École Normale supérieure de Lyon

ENS DE LYON

Rapport de stage de L3

Formes modulaires de poids 1

Auteur :
Dylan Laird

Encadrant:
Didier Lesesvre
Laboratoire Paul Painlevé, Université de Lille

Laboratoire Paul Painlevé

Table des Matières

Introduction

Les formes modulaires sont des fonctions définies sur le demi-plan de Poincaré $\mathcal{H}$ et possédant un développement de Fourier $f(z) = \sum_{n\geq 0} a_n e(z)$ (dans la suite $e(\cdot) = \exp(2i\pi\cdot)$), possédant de bonnes propriétés de symétrie par certains groupes discrets d'homographies. Les coefficients de Fourier de ces formes sont d'un intérêt arithmétique important. Soit par exemple $r_8(n)$ le nombre de représentations de n en somme de 8 carrés d'entiers relatifs. On peut s'intéresser à la fonction génératrice exponentielle $f(z) = \sum_{n\geq 0} r_8(n)e(nz)$, on vérifie alors que :

$$f(z) = \sum_{n\geq 0} r_8(n)e(nz) = \sum_{n\geq 0} \sum_{v_1^2+\dots v_8^2=n} e((v_1^2+\dots v_8^2)z) = \big(\sum_{n\in\mathbb{Z}} e(n^2 z)\big)^8 = \vartheta(z)^8$$

où l'on a noté $\vartheta(z) = \sum_{n\in\mathbb{Z}} e(n^2 z)$ la fonction thêta de Jacobi. Cette fonction est 1-périodique. Elle prend la forme d'une somme sur $\mathbb{Z}$ de gaussiennes, ce qui permet d'appliquer la formule sommatoire de Poisson pour obtenir :

$$\forall z \in \mathcal{H}, \quad f\Big(\frac{z}{4z+1}\Big) = (4z+1)^4 f(z)$$

C'est un exemple de forme modulaire de poids 4, pour le sous-groupe de Hecke $\Gamma_0(4)$. L'espace de ces formes est de dimension finie et de petite taille, on pourrait en donner une base et enfin une formule close pour r_8.
On s'intéresse dans ce rapport à la dimension des espaces $\mathcal{S}_k(q)$ de telles formes modulaires, pour lesquels on a des formules de dimensions en poids $k \geq 2$ avec un terme principal :

$$\dim \mathcal{S}_k(q) \asymp \frac{q(k-1)}{12}$$

Au vu de cette formule, on peut s'attendre à un phénomène de chute de dimension en poids $k = 1$. Un tel résultat a été obtenu par Duke dans [5] où il a prouvé que $\dim \mathcal{S}_1(q) \ll q^{11/12}\log^4(q)$. L'objectif de mon stage avec Didier Lesesvre était d'étudier la théorie des formes modulaires et comprendre certains aspects de l'article de Duke.
Dans une première partie de ce rapport, je présente quelques aspects classiques de la théorie des formes modulaires. La deuxième partie est consacrée à une étude plus approfondie des fonctions L attachées aux formes cuspidales. La troisième partie traite de représentations galoisiennes (complexes) et des fonctions L d'Artin associées. La comparaison des fonctions L obtenues sera l'occasion d'introduire le théorème de Deligne-Serre [2] qui est un fort résultat de correspondance entres formes cuspidales de poids 1 et représentations galoisiennes de degré 2. Ce théorème est un ingrédient clé de l'article de Duke, j'y reviendrai à la fin du rapport.

1 Formes Modulaires : Généralités

1.1 $\mathrm{SL}_2(\mathbb{R})$ et de le demi-plan de Poincaré

Commençons par introduire le demi-plan de Poincaré :

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im z > 0\}$$

Le groupe $\mathrm{GL}_2^+(\mathbb{R}) = \{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det g > 0\}$ agit naturellement sur $\mathcal{H}$ par homographies de la manière suivante : si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$ on pose

$$\gamma \cdot z = \frac{az+b}{cz+d}, \quad \forall z \in \mathcal{H}$$

On notera parfois φ_γ l'homographie associée à γ. En introduisant son **facteur d'automorphie** $j_\gamma(z) = cz + d$ on a la formule fondamentale suivante :

$$\Im(\gamma \cdot z) = \frac{\det \gamma \cdot \Im z}{|j_\gamma(z)|^2}, \quad \forall \gamma \in \mathrm{GL}_2(\mathbb{R})$$

Cette formule montre bien que les homographies de $\mathrm{GL}_2^+(\mathbb{R})$ envoient $\mathcal{H}$ sur lui-même. On peut noter que deux matrices γ et γ' déterminent la même homographie si et seulement si $\gamma \in \mathbb{R}^*\gamma'$ de sorte que le groupe des homographies réelles qui agissent sur $\mathcal{H}$ est en fait $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$. Du point de vue de l'analyse complexe, les applications φ_γ sont holomorphes, de réciproque $\varphi_{\gamma^{-1}}$ holomorphe et bijective : ce sont toutes des automorphismes de $\mathcal{H}$ (où par automorphisme on entend des bijections de $\mathcal{H}$ biholormorphes). Le théorème suivant est classique et résume les propriétés analytiques de l'action par homographies de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathcal{H}$:

Théorème 1.1 *Tout automorphisme de $\mathcal{H}$ est de la forme φ_γ pour un $\gamma \in \mathrm{SL}_2(\mathbb{R})$, et l'application $\gamma \mapsto \varphi_\gamma$ est un morphisme de groupes de $\mathrm{SL}_2(\mathbb{R})$ vers $\mathrm{Aut}(\mathcal{H})$ qui induit un isomorphisme*

$$\mathrm{Aut}\,\mathcal{H} \cong \mathrm{PSL}_2(\mathbb{R})$$

De plus l'action de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathcal{H}$ par homographies est transitive.

On peut aussi s'intéresser à une action de $\mathrm{GL}_2^+(\mathbb{R})$ sur l'espace $\mathcal{O}(\mathcal{H})$ des fonctions holomorphes sur $\mathcal{H}$. Plus précisément, pour k entier, $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ et $f \in \mathcal{O}(\mathcal{H})$ on pose :

$$f_{|[\gamma]_k} = z \mapsto (\det \gamma)^{k/2} j_\gamma(z)^{-k} f(\gamma \cdot z) \in \mathcal{O}(\mathcal{H})$$

On remarque que les opérateurs $[\gamma]_k$ préservent l'holomorphie sur $\mathcal{H}$ par la non-annulation des facteurs d'automorphie. Dans la suite j'abrègerai souvent en écrivant ${}_{|[\gamma]_k} = {}_{|\gamma}$ où le poids est rendu clair par le contexte. On mentionne au passage les règles de calcul importantes :

Proposition 1.2 *Soient $\gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R})$, $z \in \mathcal{H}$ et $f \in \mathcal{O}(\mathcal{H})$. Alors :*

$$(i). \quad j_{\gamma_1\gamma_2}(z) = j_{\gamma_1}(\gamma_2 \cdot z) j_{\gamma_2}(z) \qquad (ii). \quad f_{|[\gamma_1\gamma_2]_k} = (f_{|[\gamma_1]_k})_{|[\gamma_2]_k}$$

1.2 Formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$

La fonction génératrice du problème des 8 carrés est un premier exemple de forme modulaire. On se limitera ici aux formes modulaires pour certains sous-groupes de $\mathrm{SL}_2(\mathbb{Z})$ dits de congruence. On peut parler de formes modulaires dans un cas général pour des sous-groupes discrets de $\mathrm{SL}_2(\mathbb{R})$ appelés *groupes fuchsiens* [9], cela est notamment fait dans [8]. Il y aurait beaucoup de choses à dire sur les groupes fuchsiens et leur cadre naturel, la géométrie hyperbolique, j'y ai passé une bonne semaine en début de stage.

Définition 1.3 (Forme quasi-modulaire) *Soit $k \in \mathbb{Z}$ et Γ un groupe fuchsien, i.e un sous-groupe discret de* $\mathrm{SL}_2(\mathbb{R})$*. Une forme quasi-modulaire (pour Γ) de poids k est une fonction $f \in \mathcal{O}(\mathcal{H})$ telle que :*

$$\forall \gamma \in \Gamma, \quad f_{|[\gamma]_k} = f$$

Les groupes Fuchsiens apparaissent en réalité plus naturellement si l'on munit $\mathcal{H}$ de sa distance hyperbolique, induite par la mesure $\frac{dz}{\Im z}$. Le groupe des isométries analytiques pour cette métrique est alors exactement $\mathrm{Aut}\,\mathcal{H}$. Cette distance est telle que les points de $\mathbb{R} \cup \{i\infty\}$ sont à distance infinie. Les formes quasi-modulaires, plutôt que d'être définies sur $\mathcal{H}$ sont en fait déterminées par leur valeur sur des domaines plus restreints, les **domaines fondamentaux**.

