N\,\mathrm{id}$ donc $(f|_k w_N)|_k w_N = \varepsilon(-1)f$.

Proposition 22. *Soit p un nombre premier tel que $(p,N)=1$. Alors*

a) $fT(p)|_k w_N = \varepsilon(p)(f|_k w_N)T(p)$.

b) $w_N\delta_M = w_{NM}$.

c) $(f|_k w_N, g|_k w_N) = (f,g)$ pour $f,g \in \mathcal{C}(N,\varepsilon,k)$.

Preuve. a) $fT(p)|_k w_N = \sum_A f|_k A|_k w_N$ pas de ε car $(p,N)=1$ et $\varepsilon(\begin{pmatrix}1&u\\0&p\end{pmatrix}) = 1$. La somme est sur un système de représentants de $\Gamma_o(N)\backslash\Gamma_o(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_o(N)$. Or w_N normalise la double classe $\Gamma_o(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_o(N)$ car le conjugué de $\begin{pmatrix}1&0\\0&p\end{pmatrix}$ par w_N appartient à la double classe. Donc $w_N^{-1}Aw_N$ est un autre système de représentants.

$\sum_A f|_k A|_k w_N = \sum_{w_N^{-1}Aw_N} f|_k w_N|_k w_N^{-1}Aw_N$.

Mais $\overline{\varepsilon}(w_N^{-1}\begin{pmatrix}1&u\\0&p\end{pmatrix}w_N) = \overline{\varepsilon}(\begin{pmatrix}p&0\\-uN&1\end{pmatrix}) = \overline{\varepsilon}(p)$. Donc

$f|_k w_N|_k w_N^{-1} A w_N = \varepsilon(p) f|_k w_N|_{k,\overline{\varepsilon}} w_N^{-1} A w_N$.

c) $(f|_k w_N, g) = \varepsilon(-1)(f, g|_k w_N)$ pour $f \in \mathcal{C}(N, \varepsilon, k), g \in \mathcal{C}(N, \overline{\varepsilon}, k)$. En effet, $(f|_k w_N, g)_\Gamma = (f, g|_k w_N^*)_\Gamma$ où $w_N^* = w_N^{-1} \det w_N = -w_N$, pour Γ un sous-groupe d'indice fini de $\Gamma_1(N) \cap w_N^{-1}\Gamma_1(N) w_N$, et de $w_N \Gamma_1(N) w_N^{-1} \cap \Gamma_1(N)$. Comme w_N normalise $\Gamma_1(N))$, on peut prendre $\Gamma = \Gamma_1(N)$. On a $g|_k(-\mathrm{id}) = \varepsilon(-1) g$.

Remarque 7. Si f est ancienne, $f = g|_k \delta_M$ avec $g \in \mathcal{C}(N', \varepsilon, k)$ avec $N'MM' = N$ et $M > 1$, alors $f|_k w_N = g|_k w_{N'} \delta_{M'}$ par b). Si $M' > 1$ alors $f|_k w_N$ est ancienne.

Proposition 23. *Si $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$ est primitive, alors $f|_k w_N = \lambda_N(f) f_\rho$ pour une constante $\lambda_N(f) \in \mathbf{C}^*$, appelée pseudo-valeur propre de f pour $|_k w_N$.*

Preuve. Comme $fT(p) = a_p f$ et $a_p = \varepsilon(p)\overline{a}_p$, on a $f|_k w_N T(p) = \overline{a}(p) f|_k w_N$ pour tout p premier à N.

Comme f_ρ est primitive et a les mêmes valeurs propres que $f|_k w_N$ pour $T(p)$ pour $(p, N) = 1$, par le théorème de de multiplicité 1, $f|_k w_N$ est un multiple de f_ρ.

Donc $f|_k w_N$ est propre pour tous les opérateurs de Hecke $T(p)$ si f est primitive L'équation fonctionnelle relie

$$L(f, s) = \prod_p (1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s})^{-1},$$

$$L(f|_k w_N, s) = \lambda_N(f) \prod_p (1 - \overline{a}_p p^{-s} + \overline{\varepsilon}(p) p^{k-1-2s})^{-1}.$$

Corollaire 14. *$|_k w_N$ respecte les formes nouvelles et les formes anciennes.*

Corollaire 15. *La valeur absolue de la pseudo-valeur propre $\lambda_N(f)$ de $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$ primitive est égale à 1.*

Preuve. $(f|_k w_N, f|_k w_N) = \lambda_N(f)\overline{\lambda}_N(f)(f_\rho, f_\rho) = (f, f)$ et $(f_\rho, f_\rho) = (f, f)$.

Supposons que le caractère de Dirichlet modulo N est trivial (ce qui implique k pair car $\varepsilon(-1) = (-1)^k$). Alors λ_N est une vraie valeu propre.

Proposition 24. *Soit $f \in \mathcal{C}(N, 1, k)^{prim}$. On a $f|_k w_N = \lambda_N f$ avec*

$$\lambda_N = \pm 1.$$

L'equation fonctionnelle de la fonction $\Lambda(f, s)$ est

$$\Lambda(f, s) = (-1)^{k/2} \lambda_N \Lambda(f, k - s)$$

Preuve. Les coefficients de Fourier de f sont réels donc $f_\rho = f$. Comme $w_N = N\,\mathrm{id}$ et k est pair, on a $\lambda_{p^n}^2 = 1$.