Définition 1.4 (Domaine fondamental) *Soit Γ un sous-groupe de* $\mathrm{SL}_2(\mathbb{R})$*, on note $\overline{\Gamma}$ son image projective dans* $\mathrm{PSL}_2(\mathbb{R})$*. Un **domaine fondamental** pour l'action de Γ est un fermé $\mathcal{F}$ de $\mathcal{H}$ tel que :*

$$1.\, \mathcal{H} = \bigcup_{\gamma \in \Gamma} \gamma \mathcal{F} \qquad 2.\, \forall \gamma \in \overline{\Gamma}, \quad \gamma \mathring{\mathcal{F}} \cap \mathring{\mathcal{F}} \neq \emptyset \implies \gamma = 1$$

La théorie générale des groupes fuchsiens montre qu'ils admettent tous un domaine fondamental (voir [9]). Un choix priviligié est un domaine de Dirichlet qui est toujours connexe par arcs et hyperboliquement convexe, et dans notre cas polygonal. Dans le cas de $\mathrm{SL}_2(\mathbb{Z})$, celui-ci est donné par :

$$\mathcal{F} = \left\{ z \in \mathcal{H} \mid |z| \geq 1, \Re z \leq \frac{1}{2} \right\} \text{ (voir 1 pour une illustration)}$$

Géométriquement, le bord de ce domaine fondamental va rencontrer le point à l'infini $i\infty$. Pour obtenir la bonne notion de forme modulaire il faut imposer en plus une régularité en ce point $i\infty$. On parle d'une **pointe** (ou cusp) pour $\mathrm{SL}_2(\mathbb{Z})$. C'est cette condition de régularité qui permet d'avoir la finitude de la dimension des espaces de formes modulaires, et donc la bonne notion de forme modulaire.
Si f est une forme quasi-modulaire pour $\mathrm{SL}_2(\mathbb{Z})$, elle se doit d'être 1-périodique car invariante par l'action de $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ qui correspond à l'homographie $z \mapsto z+1$. Plus généralement, si $f \in \mathcal{O}(\mathcal{H})$ est 1-périodique, on sait par le cours d'analyse complexe que f admet un développement de Fourier de la forme :

$$\forall z \in \mathcal{H}, f(z) = \sum_{n \in \mathbb{Z}} a_n e(nz), \quad (a_n) \in \mathbb{C}^{\mathbb{Z}}$$

où $q \mapsto \sum_{n \in \mathbb{Z}} a_n q^n$ est une fonction holomorphe sur le disque épointé $D = D^*(0,1)$. On notera souvent $f = \sum a_n q^n$ son développement de Fourier avec $q = e(z)$ sous-entendu. L'application e réalise un biholomorphisme local qui envoie les voisinages de $i\infty$ dans $\overline{\mathcal{H}}$ sur des voisinages de 0 dans D. Cela motive la définition suivante :

Définition 1.5 (Holomorphie à l'infini) *Soit $f \in \mathcal{O}(\mathcal{H})$ une fonction 1-périodique de développement $f(z) = \sum_{n \in \mathbb{Z}} a_n e(nz)$. On dit que f est **holomorphe à l'infini** si l'application $g = q \mapsto \sum_{n \in \mathbb{Z}} a_n q^n$ se prolonge par holomorphie en 0, ce qui est équivalent à demander que le développement de g soit de la forme*

$$g = \sum_{n \in \mathbb{N}} a_n q^n$$

On peut de manière analogue définir l'holohomorphie à l'infini pour des fonctions holomorphes ℓ-périodique avec des développements en puissances de $q^{1/l}$.

Définition 1.6 (Forme modulaire pour $\mathrm{SL}_2(\mathbb{Z})$) *L'ensemble $\mathcal{M}_k$ des formes modulaires de poids k pour* $\mathrm{SL}_2(\mathbb{Z})$ *est l'ensemble des formes quasi-modulaires de poids k qui sont également holomorphes à l'infini. On dit de plus qu'une forme modulaire f est **cuspidale** si le terme constant de son développement de Fourier est nul, autrement dit que f est nulle en la pointe $i\infty$. On note $\mathcal{S}_k$ l'ensemble des telles formes. Ce sont tous deux des $\mathbb{C}$ espace-vectoriels.*

Proposition 1.7 *Si k est impair, on a $\mathcal{M}_k = \{0\}$*

Preuve. Soit $f \in \mathcal{M}_k$, On fait agir $\gamma = z \mapsto -1/z$ de matrice $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ en posant $g = f_{|\gamma} = f$ par modularité. En comparant les égalités $g = f$ évaluées en z et $-1/z$ on obtient $(-1)^k f = f$ ce qui implique $f = 0$ pour k impair. □

Notons que si f est une forme cuspidale, en écrivant $f(z) = \sum_{n \geq 1} a_n e(nz)$ le théorème de convergence dominée montre qu'on a $C > 0$ tel que :

$$|f(z)| \leq Ce(z), \quad \text{uniformément sur } \mathcal{H}$$

Cette propriété de décroissance rapide aux pointes (voir plus bas) est une propriété importante des formes cuspidales.
Pour $f \in \mathcal{M}_k$, la fonction $\varphi_f = z \mapsto |\Im z|^{k/2} f(\gamma \cdot z)$ est invariante par $\mathrm{SL}_2(\mathbb{Z})$. On a alors la :

Proposition 1.8 *Si $f \in \mathcal{S}_k$ une forme cuspidale, φ_f est bornée sur $\mathcal{H}$.*

Preuve. Par $\mathrm{SL}_2(\mathbb{Z})$-invariance de φ_f il suffit de voir que φ_f est bornée sur $\mathcal{F}$. Dans $\mathcal{F}$, φ_f est bornée à l'infinie par décroissance rapide de f à l'infini et croissances comparée. De plus, φ_f est clairement bornée sur les compacts de la forme $\mathcal{F} \cap \{\Im z \leq c\} \subset \{3/4 \leq \Im z \leq c\}$, cela conclut. □

Un exemple important de forme modulaire est le **discriminant modulaire** :

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} = q - 24q^2 + 252q^3 + \cdots \in \mathcal{S}_{12}$$

Avec cette définition, le fait que $\Delta \in \mathcal{S}_{12}$ n'est pas clair, on l'admettra. On peut définir Δ et obtenir cette propriété plus naturellement dans le cadre des fonctions elliptiques. Son développement de Fourier est à coefficients entiers notés $\tau(n)$. Ramanujan conjectura trois choses essentielles sur Δ. Les deux premières sont que la suite $(\tau(n))$ des coefficients de Δ est multiplicative, au sens que $\tau(mn) = \tau(m)\tau(n)$ dès que m et n sont premiers entre-eux et qu'on a une relation de récurrence :

$$\forall p \in \mathbb{P}, \quad \tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$$

Cette propriété de multiplicativité de coefficients de formes cuspidales et la relation de récurrence sont plus en fait plus générales t et on sera en mesure de les établir après avoir parlé de la théorie de Hecke. La troisième, plus profonde, est que $|\tau(p)| \leq 2p^{11/2}$ pour tout premier p. On peut calculer la dimension des espaces $\mathcal{M}_k$:

Proposition 1.9 *Pour k impair on a $\mathcal{M}_k = \{0\}$. Pour $k \geq 0$ pair, on a :*

$$\dim \mathcal{M}_k = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor, & \text{si } k \equiv 2 \pmod{12} \\ 1 + \left\lfloor \frac{k}{12} \right\rfloor, & \text{sinon} \end{cases}$$

Preuve. [4], Théorème 5.3. □

1.3 Formes modulaires pour $\Gamma_1(q)$ et de type $(\Gamma_0(q), \chi)$

On introduit pour $q > 1$ le sous-groupe de congruence :

$$\Gamma_1(q) = \{M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod q, a \equiv d \equiv 1 \mod q\}$$

Avec pour convention $\Gamma_1(1) = \mathrm{SL}_2(\mathbb{Z})$. On généralise la notion de forme quasi-modulaire à $\Gamma_1(q)$ en demandant l'invariance par les opérateurs $_{|\gamma}$ pour $\gamma \in \Gamma_1(q)$ seulement. Notons que :

Proposition 1.10 $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(q)] < \infty$

Preuve. Voir 1.2 de [3]. □

On peut écrire une décomposition en classe :

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{\gamma \in \Gamma_1(q)\backslash \mathrm{SL}_2(\mathbb{Z})} \gamma\Gamma_1(q)$$

On prouve alors que si $\mathcal{F}$ est le domaine fondamental de Dirichlet pour $\mathrm{SL}_2(\mathbb{Z})$, obtient un domaine fondamental pour $\Gamma_1(q)$ en posant :

$$\mathcal{F}' = \bigsqcup_{\gamma \in \Gamma_1(q)\backslash \mathrm{SL}_2(\mathbb{Z})} \gamma\Gamma_1(q)$$

Cela reste plus généralement vrai pour un sous-groupe Γ d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$. Ce domaine étant une union de translatés par des homograhies, il se peut maintenant qu'il rencontre en son bord plusieurs point à l'infini de $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{i\infty\}$. Pour avoir une bonne notion de forme modulaire, on a encore besoin de l'holomorphie en ces points à l'infini.

Les points à l'infini qu'il faut considérer s'appellent *pointes* de Γ. Il s'agit des points $\alpha \in \mathbb{P}^1(\mathbb{R})$ (non-équivalents sous l'action de Γ) qui sont fixés par un certain $g_\alpha \neq 1 \in \Gamma$. La théorie des groupes Fuchsiens explique le lien entre ces points et les points à l'infini qui rencontrent le bord d'un bon domaine fondamental. Dans le cas de $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, elles se trouvent donc dans $\mathbb{P}^1(\mathbb{Q})$. Comme $\mathrm{SL}_2(\mathbb{Z})$ agit transitivement sur $\mathbb{P}^1(\mathbb{Q})$ (par homographies, toujours), si α est une pointe pour Γ on a $\sigma_\alpha \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\sigma_\alpha \cdot \infty = \alpha$.

Revenons au cas $\Gamma = \Gamma_1(q)$. Si f est quasi-modulaire pour $\Gamma_1(q)$, alors $f_{|\sigma_\alpha}$ est quasi-modulaire pour $\sigma_\alpha^{-1}\Gamma_1(q)\sigma_\alpha$, sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ qui contient $t_\alpha = \sigma_\alpha^{-1} g_\alpha \sigma_\alpha$ qui vérifie $t_\alpha \infty = \infty$. C'est un exercice de vérifier que cela implique que t_α est une translation (entière) $z \mapsto z + h$ pour $h > 0$ et donc que $f_{|\sigma_\alpha}$ est h-périodique. On peut alors parler de l'holomorphie à l'infini de $f_{|\sigma_\alpha}$. Comme le comportement de f au voisinage de α est donné par celui de $f_{|\sigma_\alpha}$ au voisinage de l'infini par hypothèse, on dit que f est holomorphe en α si $f_{|\sigma_\alpha}$ est holomorphe à l'infini.

Définition 1.11 (Formes modulaires pour $\Gamma_1(q)$) *Une forme modulaire f pour $\Gamma_1(q)$ est une forme quasi-modulaire pour $\Gamma_1(q)$ holomorphe en toutes les pointes. On dit qu'elle est cuspidale si de plus f est nulle en chaque pointe.*

On peut avoir différent développements de Fourier en fonction du choix de σ_α mais la notion de nullité en une pointe, elle, ne dépend pas de ces différents choix. On montre que les formes cuspidales vérifient la condition de décroissance exponentielle en toutes les pointes et que si f est cuspidale on a toujours φ_f bornée sur $\mathcal{H}$ avec les notations précédentes. On a alors la proposition clé :

Proposition 1.12 *L'espace $\mathcal{M}_k(\Gamma_1(q))$ est de dimension finie majorée par* $1 + \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(q)]$.

Preuve. On peut voir [4], théorème 5.6. Le $k/12$ provient des formules de dimension pour $\mathrm{SL}_2(\mathbb{Z})$ et cette majoration résulte alors seulement de celles-ci et de la finitude de l'indice. □

On introduit maintenant le groupe de congruence de Hecke de niveau q :

$$\Gamma_0(q) = \{M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c = 0 \mod q\}$$

Avec la convention que $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. C'est un sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ et on a même la :

Proposition 1.13 $\Gamma_1(q) \triangleleft \Gamma_0(q)$ *et* $\Gamma_0(q)/\Gamma_1(q) \cong (\mathbb{Z}/q\mathbb{Z})^\times$.

Preuve. Soit π la réduction modulo q, alors $\Gamma_0(q) = \pi^{-1}(T(q))$ où $T(q)$ est le groupe des matrices triangulaires supérieures de déterminant 1 modulo q. On a alors un morphisme surjectif $\Gamma_0(q) \to (\mathbb{Z}/q\mathbb{Z})^\times$ qui associe à M son coefficient d'indice $(2,2)$ modulo q, de noyau $\Gamma_1(q)$, ce qui conclut. □

Soit χ un caractère de Dirichlet modulo q, à savoir un morphisme $\chi : \left(\mathbb{Z}/q\mathbb{Z}\right)^\times \to \mathbb{C}^\times$, celui-ci s'étend naturellement à $\Gamma_0(q)$ via $\chi(\gamma) = \chi(d_\gamma)$ où $\gamma = \left(\begin{smallmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{smallmatrix}\right)$ car $a_\gamma d_\gamma = 1 \mod q$ par hypothèse. On dit que χ est pair si $\chi(-1) = 1$ et impair si $\chi(-1) = -1$. Notons que $\gamma{\gamma'}^{-1} \in \Gamma_1(q) \iff d_\gamma = d_{\gamma'}$, de sorte que pour $\gamma \in \Gamma_0(q)$ et $f \in \mathcal{M}_k(\Gamma_1(q))$ la valeur de $f_{|\gamma}$ ne dépend que de d_γ.

Définition 1.14 (Formes modulaires de type $(\Gamma_0(q), \chi)$) *Une forme modulaire de poids k (resp. cuspidale) de type $(\Gamma_0(q), \chi)$ est une forme modulaire de poids k (resp. cuspidale) pour $\Gamma_1(q)$ telle que :*

$$\forall \gamma \in \Gamma_0(q), \quad f_{|\gamma} = \chi(d_\gamma) f$$

Notons que si χ et k sont de parités différentes, $\mathcal{M}_k(\Gamma_0(q), \chi) = \{0\}$. Si χ est impair, on peut donc avoir des formes de poids impair.

Proposition 1.15 *On a une décomposition :*

$$\mathcal{M}_k(\Gamma_1(q)) = \bigoplus_{\chi \in \mathrm{Hom}((\mathbb{Z}/q\mathbb{Z})^\times, \mathbb{C}^\times)} \mathcal{M}_k(\Gamma_0(q), \chi)$$

En particulier, les $\mathcal{M}_k(\Gamma_0(q), \chi)$ sont de dimension finie.

Preuve. On a une action $\mathbb{C}$-linéaire de $\Gamma_0(q)/\Gamma_1(q) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ sur $\mathcal{M}_1(\Gamma_1(q))$ donnée par $\gamma \cdot f = f_{|\gamma^{-1}}$. On a donc défini sur $\mathcal{M}_k(\Gamma_1(q))$ une représentation complexe du groupe abélien fini $(\mathbb{Z}/q\mathbb{Z})^\times$. Elle se décompose comme somme directe de droites (fait classique) qui prennent exactement la forme $\mathcal{M}_k(\Gamma_0(q), \chi)$ (il faut l'écrire pour s'en convaincre) pour un certain caractère de Dirichlet χ modulo q. □

2 Formes Modulaires : Fonctions L

Dans cette partie on va attacher aux formes cuspidales $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$ leurs fonctions L qui vont posséder des bonnes propriétés : un produit eulérien ainsi qu'un prolongement holomorphe sur $\mathbb{C}$ et une équation fonctionnelle. Ces fonctions L nous permettront de faire le lien plus tard entre nos formes cuspidales et certaines représentations galoisiennes. Les résultats de cette section sont présentés dans [8] aux chapitres 6 et 7.

2.1 Premières définitions

Soit $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$ et $f(z) = \sum_{n \geq 1} a_n e(nz)$ sa série de Fourier à l'infini. Pour $n \geq 1$ et $y > 0$, on a :

$$\begin{aligned}
\int_0^1 f(x+iy) e(-n(x+iy)) dx &= \int_0^1 \sum_{m \geq 1} a_m e((m-n)(x+iy)) dx \\
&= \sum_{m \geq 1} a_m \int_0^1 \exp(2i\pi(m-n)(x+iy)) dx \quad \text{(interversion justifiée par convegence normale)} \\
&= \sum_{m \geq 1} a_m \exp(-2\pi(m-n)y) \delta_{m=n} \\
&= a_n
\end{aligned}$$

Comme f est cuspidale, $\tau \mapsto (\Im \tau)^{\frac{k}{2}} f(\tau)$ est majorée sur $\mathcal{H}$ par un $C > 0$, dont on tire :

$$|a_n| \leq C y^{-\frac{k}{2}} \exp(-2n\pi y)$$

On peut alors optimiser la borne pour a_n en choisissant $y = \frac{1}{2n\pi}$ ce qui conduit à :

Proposition 2.1 (Borne de Hecke) *Soit $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$ une forme cuspidale et $f(z) = \sum_{n\geq 1} a_n e(nz)$ sa série de Fourier à l'infini. on dipose d'une constante $C > 0$ telle que pour tout $n \geq 1$:*

$$a_n \leq C n^{\frac{k}{2}}$$

Corollaire 2.2 *La série $L_f(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ attachée à une forme cuspidale f converge normalement sur les compacts de $\{\Re s > k/2 + 1\}$.*

On définit l'opérateur $W = |_w$, l'involution de Fricke, sur $\mathcal{S}_k(\Gamma_0(q), \chi)$ où $w = \left(\begin{smallmatrix} 0 & -1 \\ q & 0 \end{smallmatrix}\right)$. Cet opérateur agit par $(Wf) = z \mapsto q^{-\frac{k}{2}} z^{-k} f\left(\frac{-1}{qz}\right)$. Si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(q)$ en remarquant que $w^{-1} = -\frac{w}{q}$ on obtient :

$$wgw^{-1} = \begin{pmatrix} d & -\frac{c}{q} \\ -bq & a \end{pmatrix} \in \Gamma_0(q)$$

De sorte que w est dans le normalisateur de $\Gamma_0(q)$ i.e $w\Gamma_0(q) = \Gamma_0(q)w$.