Corollaire 16.

$$\Lambda(f, k/2+s) = (-1)^{k/2}\lambda_N \Lambda(f, k/2-s), \quad \lambda_N = \pm 1$$

Comme $\Gamma(k/2)\neq 0$, on déduit que $L(f, k/2) = 0$ si $\lambda_N = -(-1)^{k/2}$.

Soit $N = QQ'$ une factorisation de N en deux entiers Q, Q' premiers entre eux. Soit $\varepsilon = \varepsilon_Q\varepsilon_{Q'}$ la factorisation correspondante du caractère de Dirichlet ε. Nous allons voir que l'application $|_k w_N$ est presque multiplicative, i.e. presque la composée d'opérateurs $|_k w_Q$ et $|_k w_{Q'}$.

On choisit une matrice

$$w_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} = \begin{pmatrix} x & y \\ Q'z & Qw \end{pmatrix} \delta_Q$$

avec $x, y, z, w \in \mathbf{Z}$, $Qxw - Q'yz = 1$, $x \equiv 1$ modulo Q' et $y \equiv 1$ modulo Q. Par exemple, $x = y = 1$. Soit $w'_Q = \begin{pmatrix} Qx' & y' \\ Nz' & Qw' \end{pmatrix}$ avec $x', y', z', w' \in \mathbf{Z}$, $Qx'w' - Q'y'z' = 1$.

Proposition 25. *Soit $f \in \mathcal{C}(N, \varepsilon, k)$.*

1) $f|_k w_Q = \varepsilon_Q(y')\varepsilon_{Q'}(x') f|_k w'_Q$ ne dépend pas des choix de x, y, x, w et

$f|_k w_Q \in \mathcal{C}(N, \overline{\varepsilon}_Q\varepsilon_{Q'}, k)$.

2) $f|_k w_Q^2 = \varepsilon_Q(-1)\overline{\varepsilon}_{Q'}(Q) f$.

$f|_k w_{QQ_1} = \varepsilon_{Q_1}(Q) f|_k w_Q w_{Q_1}$ si $Q' = Q_1Q_2$ avec $(Q_1, Q_2) = 1$.

3) $(f|_k w_Q, g|_k w_Q) = (f, g)$.

4) $fT(p)|_k w_Q = \varepsilon_Q(p)(f|_k w_Q)T(p)$ pour tout nombre premier p ne divisant pas Q.

Preuve. 1) On a $f|_k w_Q = \varepsilon_Q(y')\varepsilon_{Q'}(x') f|_k w'_Q$ car $w'_Q w_Q^{-1}$ appartient à $\Gamma_o(N)$ et son "a" est $Qx'w - Q'y'z$ congru à y' modulo Q et à x' modulo Q', donc $\varepsilon(w'_Q w_Q^{-1}) = \varepsilon_Q(y')\varepsilon_{Q'}(x')$.

On a $f|_k w_Q A = \varepsilon_Q(a)\overline{\varepsilon}_{Q'}(a) f$ pour $A \in \Gamma_o(N)$ car w_Q normalise $\Gamma_o(N)$ et $\varepsilon(w_Q A w_Q^{-1}) = \overline{\varepsilon}_Q(A)\varepsilon_{Q'}(A)$. En effet,

$$\begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} \begin{pmatrix} w' & -y'Q^{-1} \\ -Q'z' & x' \end{pmatrix} = \begin{pmatrix} Qxw' - Q'yz' & yx' - xy' \\ Nzw' - Nwz' & Qwx' - Qzy' \end{pmatrix}.$$

Si $(x, y, z, w) = (x', y', z', w')$ et si $Qxw - Q'yz = 1$, le produit est la matrice unité. Donc

$$w_Q^{-1} = \begin{pmatrix} w & -yQ^{-1} \\ -Q'z & x \end{pmatrix}.$$

$$\begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \begin{pmatrix} Qxa+yNc & yd+Qxb \\ Nza+QwNc & Qwd+Ncb \end{pmatrix}$$

$$\begin{pmatrix} Qxa+yNc & yd+Qxb \\ Nza+QwNc & Qwd+Ncb \end{pmatrix}\begin{pmatrix} w' & -y'Q^{-1} \\ -Q'z' & x' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix}$$

avec $N\gamma = (za+Qwc)Nw' - Q'z'(Qwd+Ncb) = N(zaw'+Qwcw' - z'wd - z'Q'cb)$ et $\alpha \equiv Qxaw' - Q'ydz' \bmod N$, donc

$\alpha \equiv Qxaw' \bmod Q',\ \alpha \equiv -Q'yz'd \bmod Q$.

Si $Qxw - Q'yz = 1, (z', w') = (z, w)$ on a

$\alpha \equiv a \bmod Q',\ \alpha \equiv d \bmod Q$ et

$\varepsilon(\alpha) = \varepsilon_Q(\alpha)\varepsilon_{Q'}(\alpha) = \varepsilon_Q(d)\varepsilon_{Q'}(a) = \overline{\varepsilon}_Q(a)\varepsilon_{Q'}(a)$.

2) Le produit $Q^{-1}w_Q^2$ appartient à $\Gamma_o(N)$ et son "a" est $Qx^2 + Q'yz$ congru à -1 modulo Q et à Q modulo Q', donc $\varepsilon(Q^{-1}w_Q^2) = \varepsilon_Q(-1)\varepsilon_{Q'}(Q)$.

Prenant w_Q, w_{Q_1} avec $x = y = 1$, on a $w_Q w_{Q_1} = w'_{QQ_1}$ avec le $x' \equiv 1 \bmod Q_2$ et $y' = Q_1 w_1 + Q$, donc $\varepsilon_{QQ_1}(y') = \varepsilon_{Q_1}(Q)$.

$$\begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}\begin{pmatrix} Q_1x' & y' \\ Nz' & Q_1w' \end{pmatrix} = \begin{pmatrix} QxQ_1x' + yNz' & yQ_1w' + Qxy' \\ NzQ_1x' + QwNz' & QwQ_1w' + Nzy' \end{pmatrix}.$$

Si $Q(x, y, z, w) = Q_1(x', y', z', w')$ c'est

$$\begin{pmatrix} Q^2x^2 + Nyz & Qy(w+y) \\ NQ(zx+wz) & Q^2w^2 + Nzy \end{pmatrix} = Q\begin{pmatrix} Qx^2 + Q'yz & y(w+y) \\ N(zx+wz) & Qw^2 + Q'zy \end{pmatrix}$$

Si $Qxw - Q'yz = 1$, le produit appartient à $Q\Gamma_o(N)$.

Lorsque $Q' = Q_1Q_2,\ (Q_1, Q_2) = 1$, on choisit $x = x' = y = y' = 1$ donc

$$\begin{pmatrix} Q & 1 \\ Nz & Qw \end{pmatrix}\begin{pmatrix} Q_1 & 1 \\ Nz' & Q_1w' \end{pmatrix} = \begin{pmatrix} QQ_1(1+Q_2z') & Q_1w' + Q \\ N(zQ_1 + Qwz') & QQ_1(ww' + Q_2z) \end{pmatrix}.$$

3) On a $(f|_k w_Q, g) = (f, f|_k w_Q^*)$ et $w_Q^* = Qw_Q^{-1} = \begin{pmatrix} Qw & -y \\ -Nz & Qx \end{pmatrix}$ est un "w'_Q" et $\varepsilon_Q(-y)\varepsilon_{Q'}(w) = \varepsilon_Q(-1)\varepsilon_{Q'}(Q)^{-1}$ car $wQ \equiv 1 \bmod Q'$.

4) Je faiblis pour $T(p)$. C'est plus long mais sans astuce. Exercice !

Proposition 26. *Si $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$ est primitive, alors il existe $f_Q \in \mathcal{C}(N, \overline{\varepsilon}_Q\varepsilon_{Q'}, k)^{prim}$ primitive et une constante $\lambda_Q = \lambda_Q(f)$, uniques, tels que $f|_k w_Q = \lambda_Q f_Q$. On dit que f est pseudo propre pour $|_k w_Q$ de pseudo valeur propre λ_Q.*

Notons $f = q + \sum_{n\geq 2} a_n q^n$ et $f_Q = q + \sum_{n\geq 2} b_n q^n$. On a pour tout nombre premier p,

$b_p = \overline{\varepsilon}_Q(p)a_p$ si p ne divise pas Q et $b_p = \varepsilon_{Q'}(p)\overline{a}_p$ si p divise Q'.

Non montré en cours. Exercice ?

Si ε_Q est trivial, on a $f_Q = f$ par le théorème de multiplicité 1 et λ_Q est une vraie valeur propre.

On déduit que $|a_n| = |b_n|$ pour tout $n \geq 1$. La série

$$L(f \otimes f, s) = \sum_{n \geq 1} a_n \overline{a}_n n^{-s+k-1}$$

est égale à $L(f_Q \otimes f_Q, s)$. On sait (non montré en cours) qu'elle se prolonge en un fonction méromorphe sur $\mathbf{C}$ de pole simple en $s = 1$ de résidu $(f, f)c$ pour une constante non nulle c dépendant seulement de N, k. Donc

$$(f, f) = (f_Q, f_Q).$$

Comme $(f, f) = (f|_k w_Q, f|_k w_Q)$, on a:

Proposition 27. *La pseudo valeur propre λ_Q est de valeur absolue 1.*

Attention, si ε n'est pas trivial, les opérateurs $|_k w_Q$ ne commutent pas toujours.

Supposons que le caractère ε est trivial. Soit $N = \prod_p p^n$ la factorisation de N en produit de nombres premiers. Le produit des endomorphismes $|_k w_{p^n}$ de $\mathcal{C}(N, 1, k)$ est $|_k w_N$.