Proposition 2.3 *L'involution de Fricke W envoie $\mathcal{S}_k(\Gamma_0(q), \chi)$ sur $\mathcal{S}_k(\Gamma_0(q), \bar{\chi})$.*

Preuve. On va admettre que W préserve bien les conditions de régularité aux pointes. Pour $g \in \Gamma_0(q)$ on a un $g' \in \Gamma_0(q)$ avec $\chi(g') = \chi(g)^{-1}$ tel que $wg = g'w$. Si $h = Wf$ pour $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$ on a donc :

$$h_{|g} = f_{|wg} = f_{|g'w} = \chi(g')Wf = \overline{\chi(g)}h$$

□

2.2 Prolongement holomorphe et équations fonctionnelles

Avec les notations précédentes, on a d'une part une forme cuspidale f de série de Fourier $f(z) = \sum_{n\geq 1} a_n e(nz)$ et d'autre part sa fonction L associée $L_f(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ dont on aimerait obtenir un prolongement entier à $\mathbb{C}$. Ces deux objets sont en fait reliés par la **transformée de Mellin**, qui donne une représentation intégrale de L_f en termes de f. Comme pour une transformation de Fourier, les propriétés de décroissance rapide de f résultent en des bonnes propriétés analytiques pour sa transformée de Mellin $\mathcal{M}_f$. Cela tombe bien, on a une telle propriété pour f car elle est cuspidale. On présente le calcul formel de transformée de Mellin de f :

$$\begin{aligned}\mathcal{M}_f(s) = \int_0^\infty f(it)t^s \frac{dt}{t} &= \int_0^\infty \sum_{n\geq 1} a_n \exp(-2\pi nt)t^{s-1}dt \\ &= \sum_{n\geq 1} \frac{a_n}{(2\pi n)^s} \int_0^\infty \exp(t')t'^{s-1}dt' \\ &= (2\pi)^{-s}\Gamma(s)L_f(s)\end{aligned}$$

On voit alors que la fonction sur laquelle il convient de travailler n'est pas exactement L_f mais une version "complétée". Onn introduit un autre facteur de normalisation dans la définition suivante pour avoir de belles équations fonctionnelles plus tard :

Définition 2.4 (Fonction L complétée) *Soit $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$. On définit sa fonction L complétée par :*

$$\Lambda_f(s) = \left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s)L_f(s)$$

On laissera le lecteur vérifier que dans le calcul précédent la transformée de Mellin de f est bien définie (CVA) et que l'interversion est justifée sur le demi-plan $\{\Re s > \frac{k}{2} + 1\}$ de sorte qu'on a sur ce demi-plan:

$$q^{\frac{s}{2}} M_f(s) = \Lambda_f(s)$$

On va enfin prouver le :

Théorème 2.5 (Hecke) *Soit $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$ une forme cuspidale et soit $g = Wf$. Alors, la fonction L complétée Λ_f admet un prolongement holomorphe à $\mathbb{C}$ entier et satisfait à l'équation fonctionnelle :*

$$\Lambda_f(s) = i^k \Lambda_g(k-s)$$

Preuve. Pour $\Re s > \frac{k}{2} + 1$ on a vu que :

$$\Lambda_f(s) = q^{\frac{s}{2}} \mathcal{M}_f(s) = \int_0^\infty q^{\frac{s}{2}} f(it) t^s \frac{dt}{t}$$

On va essayer de donner un sens au membre de droite de cette égalité pour tout $s \in \mathbb{C}$. Pour cela, on va découper notre intégrale et utiliser la relation

$$f(it) = i^k q^{-\frac{k}{2}} t^{-k} g(\frac{i}{qt})$$

On exploite la décroissance rapide de f et g à l'infini en écrivant que :

$$\forall \Re s > \frac{k}{2} + 1, \quad \Lambda_f(s) = \int_0^\infty q^{\frac{s}{2}} f(it) t^s \frac{dt}{t} = \underbrace{\int_0^1 q^{\frac{s}{2}} f(it) t^s \frac{dt}{t}}_{I_1(s)} + \underbrace{\int_1^\infty q^{\frac{s}{2}} f(it) t^s \frac{dt}{t}}_{I_2(s)}$$

Avec

$$\begin{aligned} I_1(s) = \int_0^1 q^{\frac{s}{2}} f(it) t^s \frac{dt}{t} &= i^k \int_0^1 q^{\frac{(s-k)}{2}} t^{s-k} g(\frac{i}{qt}) \frac{dt}{t} \quad \text{, en posant } u = \frac{1}{t} \\ &= i^k \int_1^\infty q^{\frac{(s-k)}{2}} u^{k-s} g(\frac{iu}{q}) \frac{du}{u} \end{aligned}$$

On a donc la relation valable pour $\Re s > \frac{k}{2} + 1$:

$$\Lambda_f(s) = i^k \int_1^\infty q^{\frac{(s-k)}{2}} u^{k-s} g(\frac{iu}{q}) \frac{du}{u} + \int_1^\infty q^{\frac{s}{2}} f(it) t^s \frac{dt}{t}$$

Maintenant, par décroisasnce rapide à l'infini de f et g le membre de droite converge absolument pour toute valeur de s. Il nous reste à vérifier que le membre de droite définit une fonction entière de s pour conclure.
Sans perte de généralités, il nous suffit de voir que I_2 est entière. On utilise le théorème d'holormoprhie à paramètres : pour $s \in \mathbb{C}$ on a $t \mapsto q^{\frac{s}{2}} f(it) t^{s-1}$ mesurable sur $[1, \infty[$, pour tout $t \geq 1$, $s \mapsto q^{\frac{s}{2}} f(it) t^{s-1}$ est entière et par décroissance rapide à l'infini de f, $(s,t) \mapsto q^{\frac{s}{2}} f(it) t^{s-1}$ a une domination intégrable indépendante de s sur tout compact $K \subset \mathbb{C}$. L'équation fonctionnelle s'obtient facilement à partir de la représentation intégrale :

$$\begin{aligned} \Lambda_f(s) = q^{\frac{s}{2}} \mathcal{M}_f(s) &= \int_0^\infty q^{\frac{s}{2}} f(it) t^s \frac{dt}{t} \\ &= i^k \int_0^\infty q^{\frac{(s-k)}{2}} t^{s-k} g(\frac{i}{qt}) \frac{dt}{t} \quad \text{posant } u = \frac{1}{qt} \\ &= i^k \int_0^\infty q^{\frac{k-s}{2}} u^{k-s} g(iu) \frac{du}{u} \\ &= i^k q^{\frac{k-s}{2}} \mathcal{M}_g(k-s) = i^k \Lambda_g(k-s) \end{aligned}$$

□

Corollaire 2.6 *Pour une forme cuspidale $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$, sa fonction L_f possède un prolongement holormorphe à $\mathbb{C}$.*

Je mentione au passage (même si je n'ai pas regardé cela en détails pendant mon stage) qu'on peut "tordre" les séries de Fourier de formes cuspidales $f(z) = \sum_{n \geq 1} a_n e(nz)$ par certains caractères de Dirichlet ψ en posant $f_\psi(z) = \sum_{n \geq 1} \psi(n) a_n e(nz)$. Sous de bonnes conditions arithmétiques sur les caractères en jeu, f_ψ sera toujours une forme cuspidale (d'un niveau supérieur q' et pour un autre caractère que χ) et on pourra parler d'une fonction complétée $\Lambda_f(s, \psi)$. On aura alors une équation fonctionnelle du même genre que celle qu'on a rencontrée qui lie $\Lambda_f(-, \psi)$ et $\Lambda_g(-, \overline{\psi})$. En fait on a même une réciproque donnée par un théorème de Weil dont l'énoncé, assez lourd, peut-être trouvé dans [8]. Grossièrement si l'on a des séries de Fourier f et g, on peut leur associer des séries L (du moins formellement), et si on a des prolongements entiers et des équations fonctionnelles liant les $\Lambda_f(-, \psi)$ et $\Lambda_g(-, \overline{\psi})$ pour suffisament de bons caractères ψ alors c'est que f et g étaient des formes cuspidales du type $\mathcal{S}_k(\Gamma_0(q), -)$ avec $f = Wg$ au départ.

2.3 L'espace hermitien $\mathcal{S}_k(\Gamma_0(q), \chi)$, opérateurs de Hecke

La mesure $d\mu(z) = \frac{dxdy}{y^2}$ sur $\mathcal{H}$ est invariante par $\mathrm{SL}_2(\mathbb{R})$. Cette mesure donne l'aire hyperbolique sur $\mathcal{H}$. Si $f, g \in \mathcal{M}_k(\Gamma_0(q), \chi)$ on peut former l'expression

$$(f, g)(z) = y^k f(z) \overline{g}(z) d\mu(z)$$

Celle-ci est alors invariante par $\Gamma_0(q)$. Sous-réserve de convergence absolue, l'intégrale suivante ne dépend pas du choix de domaine fondamental pour $\Gamma_0(q)$ (l'intégrale ne dépend pas du domaine, qui ont tous même aire hyperbolique finie, et des bords d'aire nulle) :

$$\langle f, g \rangle = \int_{\Gamma_0(q) \backslash \mathcal{H}} (f, g)(z)$$

Proposition 2.7 *Dès lors que f ou bien g est une forme cuspidale, l'intégrale précédente converge absolument. De plus, $(f, g) \mapsto \langle f, g \rangle$ définit un produit scalaire hermitien sur l'espace de dimension finie $\mathcal{S}_k(\Gamma_0(q), \chi)$, appelé* ***produit scalaire de Petersson****.*

La théorie de Hecke exploite de manière spectaculaire la structure hermitienne de cet espace et va permettre de répondre à la question de la multiplicativité des coefficients de Fourier de nos formes cuspidales et de donner un produit Eulérien aux fonctions L_f qu'on a définies et prolongées entièrement à $\mathbb{C}$.

Pour $f \in \mathcal{S}_k(\Gamma_0(q), \chi)$ on notera $f(q) = \sum_{n \geq 0} a_f(n) q^n$ son développement de Fourier à l'infini. On a une famille d'opérateurs dits de Hecke $(T_n)_{n \in \mathbb{N}}$ (qu'on ne définira pas ici) qui agissent par :

$$T_n f = \sum_{m \geq 0} a_n(m) q^m \quad \text{où : } a_n(m) = \sum_{d | (m,n)} \chi(d) d^{k-1} a_f(mnd^{-2})$$

On montre les propriétés suivantes :

$$(i). \quad T_a T_b = T_b T_a = T_{ab} \text{ si } (a, b) = 1 \qquad (ii). \quad T_{p^{n+1}} = T_{p^n} T_p - \chi(p) p^{k-1} T_{p^{n-1}} \quad \forall p \in \mathbb{P}$$

On en déduit que l'algèbre $\mathbb{Z}[T_n]_{n \in \mathbb{N}}$ est commutative engendrée par les $(T_p)_{p \in \mathbb{P}}$. Notons que plus généralement on a :

$$\forall (m, n) \in \mathbb{N}^2_{>0}, \quad T_m T_n = \sum_{d | (m,n)} \chi(d) d^{k-1} T_{mnd^{-2}}$$

On a de plus la proposition cruciale :

Proposition 2.8 *Les sous-espaces $\mathcal{M}_k(\Gamma_0(q), \chi)$ et $\mathcal{S}_k(\Gamma_0(q), \chi)$ sont stables sous l'opération des opérateurs de Hecke, qui y définissent donc des endomorphismes $\mathbb{C}$-linéaires.*

2.4 Théorie de Hecke : le cas du groupe modulaire

Dans le cas de formes modulaires de niveau 1, c'est-à-dire modulaires pour $\mathrm{SL}_2(\mathbb{Z})$, on montre que les opérateurs de Hecke sont auto-adjoints (dans S_k) pour le produit scalaire de Petersson. Les opérateurs de Hecke $(T_n)_{n\in\mathbb{N}}$ forment alors une famille commutative d'opérateurs auto-adjoints de l'espace hermitien $\mathcal{S}_k$, on peut les co-diagonaliser ce qui conduit au :

Théorème 2.9 (Hecke) *$\mathcal{S}_k$ possède une base orthonormée de fonctions propres de tous les opérateurs de Hecke.*

Soit $f = \sum_{n\geq 1} a_f(n)q^n$ une telle fonction propre. Pour $n \geq 1$ on a $T_n f = \lambda_n f$ pour un certain complexe λ_n. Mais d'autre part on sait que que :

$$T_n f = \sum_{m\geq 1} \Big(\sum_{d|(m,n)} d^{k-1} a_f(mnd^{-2}) \Big) q^m$$

En identifiant les coefficients devant q on obtient alors :

$$\forall n, \quad a_f(n) = \lambda_n a_f(1)$$

Comme $f \neq 0$, cela force à avoir $a_f(1) \neq 0$ et on peut donc normaliser f en considérant $f/a_f(1)$.

Corollaire 2.10 *Soit $f \in \mathcal{S}_k$ une fonction propre normalisée des opérateurs de Hecke. Alors, si $T_n f = \lambda_n f$ on a :*

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

Pour des fonctions propres des opérateurs de Hecke, les relations entre les opérateurs se répercutent sur les valeurs propres. Si on normalise la forme en imposant $a_f(1) = 1$ de sorte que $\lambda_n = a_f(n)$ on a alors de beaux énoncés sur les coefficients (je laisse apparent un caractère χ pour que les formules soient générales mais en niveau 1 forcément $\chi = 1$) :

Proposition 2.11 *Soit $f = \sum_{n\geq 1} a_f(n)q^n \in \mathcal{S}_k$ une fonction propre normalisée de tous les opérateurs de Hecke. On a que :*

$$a_f(n)a_f(m) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_f(mnd^{-2})$$

De sorte que la suite des coefficients $(a_f(n))_{n\in\mathbb{N}}$ est multiplicative. De plus, on a la relation de récurrence :

$$\forall p \in \mathbb{P}, \quad \forall n \geq 1, \quad a_f(p^{n+1}) = a_f(p^n)a_f(p) - \chi(p)p^{k-1}a_f(p^{n-1})$$

L'espace $\mathcal{S}_{12}$ est de dimension 1, toute forme cuspidale non-nulle de poids 12 est donc automatiquement fonction propre de tous les opérateurs de Hecke. Le discriminant modulaire Δ est de plus une forme normalisée donc la proposition précédente répond aux deux premières conjectures de Ramanujan sur la suite $(\tau(n))$!

2.5 Théorie de Hecke : le cas $\mathcal{S}_k(\Gamma_0(q), \chi)$

La situation est un peu plus complexe, la famille $(T_n)_{n\in\mathbb{N}}$ n'est plus auto-adjointe. On a en revanche que les $(T_n)_{(n,q)=1}$ sont normaux avec $T_n^* = \overline{\chi(n)} T_n$. On a donc la

Proposition 2.12 *Il existe une base orthonormée de $\mathcal{S}_k(\Gamma_0(q), \chi)$ formée de fonctions propres des $(T_n)_{(n,q)=1}$.*

Pour une telle fonction propre $f = \sum_{n\geq 1} a_f(n)q^n$ avec $T_n f = \lambda_n f$ pour $(n, q) = 1$ on déduit comme précédemment :

$$\forall (n, q) = 1, \quad \lambda_n a_f(1) = a_f(n)$$

Cette condition ne permet pas en général de conclure que $a_f(1) \neq 0$ comme on l'avait fait dans la section précédente. Pour retrouver de telles formes il va falloir en exclure certaines.
Si $q^* \mid q$ est le conducteur de χ (c'est-à-dire que χ se factorise modulo q^* mais pas modulo $q' \mid q^*$), q' est un entier tel que $q^* \mid q' \mid q$ et d un entier tel que $qd' \mid q$ on peut vérifier que si $f \in \mathcal{S}_k(\Gamma_0(q'), \chi')$ (où χ' est le caractère induit par χ modulo q') alors $(z \mapsto f(dz)) \in \mathcal{S}_k(\Gamma_0(q), \chi)$ et a un premier coefficient de Fourier nul si $d \neq 1$. On note $\mathcal{S}_k^\flat(\Gamma_0(q), \chi)$ le sous-espace engendré par les formes de ce type qu'on appelle sous-espace des formes anciennes (elles proviennent de formes de plus petit niveau).
On définit alors $\mathcal{S}_k^\sharp(\Gamma_0(q), \chi)$ comme son orthogonal pour le produit scalaire de Petersson, qui est le sous-espace des formes *nouvelles*, on a donc une décomposition en somme directe orthogonale:

$$\mathcal{S}_k(\Gamma_0(q), \chi) = \mathcal{S}_k^\flat(\Gamma_0(q), \chi) \oplus \mathcal{S}_k^\sharp(\Gamma_0(q), \chi)$$

On montre que les opérateurs de Hecke T_n pour $(n, q) = 1$ préseve cette décomposition en somme directe et ces sous-espaces possèdent donc des bases orthonormées formées de fonctions propres de ces opérateurs. Cependant dans l'espace des formes nouvelles on a un principe dit **principe de multiplicité 1** : si $(\lambda_n)_{(n,q)=1}$ est une suite de complexes alors le sous-espace de $\mathcal{S}_k^\sharp(\Gamma_0(q), \chi)$ formé de fonctions propres f des $(T_n)_{(n,q)=1}$ avec $T_n f = \lambda_n$ pour tout $(n, q) = 1$ est de dimension au plus 1. Donc si f est une forme nouvelle, fonction propre des T_n pour $(n, q) = 1$, elle appartient à une droite vetorielle stable par tous les (T_n) pour $(n, q) = 1$. On sait que tous les opérateurs de Hecke commutent donc ils stabilisent tous cette droite et ainsi f est automatiquement fonction propre de tous les opérateurs de Hecke. Une forme nouvelle fonction propre de tous les opérateurs de Hecke est appelée **forme primitive**. On a donc le théorème :

Théorème 2.13 *Le sous-espace des formes nouvelles $\mathcal{S}_k^\sharp(\Gamma_0(q), \chi)$ possède une base orthonormée constituée de formes primitives, qui sont en particulier fonctions propres de tous les opérateurs de Hecke $(T_n)_{n \geq 1}$.*

On peut donc trouver une base de formes primitives normalisées dans le sous-espace des formes nouvelles et de telles formes vérifieront les mêmes propriétés sur les coefficients/valeurs propres qu'on a citées auparavant.