Proposition 28. *Si $f \in \mathcal{C}(N, 1, k)^{prim}$, la pseudo valeur propre $\lambda_p(f)$ de f pour $|_k w_{p^n}$ est ± 1.*

Preuve. On a $f|_k w_{p^n} = \lambda_p(f) f_{p^n}$ avec $f_{p^n} \in \mathcal{C}(N, 1, k)^{prim}$ où f_{p^n} a même valeur propre que f pour $T(p')$ lorsque $p' \neq p$ par la proposition 26, donc $f_{p^n} = f$ par le théorème de multiplicité 1.

Comme $w_{p^n} = -p^n \,\mathrm{id}$ et k est pair, on a $\lambda_{p^n}^2 = 1$.

Si p est un nombre premier divisant N, on note $N = N_p N_p'$ avec $(N_p', p) = 1$.

Proposition 29. *Soit $f = q + \sum_{n \geq 2} a_n q^n \in \mathcal{C}(N, \varepsilon, k)^{prim}$ primitive et soit p un nombre premier divisant N et ε_p la composante en p de ε. Alors*

- Si ε_p est primitif, alors $|a_p| = p^{(k-1)/2}$.

- Si $N_p = p$ et si ε_p est trivial, alors $a_p^2 = p^{k-2} \varepsilon_{N_p'}(p)$.

- Sinon (p^2 divise N_p et ε_p n'est pas primitif), $a_p = 0$.

Non démontré en cours. Voir Li Theorem 3 page 295, Miyake 4.6.17.

Proposition 30. *(Lien entre la valeur propre de $T(p)$ et la pseudo-valeur propre de w_{p^n} lorsque $p^n||N$)*

Soit $f = q + \sum_{n\geq 2} a_n q^n \in \mathcal{C}(N,\varepsilon,k)^{prim}$ primitive et soit p un nombre premier divisant N tel que $a_p \neq 0$.

Si $p||N$ et ε_p est trivial, alors $\lambda_p a_p = -p^{(k/2-1)}$.

Si $p^n||N$ et ε_p est primitif, alors $\lambda_{p^n} a_p^n = p^{n(k/2-1)} G(\varepsilon_p)$ où

$$G(\varepsilon_p) := \sum_{x \bmod p^n} \varepsilon_p(x) e^{2i\pi/p^n}$$

la somme de Gauss du caractère de Dirichlet primitif ε_p de condcteur p^n.

Comme $a_p \neq 0$, alors ε_p est primitif ou $p||N$ et ε_p est trivial par la proposition 29.

Le premier coefficient de Fourier de $fT(p)^n|_k w_{p^n} = a_p^n \lambda_{p^n} f_{p^n}$ est $a_p^n \lambda_{p^n}$. On va le calculer directement.

Remarquer que $\prod_{1\leq i\leq n} \begin{pmatrix} 1 & u_i \\ 0 & p \end{pmatrix} = \begin{pmatrix} 1 & \sum_i p^{n-i} u_i \\ 0 & p^n \end{pmatrix}$ et que $\varepsilon(p) = 0$ donc

$fT(p)^n = p^{n(k/2-1)} \sum_{u \bmod p^n} f|_k \begin{pmatrix} 1 & u \\ 0 & p^n \end{pmatrix}$

Vérifions que le terme constant c de $fT(p)^n|_k w_{p^n}$ ne provient de que la somme avec $(u,p) = 1$. Notons que $u = pv$ modulo p^n est équivalent à v modulo p^{n-1}. Posons $N = p^n q'$, on peut choisir une matrice

$$w'_{p^n} = \begin{pmatrix} p^n x & y \\ Nz & p^n w \end{pmatrix}, \quad p|x, p^n xw - q'yz = 1.$$

On a $|_k w_{p^n} = |_k w'_{p^n} \varepsilon_{p^n}(y) \varepsilon_{q'}(x)$.

$\begin{pmatrix} 1 & pv \\ 0 & p^n \end{pmatrix} w'_{p^n} = \begin{pmatrix} 1 & v \\ 0 & p^{n-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p^n x & y \\ Nz & p^n w \end{pmatrix} \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & v \\ 0 & p^{n-1} \end{pmatrix} \begin{pmatrix} p^{n-1} x & y \\ Nz & p^{n+1} w \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

La matrice du mileu est une matrice type w_{p^n}. A un facteur près, la somme sur les v modulo p^{n-1} donne $fT(p)^{n-1}|_k w_{p^n}(pz)$ qui a un terme constant nul.

On néglige donc les u divisibles par p. Le terme constant de $fT(p)^n|_k w_{p^n}$ est $p^{n(k/2-1)} \varepsilon_{p^n}(y) \varepsilon_{q'}(x)$ fois le terme constant de A où

$A = \sum_{u \bmod p^n, (u,p)=1} f|_k \begin{pmatrix} 1 & u \\ 0 & p^n \end{pmatrix} w'_{p^n}$.

On note v tel que $uzq'v \equiv y$ modulo p^n. Alors $\begin{pmatrix} 1 & u \\ 0 & p^n \end{pmatrix} w'_{p^n} \begin{pmatrix} 1 & -vp^{-n} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p^n x + Nuz & -xv - uzvq' + y + p^n wu \\ p^n Nz & -vzN + p^{2n} w \end{pmatrix} = p^n \begin{pmatrix} * & * \\ * & -vzq' + p^n w \end{pmatrix}$ appartient à $p^n \Gamma_o(N)$.

$A = \sum_{v \bmod p^n, (v,p)=1} \varepsilon(-vzq' + p^b w) f|_k \begin{pmatrix} 1 & vp^{-n} \\ 0 & 1 \end{pmatrix}$

Comme $(\varepsilon_p \varepsilon_{q'})(-vzq' + p^n w) = \varepsilon_p(v)\varepsilon_p(-zq')\varepsilon_{q'}(p^n w)$ et $1 = (\varepsilon_p \varepsilon_{q'})(-yzq' + p^n xw) = \varepsilon_p(y)\varepsilon_p(-zq')\varepsilon_{q'}(p^n w)\varepsilon_{q'}(x)$, le terme constant de $fT(p)^n|_k w_{p^n}$ est donc $p^{n(k/2-1)}$ fois le terme constant de $\sum_{v \bmod p^n, (v,p)=1} \varepsilon_p(v) f(z + vp^{-n})$, i.e.

$$c = p^{n(k/2-1)} \sum_{v \bmod p^n, (v,p)=1} \varepsilon_p(v) e^{2i\pi v p^{-n}}.$$

8. Torsion par un caractère de Dirichlet

Référence. Miyake, pour les sommes de Gauss. Atkin-Li pour les formes modulaires tordues.

Soit χ un caractère de Dirichlet modulo M et soit $a \in \mathbf{Z}$. La somme de Gauss $G(\chi, a)$ est le nombre complexe

$$G(\chi, a) = \sum_{x=0}^{M-1} \chi(x) e^{2i\pi a x/M} = \sum_{x \in (\mathbf{Z}/M\mathbf{Z})^*} \chi(x) e^{2i\pi a x/M}$$

Elle ne dépend que de a modulo M. Si $a = 1$, on dit simplement que c'est la somme de Gauss de χ.

Si χ est le caractère trivial 1_M modulo M, alors

$$G(1_M, a) = \sum_{x \in (\mathbf{Z}/M\mathbf{Z})^*} e^{2i\pi a x/M}.$$

Si $\chi \neq 1_M$ et si $a \equiv 0 \bmod M$ alors $G(\chi, 0) = 0$.
On a $G(1_M, 0) = \phi(M)$.
Si $M = p$ est un nombre premier et $(a, p) = 1$ alors $G(1_p, a) = -1$.

Proposition 31. *Soit χ un caractère de Dirichlet primitif modulo M. Alors*

$$G(\chi, a) = \overline{\chi}(a) G(\chi).$$

Preuve. Si $(a, M) = 1$, on a

$$\chi(a) \sum_{x \bmod M} \chi(x) e^{2i\pi xa/M} = G(\chi)$$

car xa parcourt les entiers modulo M et $\chi(a)\chi(x) = \chi(ax)$. Si $(a, M) \neq 1$ on a $\overline{\chi}(a) = 0$. La somme de Gauss $G(\chi, a)$ est nulle car χ est primitif.

En effet, le dénominateur de a/M' est $M' < M$ et $G(\chi, a)$ est multiple de $\sum_{h\in H} \chi(h)$ pour h parcourant le noyau de $(\mathbf{Z}/M\mathbf{Z})^* \to (\mathbf{Z}/M'\mathbf{Z})^*$. Comme χ est primitif, sa restriction au noyau n'est pas triviale donc $\sum_{h\in H} \chi(h) = 0$.

Corollaire 17. *(i)* $G(\chi)\overline{G(\chi)} = M$.
(ii) $\overline{G(\chi)} = \chi(-1)G(\overline{\chi})$ *et* $G(\chi)G(\overline{\chi}) = \chi(-1)M$

Preuve. (i)Par la proposition $G(\chi)\overline{G}(\chi) = \sum_{a \bmod M} G(\chi)\, \overline{\chi}(a) e^{-2i\pi a/M}$ est

$$\sum_{a \bmod M} G(\chi, a) e^{-2i\pi a/M} = \sum_{a,x \bmod M} \chi(x) e^{2i\pi(x-1)a/M}$$

Rappelant $\sum_{a \bmod M} e^{2i\pi ma/M} = M$ si $M|m$ et 0 sinon, il ne reste que $x = 1 \bmod M$.

(ii) On applique la proposition $\overline{G(\chi)} = G(\overline{\chi}, -1)$.

Corollaire 18. *Factorisation. Soit $M = RR'$ une factorisation de M en entiers R, R' premiers entre eux. Alors*

$$G(\chi) = G(\chi_R)G(\chi_{R'})\chi_R(R')\chi_{R'}(R).$$

Par le lemme chinois, si $mR + nR' = 1$ alors

$$G(\chi) = \sum_{a \bmod R, b \bmod R'} \chi_R(a)\chi_{R'}(b) e^{2i\pi(Rmb+R'na)/RR'}.$$

Par la proposition $G(\chi) = G(\chi_R)G(\chi_{R'})\overline{\chi}_R(n)\overline{\chi}_{R'}(m)$ et remarquer que $\overline{\chi}_R(n) = \chi_R(R')$ et $\overline{\chi}_{R'}(m) = \chi_{R'}(R)$.