Soit maintenant $f \in \mathcal{S}_1^\sharp(\Gamma_0(q), \chi)$ une forme primitive normalisée. Si $f = \sum_{n \geq 1} a_n q^n$ on sait que la suite des coefficients (a_n) est multiplicative, la fonction $L_f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ qui convergee normalement sur les compacts de $\{\Re s > \frac{3}{2}\}$ y admet donc un développement en produit Eulérien :

$$L_f(s) = \prod_{p \in \mathbb{P}} L_{f,p}(s), \quad L_{f,p}(s) = \sum_{n \geq 0} \frac{a_{p^n}}{p^{ns}}$$

D'autre part les coefficients (a_n) vérifient la relation de récurrence valable pour tout p premier :

$$a_f(p^{n+1}) = a_f(p^n) a_f(p) - \chi(p) a_f(p^{n-1})$$

Cette formule permet de calculer les facteurs Eulériens $L_{f,p}$ en prenant garde au fait que si $p \mid q$ on a $\chi(p) = 0$, on obtient finalement le produit Eulérien pour L_f valable pour $\Re s > 3/2$:

$$\boxed{L_f(s) = \prod_{p \in \mathbb{P}, p \mid q} \frac{1}{1 - a_f(p) p^{-s}} \prod_{p \in \mathbb{P}, p \nmid q} \frac{1}{1 - a_f(p) p^{-s} + \chi(p) p^{-2s}}}$$

3 Représentations Galoisiennes

Dans cette partie on va parler un peu de représentations galoisiennes ainsi que de leurs fonctions L. Cela nous permettra enfin de voir le lien (via les fonctions L) entre certaines représentations galoisiennes complexes de degré 2 et les formes modulaires de poids 1 : c'est l'objet du théorème de Deligne-Serre [2]. On aura besoin dans cette section d'un peu de théorie de Galois infinie et de théorie algébrique des nombres du cours de M1S2, pour lesquelles je renvoie à [10] et [11]. J'utilise aussi les notions vues en cours de prémaster sur les groupes topologiques.

3.1 Représentations galoisiennes de $G_{\mathbb{Q}}$

On rappelle qu'une extension galoisienne L/K (potentiellement infinie) est une extension algébrique telle que $K^{\mathrm{Aut}_K(L)} = K$. On va s'intéresser à des représentations du groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$, mais pour cela on doit d'abord dire deux mots sur ce à quoi ressemble ce groupe.
Pour commencer, l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ contient toutes les sous-extensions de corps de nombres (les extensions finies de $\mathbb{Q}$) donc $G_{\mathbb{Q}}$ contient de l'information sur énormléments de groupes de Galois intéressant d'un point de vue arithmétique. Cette richesse implique également qu'il est dur de l'étudier dans sa globalité donc on doit se restreindre à l'étudier par morceaux via ses représentations. D'un point de vue de l'arithmétique, les représenations intéressantes sont celles d'image un groupe de Galois fini et c'est là que va intervenir la notion de **représentation galoisienne**.

L'ensemble $\{K/\mathbb{Q} \mid K/\mathbb{Q} \text{ est galoisienne finie}\}$ est muni d'une structure de treillis et si on a des extensions galoisiennes $M/L/K/\mathbb{Q}$ on a des flèches de restriction $\varphi_{L,K} : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ avec $\varphi_{K,K} = \mathrm{Id}_K$ et $\varphi_{L,K} \circ \varphi_{M,L} = \varphi_{M,K}$. Ces données permettent de définir la *limite projective* de tous ces groupes de Galois qui est en quelque-sorte une limite croissante sur le treillis des groupes $\mathrm{Gal}(K/\mathbb{Q})$ pour $K/\mathbb{Q}$ galoisienne finie. Un élément de cette limite projective n'est rien d'autre qu'une famille "croissante" d'automorphismes compatible aux flèches de restriction. Formellement, cette limite est donnée par :

$$\varprojlim_{K/\mathbb{Q} \text{ Galoisienne finie}} \mathrm{Gal}(K/\mathbb{Q}) = \{(f_K) \in \prod_{K/\mathbb{Q} \text{ Galoisienne finie}} \mathrm{Gal}(K/\mathbb{Q}) \mid \forall L/K, \quad \varphi_{L,K}(f_L) = f_K\}$$

Cette limitive projective est munie d'une structure de groupe naturelle. Notons de plus que chacun de ces groupes de galois fini peut-être muni de sa topologie discrète pour laquelle c'est un groupe topologique compact et leur produit est donc compact par le théorème de Tychonoff. Leur produit est aussi totalement discontinu. On pourra vérifier que la limite projective de groupes topologiques séparés est un sous-groupe topologique fermé de leur produit. Cette limite donc également compacte et totalement discontinue. On a enfin la :

Proposition 3.1

$$G_{\mathbb{Q}} \cong \varprojlim_{K/\mathbb{Q} \text{ Galoisienne finie}} \mathrm{Gal}(K/\mathbb{Q})$$

Cette proposition montre que le groupe de galois absolu $G_{\mathbb{Q}}$ possède une structure naturelle de **groupe profini** c'est-à-dire de limite projective de groupes finis discrets ou, de manière équivalente, de groupe compact totalement discontinu. On peut alors donner la définition qui nous intéresse :

Définition 3.2 (Représentation galoisienne complexe) *Une représentation galoisienne complexe est un morphisme continu $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$.*

En quoi cette définition permet-elle de retrouver des représenations de groupes de Galois fini ? Un théorème de Van Dantzig affirme que les voisinages de l'identité dans un groupe profini contiennent tous un sous-groupe compact ouvert. Mais la théorie de Galois infinie elle caractérise les sous-groupes compacts ouverts de $G_{\mathbb{Q}}$: ce sont les $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ où $K/\mathbb{Q}$ est galoisienne finie. La topologie de $\mathrm{GL}_n(\mathbb{C})$ est elle très différente : les petits voisinages de l'identité ne contiennent pas de sous-groupes non-triviaux. Ainsi, une représentation galoisienne (complexe) se factorise par un $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathrm{K})$ pour $K/\mathbb{Q}$ galoisienne finie, de sorte qu'elle induit une représentation de :

$$G_{\mathbb{Q}}/\mathrm{Gal}(\overline{\mathbb{Q}}/\mathrm{K}) \cong \mathrm{Gal}(K/\mathbb{Q})$$

C'est alors un exercice de théorie de Galois finie de prouver la :

Proposition 3.3 *Soit ρ une représentation Galoisienne complexe. On dispose alors de $K/\mathbb{Q}$ une extension galoisienne finie telle que ρ se factorise par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathrm{K})$ et que le morphisme induit $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ est injectif.*

3.2 Fonction L d'Artin d'une représentation

Dans cette section on va attacher une fonction L aux représentations galoisiennes complexes. On va la construire dans le cas d'une représentation $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ d'une extension galoisienne finie. Maintenant, si ρ est une represénation Galoisienne de $G_{\mathbb{Q}}$ elle donne naissance à une telle represénation finie par ce qu'on a vu avant, pour laquelle on saura définir sa fonction L. On peut vérifier que le choix de factorisation n'influe pas sur la fonction L obtenue.
Pour définir une fonction $L(\rho, -)$ il semble raisonnable, du moins l'on souhaiterait, qu'elle s'exprime sous forme d'un produit Eulérien :

$$L(\rho, -) = \prod_{p \in \mathbb{P}} L_p(\rho, -)$$

Il s'agit donc de définir chacun des facteurs Eulériens. En vue de cela on a besoin d'un peu de théorie algébrique des nombres.
L'anneau des entiers $\mathcal{O}_K = \{x \in K \mid \exists P \in \mathbb{Z}[X] \text{ unitaire}, P(x) = 0\}$ est un $\mathbb{Z}$-module libre de rang fini $[K : \mathbb{Q}]$ et c'est de plus un anneau de Dedekind. Ainsi tous ses idéaux premiers sont maximaux et les idéaux se factorisent de manière unique en produits d'idéaux premiers. Soit $p \in \mathbb{P}$. On peut décomposer l'idéal $p\mathcal{O}_K$ en produits d'idéaux premiers dans $\mathcal{O}_K$:

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

On a alors que $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$, on dit que $\mathfrak{p}_i$ est *au-dessus* de p dans $\mathcal{O}_K$. On a alors que $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_{\mathfrak{p}_i}$ est une extension finie de $\mathbb{F}_p$ de degré noté f_i. En effet, comme $\mathfrak{p}_i$ est premier dans $\mathcal{O}_K$ il est maximal donc ce quotient est un corps dans lequel l'image de $p\mathcal{O}_K$ est $\{0\}$ donc en particulier de caractéristique p. La finitude vient de l'inclusion $p\mathcal{O}_K \hookrightarrow \mathfrak{p}_i$ qui par passage au quotient donne $\mathbb{F}_{\mathfrak{p}_i} \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$ qui est de cardinal $p^{[K:\mathbb{Q}]}$. Si $\mathfrak{P}$ est un idéal premier de $\mathcal{O}_K$ alors $\mathfrak{P} \cap \mathbb{Z}$ est premier dans $\mathbb{Z}$ donc s'écrit $q\mathbb{Z}$ pour q premier et $\mathfrak{P}$ est au-dessus de q dans $\mathcal{O}_K$. Les idéaux premiers de $\mathcal{O}_K$ sont donc tous au-dessus d'un certain premier de $\mathbb{Z}$.
Naturellement, le groupe $\mathrm{Gal}(K/\mathbb{Q})$ agit par permutation sur l'ensemble $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ des idéaux au-dessus de p car pour f un tel automorphisme, $f(p\mathcal{O}_K) = p\mathcal{O}_K$ et f envoie des idéaux premiers sur des idéaux premiers. Dans le cas d'une extension galoisienne, c'est un théorème connu que cette action est transitive. En particulier on a $e_1 = \ldots = e_r = e$ et $f_1 = \ldots = f_r = f$. On montre alors que : $e \cdot f \cdot r = [K : \mathbb{Q}]$.
Fixons $p \in \mathbb{P}$ et $\mathfrak{P}$ au-dessus de p. On introduit le **sous-groupe de décomposition** :

$$D_{\mathfrak{P}} = \{g \in \mathrm{Gal}(K/\mathbb{Q}) \mid g \cdot \mathfrak{P} = \mathfrak{P}\}$$

Tout élément de ce sous-groupe induit un automorphisme $\mathbb{F}_p$ linéaire du corps résiduel $\mathbb{F}_{\mathfrak{P}}$ de sorte qu'on a une flèche $D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$, où l'on rappelle que $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$ est cyclique de cardinal f engendré par le Frobenius $x \mapsto x^p$. Ce sous-groupe est de carinal $f \cdot e$ et c'est un théorème que cette flèche est surjective de sorte que son noyau, le **sous-groupe d'inertie** $I_{\mathfrak{P}} = \{g \mid g_{|\mathfrak{P}} = \mathrm{Id}\}$ est de cardinal e. On résume cela par la suite exacte courte :

$$\{0\} \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p) \cong \mathbb{Z}/f\mathbb{Z} \to \{0\}$$

Notons que si $\mathfrak{P}'$ est un autre idéal premier au-dessus de p, on a $g \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $\mathfrak{P}' = g \cdot \mathfrak{P}$ de sorte que les sous-groupes d'inerties et de décomposition sont conjugués. On voit apparaître un automorphisme important attaché au nombre premier p : l'automorphisme de Frobenius qui engendre $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$. On peut également considérer l'uniquement élément $\sigma_{\mathfrak{P}}$ du quotient $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ qui s'envoie sur ce Frobenius via l'isomorphisme précédent.
Un cas important est celui où p est *non-ramifié* dans K c'est-à-dire que $e = 1$. Dans ce cas, on a un isomorphisme $D_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$ et on a un élément, dit de Frobenius également, $\sigma_{\mathfrak{P}}$ de $D_{\mathfrak{P}}$ qui s'envoie sur le Frobenius du corps résiduel. Cet élément est défini uniquement à conjugaison près par ce qui précède. Notons que tous les nombres premiers sont ramifiés dans K sauf un nombre fini d'entre-eux, ceux qui divisent le discriminant de K.

Pour définir le facteur Eulérien en p (non-ramifié), il fait maintenant sens de s'intéresser à un invariant de conjugaison de $\rho(\sigma_{\mathfrak{P}})$ de sorte que la définition ne dépendra pas du choix de $\mathfrak{P}$. Avant de faire cela, généralisons un peu la notion de ramification :

Définition 3.4 *Soit ρ une représentation galoisienne de* $\mathrm{Gal}(K/\mathbb{Q})$ *et $p \in \mathbb{P}$. On dit que ρ est non-ramifiée en p si ρ se factorise par $I_{\mathfrak{P}}$ pour tout idéal $\mathfrak{P}$ au-dessus de p (comme ces groupes sont conjugués, il suffit de le vérifier pour un seul idéal $\mathfrak{P}$). On voit que ρ est non-ramifiée en tous les p non-ramifiés dans K.*

Si ρ est non-ramifiée en p on peut donc faire sens, à conjugaison près dans $\mathrm{GL}_n(\mathbb{C})$, de l'image σ_p du Frobenius $\sigma_{\mathfrak{P}}$ pour un idéal $\mathfrak{P}$ au-dessus de p. Supposons donc que ρ ne ramifie pas en p. On introduit le facteur d'Artin local en p :

$$L_p(\rho, s) = \det(I - \sigma_p p^{-s})^{-1}$$

C'est bien un invariant de conjugaison car c'est l'inverse de $\chi_{\sigma_p}(p^{-s})$.
On étend cette définition du facteur local au cas non-ramifié en se rappelant qu'une représentation ρ est la donnée d'une action $\mathbb{C}$-linéaire sur un espace vectoriel complexe de dimension finie V. On a alors une sous-représentation de ρ non-ramifiée en p qui est la restriction de cette action au sous-espace stable $V^{\mathfrak{P}} = \{x \in V \mid g \cdot x = x, \quad \forall g \in I_{\mathfrak{P}}\}$ (ceci fait encore sens à conjugaison près). Notons que ce sous-espace peut très bien être trivial. On obtient la définition voulue :

Définition 3.5 (Fonction L d'Artin) *Soit ρ une représentation galoisienne de $G_{\mathbb{Q}}$, vue comme représentation fidèle d'une extension galoisienne finie $K/\mathbb{Q}$. Sa fonction L est donnée par :*

$$L(\rho, s) = \prod_{p \in \mathbb{P}} L_p(\rho, s)$$

Ce produit converge normalement sur les compacts de $\{\Re s > 1\}$.

Par exemple, si ρ est la représentation triviale dans $\mathbb{C}^\times$, $L_p(\rho, s) = ((1 - p^{-s}))^{-1}$ de sorte que $L(\mathrm{triv}, -) = \zeta$.

3.3 Le théorème de Deligne-Serre

Soit ρ une représentation galoisienne complexe de degré 2, c'est-à-dire à valeurs dans $\mathrm{GL}_2(\mathbb{C})$. On pose $\chi = \det \circ \rho$ qui est un caractère de $G_{\mathbb{Q}}$. Pour le calcul de $L(\rho, -)$, il s'agit de calculer les facteurs d'Artin locaux $L_p(\rho, -)$ en chaque $p \in \mathbb{P}$. On a deux cas :
- Si ρ est non-ramifiée en p, on a alors $L_p(\rho, s) = \frac{1}{\det(I_2 - \sigma_p p^{-s})} = \frac{1}{1 - \mathrm{Tr}(\sigma_p)p^{-s} + \chi(\sigma_p)p^{-2s}}$.
- Si ρ est ramifiée en p on a alors $L_p(\rho, s) = 1$ ou $L_p(\rho, s) = \frac{1}{1 - \mathrm{Tr}(\sigma_p)p^{-s}}$.
Au total, on obtient :

$$\boxed{\forall \Re s > 1, \quad L(\rho, s) = \prod_{p \text{ ramifié}, L_p(\rho, -) \neq 1} \frac{1}{1 - \mathrm{Tr}(\sigma_p)p^{-s}} \prod_{p \text{ non ramifié}} \frac{1}{1 - \mathrm{Tr}(\sigma_p)p^{-s} + \chi(\sigma_p)p^{-2s}}}$$

Le nombre de nombres premiers où ρ ramifie étant fini, cette fonction L ressemble fortement à celle précédemment obtenue pour les formes primitives normalisées en poids 1. Cette correspondance est tout l'objet du théorème de Deligne-Serre [2].

Théorème 3.6 (Deligne-Serre, 1974) *Soit $q \geq 1$ un entier, χ un caractère de Dirichlet impair modulo q et $f \in \mathcal{S}_1(\Gamma_0(q), \chi)$ non-nulle une forme primitive normalisée. On écrit $f(z) = \sum_{n \geq 1} a_n e(nz)$ son déveoppement de Fourier à l'infini. On a alors une représentation galoisienne irréductible de degré 2, ρ_f de $G_{\mathbb{Q}}$ qui est ramifiée exactement en les diviseurs premiers de q et telle que :*

$$\begin{aligned} &i. \quad \forall p \nmid q, \quad \mathrm{Tr}(\sigma_p) = a_p \\ &ii. \quad \forall p \nmid q, \quad \det \sigma_p = \chi(p) \\ &iii. \quad L_f = L(\rho, -) \end{aligned}$$

Cette représentation est unique à isomorphisme près.

Notons qu'il existe un théorème dû à Langlands-Weil [2] qui réalise la construnction dans l'autre sens, d'où une bijection entre formes primitives normalisées de poids 1 et certaines classes d'isomorphismes de représentations galoisiennes complexes irréductibles de degré 2.