La fonction de Möbius μ est définie sur les entiers ≥ 1. Elle vaut $(-1)^k$ sur un produit de k nombres premiers distincts, 0 sur les entiers divisibles par le carré d'un nombre premier. Pour $n > 1$ on a

$$\sum_{0<d|n} \mu(d) = 0$$

car $n = p_1^{d_1} \dots p_r^{d^r}$ avec $p_i \neq p_j$ premiers et $d_i \geq 1$, et la somme est $\sum_\varepsilon \mu(p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r})$ sur les $\varepsilon_i = 0, 1$, donc $1 - r + \binom{r}{2} - \binom{r}{1} + \dots = (1-1)^r = 0$.

Proposition 32. *Soit $L \geq 1$ et $\chi' : (\mathbf{Z}/ML)^* \to (\mathbf{Z}/M)^* \to \mathbf{C}^*$ le caractère modulo ML inflaté de χ primitif. Alors*

$$G(\chi', a) = G(\chi) \sum_{0<d|(L,a)} d\mu(L/d)\chi(L/d)\overline{\chi}(a/d).$$

Preuve. Miyake 3.1.3. Ceci généralise la formule $G(\chi, a) = \overline{\chi}(a)G(\chi)$ pour $L = 1$. On a $\chi'(b) = 0$ si $(b, L)\neq 1$ et $\chi'(b) = \chi(b)$ sinon. On écrit cela avec la fonction de Moebius

$$\chi'(b) = \sum_{0<d|(b,L)} \mu(d)\chi(b)$$

$$G(\chi', a) = \sum_{b \bmod LM} \sum_{0<d|(b,L)} \mu(d)\chi(b)e^{2i\pi ab/LM}$$

On écrit $L = dL', b = d\beta$. On a

$$G(\chi', a) = \sum_{0<d|L} \mu(d)\chi(d) \sum_{\beta \bmod L'M} \chi(\beta)e^{2i\pi\beta a/L'M}.$$

On montre que la dernière somme est 0 si L' ne divise pas a et que si L' divise a c'est $L'\overline{\chi}(a/L')G(\chi)$.

On a $\beta = M\gamma + \delta$ où γ modulo L' et δ modulo M et $\chi(\beta) = \chi(\gamma)$.

$$\sum_{\beta \bmod L'M} \chi(\beta)e^{2i\pi\beta a/L'M} = \Big(\sum_{\delta \bmod M} \chi(\delta)e^{2i\pi\delta a/L'M}\Big) \sum_{\gamma \bmod L'} e^{2i\pi\gamma a/L'M}$$

Si $\sum_{\gamma \bmod L'} e^{2i\pi\gamma a/L'}\neq 0$ alors $a \equiv 0 \bmod L'$ et elle vaut L'. Le premier facteur à droite est alors la somme de Gauss $G(\chi, a/L') = \overline{\chi}(a/L')G(\chi)$.

Aussi on obtient

$$G(\chi', a) = G(\chi) \sum_{0<L'|(a,L)} L'\mu(L/L')\chi(L/L')\overline{\chi}(a/L')$$

Proposition 33. *Le produit de deux caractères de Dirichlet ε et ε' est un caractère de Dirichlet $\varepsilon\varepsilon'$. Pour tout nombre premier, le conducteur de $\varepsilon\varepsilon'$ en p est le sup des conducteurs en p de ε et de ε' si ces conducteurs ont distincts; s'ils sont égaux il peut être plus petit.*

En factorisant les caractères, on se ramène au cas où ε est un caractère modulo p^n et ε' est un caractère modulo $p^{n'}$ pour un nombre premier p et deux entiers $0 \leq n \leq n'$. Le plus simple est d'identifier les caractères de Dirichlet modulo p^n avec les caractères de $\mathbf{Z}_p^*$ triviaux sur $1 + p^n\mathbf{Z}_p$. L'intersection $\mathbf{Z} \cap \mathbf{Z}_p^*$ est formée par les entiers $a \in \mathbf{Z}$

premiers à p et $a+p^n\mathbf{Z}=a(1+p^n\mathbf{Z}a^{-1})$ dans $\mathbf{Z}_p^*$. On en déduit des isomorphismes entre les groupes de cardinal $(p-1)p^{n-1}$,

$$(\mathbf{Z}/p^n\mathbf{Z})^* \simeq (\mathbf{Z}_p/p^n\mathbf{Z}_p)^* \simeq \mathbf{Z}_p^*/(1+p^n\mathbf{Z}_p).$$

Le produit des deux caractères du groupe $\mathbf{Z}_p^*$ est un caractère de $\mathbf{Z}_p^*$. Donc $\varepsilon\varepsilon'$ est un caractère de Dirichlet modulo $p^{n'}$.

Définition 4. *Pour une forme modulaire $f=\sum_{n\geq 1}a_nq^n\in\mathcal{C}(N,\varepsilon,k)$, la tordue f_χ de f par un caractère de Dirichlet χ modulo M est la fonction*

$$f_\chi=\sum_{n\geq 1}a_n\chi(n)q^n.$$

Posons $t_a=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ pour $a>0$. Alors l'opérateur $|_kt_a$ est la translation par a. On pose

$$ft_\chi=\sum_{b=0}^{M-1}\overline{\chi}(b)f|_kt_{b/M}=\sum_{b\in(\mathbf{Z}/M\mathbf{Z})^*}\overline{\chi}(b)f|_kt_{b/M}.$$

Lemme 6. $ft_\chi=G(\overline{\chi})f_\chi$.

Preuve. $ft_\chi=\sum_{b\in(\mathbf{Z}/M\mathbf{Z})^*}\overline{\chi}(b)\sum_{n\geq 1}a_nq^ne^{2i\pi nb/N}$.

Lorsque χ est primitif, l'étude de f_χ se ramène à celle de ft_χ car $G(\overline{\chi})\neq 0$. On étudie l'opérateur t_χ.

Proposition 34. *Pour $f\in\mathcal{C}(N,\varepsilon,k)$ et un caractère de Dirichlet χ modulo M, ft_χ appartient à $\mathcal{C}(\tilde{N},\varepsilon\chi^2,k)$ où $\tilde{N}$ est le p.p.c.m. de N,M^2.*

Preuve. Il est clair que ft_χ est holomorphe parabolique de poids k. Soit $A=\begin{pmatrix}a & b\\ \tilde{N}c & d\end{pmatrix}\in\Gamma_o(\tilde{N})$. Alors a,d sont premiers à M. Pour chaque $x \bmod M$ il existe x' mod M tel que $ax'\equiv dx \bmod M$. Alors

$$t_{x/M}At_{-x'/M}=\begin{pmatrix}a+cx\tilde{N}M^{-1} & (-x'a+dx)M^{-1}-x'cu\tilde{N}M^{-2}+b\\ c\tilde{N} & -cx'\tilde{N}M^{-1}+d\end{pmatrix}$$

appartient à $\Gamma_o(\tilde{N})$ qui est contenu dans $\Gamma_o(N)$. On a $\overline{\chi}(x)f|_kt_{x/m}A=\varepsilon(d)\overline{\chi}(x)f|_kt_{x'/m}$ et $\overline{\chi}(x)=\chi(d)^2\,\overline{\chi}(x')$.

Remarque 8. Si p divise M alors $(f|_k\delta_p)_\chi=0$. L'application linéaire

$$f\mapsto f_\chi:\mathcal{C}(N,\varepsilon,k)\to\mathcal{C}(\tilde{N},\varepsilon,k)$$

n'est pas injective si $(N,M)\neq 1$.

Lorsque χ est quadratique, $t_\chi:\mathcal{C}(N,1,k)\to\mathcal{C}(\tilde{N},1,k)$.

Proposition 35. *1) Soit p un nombre premier ne divisant pas M. Alors $t_\chi T(p) = \chi(p)T(p)t_\chi$ et $(f|_k\delta_p)_\chi = \chi(p)f_\chi|_k\delta_p$*

2) $(f_\chi, g_\chi) = (f, g)$.

3) Si f est ancienne, resp. nouvelle, alors f_χ est ancienne, resp. nouvelle.

4) $(ft_\chi)_\rho = \chi(-1)f_\rho t_{\overline{\chi}}$.

5) Si $N = QQ'$ est une factorisation en entiers Q, Q' premiers entre eux et $(M, Q) = 1$, alors

$$t_\chi w_Q = \overline{\chi}(Q)w_Q t_\chi.$$

6) Si χ est primitif, $(M, N) = 1$, et $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$ primitive, alors $f_\chi \in \mathcal{C}(NM^2, \varepsilon\chi^2, k)$ est primitive et

$$\lambda_{NM^2}(f_\chi) = \lambda_N(f)\varepsilon(M)\chi(N)G(\chi)/G(\overline{\chi}).$$

Non démontré. Vérifier.

Proposition 36. *(Torsion par un caractère de conducteur assez grand) Soit $f \in \mathcal{C}(N, \varepsilon, k)^{prim}$ primitive. Soit $N = qq'$ avec $(q, q') = 1$, et χ un caractère de Dirichlet primitif de conducteur m avec $(q, m) = 1, q'|m$, et tel que le conducteur de $\varepsilon_{q'}\chi$ soit m. Alors*

1) $f_\chi \in \mathcal{C}(qm^2, \varepsilon\chi^2, k)^{prim}$ est primitive.

2) $f_\chi|_k w_{m^2} = \lambda_{m^2} f_{\overline{\varepsilon}_{q'}\chi}$ avec $f_{\overline{\varepsilon}_{q'}\chi} \in \mathcal{C}(qm^2, \varepsilon_q\varepsilon_{q'}^{-1}\chi^{-2}, k)^{prim}$ primitive, et

$$\lambda_{m^2}(f_\chi) = \overline{\varepsilon}_q(m)\chi(-1)G(\varepsilon_{q'}\chi)/G(\overline{\chi})$$

3) $f_\chi|_k w_{qm^2} = \lambda_{qm^2}(f_\chi)(f_\chi)_{qm^2}$ avec $(f_\chi)_{qm^2} \in \mathcal{C}(qm^2, \varepsilon^{-1}\chi^{-2}, k)^{prim}$

$$\lambda_{qm^2}(f_\chi) = \lambda_q(f)\chi(-q)\varepsilon_{q'}(q)\overline{\varepsilon}_q(m)G(\varepsilon_{q'}\chi)/G(\overline{\chi}).$$

Atkin-Li th. 4.1. Comparer avec la proposition 35 6). Il est remarquable de voir que la pseudo valeur propre de f_χ en m^2 ne dépend que de ε.

Preuve. 1) Non fait en cours.

2) On choisit des entiers x, y, z, w vérifiant $m^2xw - qyz = 1$ avec $x \equiv 1 \bmod q$ et $y \equiv 1 \bmod m^2$ ce qui fournit une matrice w_{m^2}. Noter que $y \equiv 1 \bmod m$ et que l'application $a \mapsto a'$ dans les entiers inversibles modulo m qui envoie a sur un inverse a' de azq modulo m est une bijection. On calcule $t_{a/m}w_{m^2}t_{-a'/m} =$

$$m\begin{pmatrix} mx + zaq & -xa' + aw - (aa'q + y)/m \\ qmz & -qza' + mw \end{pmatrix} \in m\Gamma_o(N).$$

Cela implique que $ft_\chi|_k w_{m^2} = \sum_{a \bmod m} \overline{\chi}(a)f|_k t_{a/m}w_{m^2}$ est égal à la somme pour $a' \bmod m$ de $\overline{\chi}(a)\varepsilon(-qza' + mw)f|_k t_{a'/m}$. On écrit

$\varepsilon = \varepsilon_q\varepsilon_{q'}$; remarquant que $-qz \equiv 1 \bmod m^2$ et $m^2 w \equiv 1 \bmod q$, on voit que $\overline{\chi}(a)\varepsilon(-qza' + mw)$ est $\chi(-1)\overline{\varepsilon}_q(m)(\chi\varepsilon_{q'})(a')$. D'où

$$ft_\chi|_k w_{m^2} = \chi(-1)\overline{\varepsilon}_q(m) ft_{\overline{\chi\varepsilon_{q'}}}$$

Admettant que f_χ est primitive (donc $ft_{\overline{\varepsilon_{q'}\chi}}$ aussi), on obtient la formule voulue pour la pseudo-valeur propre, en utilisant $G(\overline{\chi})f_\chi = ft_\chi$.

3)
$f_\chi|_k w_{qm^2} = (\varepsilon_{q'}\chi^2)(q) f_\chi|_k w_q w_{m^2}$ par la factorisation de w_{qm^2}.
$f_\chi|_k w_q = \overline{\chi}(q)(f|_k w_q)_\chi$ par la proposition 35 5).
$f|_k w_q = \lambda_q(f) f_q$ avec $f_q \in \mathcal{C}(N, \varepsilon\varepsilon_q^{-2}, k)^{prim}$,
$(f_q)_\chi|_k w_{m^2} = \lambda_{m^2}((f_q)_\chi)(f_\chi)_{qm^2}$.
$\lambda_{m^2}((f_q)_\chi) = \varepsilon_q(m)\chi(-1)G(\varepsilon_{q'}\chi)/G(\overline{\chi})$.

Corollaire 19. *Si χ est quadratique et si ε est trivial, alors*

$$\Lambda(f_\chi, k/2 + s) = (-1)^{k/2}\chi(-q)\lambda_q(f)\Lambda(f_\chi, k/2 - s).$$

Preuve. $\lambda_{qm^2}(f_\chi) = \lambda_q(f)\chi(-q)$.

Donc $L(f_\chi, k/2) = 0$ si $\chi(-q) = -\lambda_q(f)(-1)^{k/2}$ (le corollaire 16 concerne le cas χ trivial).

9. Rationalité, intégralité

Les théorèmes suivants sont hors de portée pour l'instant. On les admet.

Théorème 5. *Il existe une base de $\mathcal{C}(N, k)$ dont les coefficients sont des nombres rationnels.*

Shimura th. 3.48 et 3.52.
On a déja admis que la dimension de $\mathcal{C}(N, k)$ est finie.

Théorème 6. *Les valeurs propres des opérateurs de Hecke $T(p)$ dans $\mathcal{C}(N, \varepsilon, k)$ appartiennent à l'anneau des entiers d'un corps de nombres (indépendant du choix du nombre premier p).*

Donc, les coefficients de Fourier des formes de la base canonique de $\mathcal{C}(N, \varepsilon, k)$ appartiennent à l'anneau des entiers d'un corps de nombres.

Proposition 37. *Les pseudo valeurs propres de $|_k w_Q$ sur les formes primitives de $\mathcal{C}(N, \varepsilon, k)$ sont algébriques.*

Atkin-Li th. 1.1.

Théorème 7. *Soit* $f = q + \sum_{n\geq 2} a_n q^n \in \mathcal{C}(N,\varepsilon,k)^{prim}$ *primitive. Alors les valeurs absolues des racines de l'equation*

$$X^2 - a_p X + \varepsilon(p)p^{k-1}$$

sont $p^{(k-1)/2}$ *pour tout nombre premier* p *ne divisant pas* N*.*

Deligne (ref ?).