4 Chute de dimension pour $\mathcal{S}_1(\Gamma_0(q), (\frac{\cdot}{q}))$

Réduction du problème

Rappelons notre objectif initial d'estimer la dimension de $\mathcal{S}_1(\Gamma_0(q), \chi)$. Supposons q premier impair de sorte que $\mathcal{S}_1(\Gamma_0(q), k) = \mathcal{S}_1^\sharp(\Gamma_0(q), \chi)$ avec $\chi impair$ de sorte à avoir des formes non-nulles.
On sait alors que $\mathcal{S}_1(\Gamma_0(q), \chi)$ possède une base de formes primitives normalisées. Mais on sait maintenant par le théorème de Deligne-Serre que si $f \in \mathcal{S}_1(\Gamma_0(q), \chi)$ est une forme primitive normalisée on a une (unique) représentation galoisienne irréductible de degré 2 associée ρ_f avec $L_f = L(\rho,)$. On a vu que $\operatorname{Im} \rho_f$ est isomorphe à un groupe de Galois d'une extension finie de $\mathbb{Q}$, en particulier c'est un sous-groupe fini de $\mathrm{GL}_2(\mathbb{C})$. Un invariant qu'on va associer à f est l'image projective dans $\mathrm{PGL}_2(\mathbb{C})$ de ρ_f, sous-groupe fini de $\mathrm{PGL}_2(\mathbb{C})$. On a alors la :

Proposition 4.1 *A isomorphisme près, les sous-groupes finis de* $\mathrm{PGL}_2(\mathbb{C})$ *sont : cycliques, dihédraux,* $\mathfrak{A}_4$, $\mathfrak{S}_4$ *ou bien* $\mathfrak{A}_5$.

Proposition 4.2 *L'image projective de ρ_f ne peut pas être cyclique.*

Preuve. Si l'image de ρ_f dans $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^\times I_2$ est cyclique on en déduit que $\operatorname{Im} \rho_f$ est commutatif. On a vu que ρ_f pouvait être vue comme représentation fidèle d'un $\mathrm{Gal}(K/\mathbb{Q})$ pour $K/\mathbb{Q}$ galoisienne finie, en particulier c'est une représentation irréductible complexe d'un G.A.F, qui sont toutes de dimension 1, absurde. □

On dira alors de f qu'elle est dihédrale, tétrahédrale, octahédrale ou icosahédrale suivant que son image projective est dihédrale, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.
Dans son article Duke [5] considère le cas $\chi = (\frac{\cdot}{q})$ le symbole de Legendre, on notera alors $S_1(q)$ pour l'espace des formes cuspidales et $N_1(q)$ l'ensemble des formes primitives normalisées. Comme on a une base de formes primitives normalisées, on en déduit :

$$\dim S_1(q) \ll |N_1(q)|$$

C'est un résultat de Serre ([5], Proposition 2.b) que pour $f \in N_1(q)$, f ne peut pas être tétahédrale. On a donc :

$$|N_1(q)| = |N_{\mathrm{dih}}(q)| + |N_{\mathrm{oct}}(q)| + |N_{\mathrm{ico}}(q)|$$

Je réfère à l'annexe pour une explication brève de comment Duke a estimé $|N_{\mathrm{oct}}(q)|$ & $|N_{\mathrm{ico}}(q)|$. On va parler un peu des formes dihédrales dans le paragraphe qui suit.

Exemples de formes de poids 1

Avant de conclure le rapport, j'aimerais revenir sur une question laissée en suspend au fil du rapport : comment construire des formes modulaires de type $(\Gamma_0(q), \chi)$. Pour le poids $k \geq 3$ on peut construire une famille génératrice de l'espace des formes cuspidales grâce aux séries de Poincaré ([8] chapitre 3), j'explique grossièrement l'idée en annexe.
Donner des exemples de formes modulaires de poids 1 est en fait quelque-chose de beaucoup plus compliqué. On en a rencontré une en introduction, ϑ^2 est modulaire de type $\mathcal{S}_1(\Gamma_0(4), \chi_{-1})$ (le seul caractère non-trivial modulo 4).

Par soucis d'exhaustivité je cite une autre construction que je ne maîtrise pas. Dans le cas $q = 3 \mod 4$ impair, ([8] chapitre 12 , [5]) il est construit des formes cuspidales de la forme :

$$\theta_\psi(z) = \sum_{I \leq \mathcal{O}_K} \psi(I) e(N(I)z)$$

Où ψ est un caractère du groupe de classe [10] du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-q})$ et où la somme porte sur les idéaux de $\mathcal{O}_K$, avec $N(I) = |\mathcal{O}_K/I|$. C'est un résultat de Serre ([5], [12]) que les formes de type dihédral sont précisément les formes induites par un caractère du groupe de classe. D'après Iwaniek, la modularité de telles formes peut être obtenue à partir des théorèmes réciproques de Weil que j'avais rapidement évoqués. D'après Duke, c'est en général un problème compliqué d'expliciter des formes cuspidales en poids 1 qui ne sont pas du type dihédral. On retiendra la conséquence suivante : pour majorer $|N_{\text{dih}}(q)|$ il nous suffit de majorer h_q le nombre de classe du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-q})$. On peut obtenir une telle majoration à partir de la **formule analytique du nombre de classes** pour un corps quadratique imaginaire [10] et **l'inégalité de Pólya-Vinogradov** [1], cela conduit à :

$$h_q \ll \sqrt{q} \log q$$

5 Conclusion & déroulé du stage

Conclusion

On a pu voir que que les formes cuspidales possédaient des fonctions L qui avaient des propriétés analytiques intéressantes : un prolongement entier à $\mathbb{C}$, une équation fonctionnelle pour leurs complétées Λ_f liant les valeurs en s et $1-s$ et un produit Eulérien dans le cas de formes propres primitives normalisées.
Les représentations galoisiennes complexes ρ possèdent des fonctions L qui héritent également de leur lot de propriété : un produit Eulérien, et les coefficients d'indice premier p de $L(\rho, -)$ où ρ n'est pas ramifiée en p sont somme de deux racines de l'unité.

La comparaison de la forme des fonctions L pour des formes propres normalisées de poids 1 et de représentations galoisiennes complexes de degré 2 suggère que ces deux objets sont liés : c'est l'objet des théorème de Deligne-Serre et de Langlands-Weil.
On obtient alors des identités entre fonctions L de différentes natures : $L_f = L(\rho, -)$. Cela permet de voir par exemple que $L(\rho, -)$ a un prolongement entier et une équation fonctionnelle liant les valeurs en s et $1-s$, ce qui est une propriété difficile à établir en toute généralité pour fonctions L d'Artin de représentations galoisiennes (conjecture d'Artin).

Cette bijection permet de voir l'espace $\mathcal{S}_1(\Gamma_0(q), \chi)$ du point de vue des représentations galoisiennes. C'est alors en combinant des propriétés analytiques connues des formes modulaires à des propriétés arithmétiques fortes qui proviennent du monde des représentations galoisiennes (et de J.P Serre) que Duke a réussi à établir son résultat de chute de dimension pour l'espace $\mathcal{S}_1(\Gamma_0(q), \chi)$.

Remerciements & déroulement du stage

Je tiens à remercier mon encadrant Didier Lesesvre pour avoir proposé et encadré ce stage. Je le remercie également pour sa disponibilité pour échanger et converser sur les points où j'avais des difficultés, bien que ce rapport ne reflète pas vraiment les parties plus analytiques dont on a longuement discuté.

Le stage s'est déroulé dans le Laboratoire Paul Painlevé de l'Université de Lille. J'ai pu prendre part à la conférence Arithmétique en Plat Pays (APP été 2024) qui avait lieu sur place. Je remercie les organisateurs et organisatrices de cette journée.

6 Annexe A : Majoration de $|N_{\mathbf{ico}}(q)|$

Expliquons rapidement les grandes lignes de la démarche de Duke pour obtenir une majoration de $|N_{\text{ico}}(q)|$, le cas octahédral étant analogue. Dans un premier temps, Duke établit une inégalité de grand crible :

Proposition 6.1 *Soit B une base orthogonale de $S_1(q)$, pour $f \in B$ on écrit son développement de Fourier $f(z) = \sum_{n\geq 1} a_f(n)e(nz)$. Alors, pour tout $(c_n) \in \mathbb{C}^{\mathbb{N}}$ et $N \geq 1$ (de manière uniforme en q, f, B):*

$$\sum_{f\in B} \Big| \sum_{n\leq N} c_n a_f(n) \Big|^2 \ll \langle f, f\rangle (1 + \frac{N}{q}) \sum_{n\leq N} |c_n|^2$$

D'autre part, par une application de la méthode dite de Rankin-Selberg (voir [7] qui explique un cas basique) il obtient pour $f \in N_1(q)$ (avec une constante uniforme) :

$$\langle f, f\rangle \ll q \log^3 q$$

Rappelons que comme f est icosahédrale, l'image projective de ρ_f est isomorphe à $\mathfrak{A}_5$ qui est d'ordre 60. On sait également par le théorème de Deligne-Serre que les $a_f(p)$ pour $p \neq q$ premiers sont somme de deux valeurs propres de $\overline{\rho_f(\sigma_p)} \in \overline{\operatorname{Im} \rho_f} \cong \mathfrak{A}_5$. Ces valeurs propres sont des racines 60-ème de l'unité. Comme le symbole de Legendre est à valeurs dans $\{\pm 1\}$, on a alors pour λ_p, μ_p deux racines 120-ème de l'unité :

$$\forall p \neq q, \quad \left(\frac{p}{q}\right) a_f(p) = \lambda_p + \mu_p$$

On peut alors utiliser les relations de Hecke qui montrent que :

$$\forall p \neq q, \left(\frac{p}{q}\right) a_f(p^2) = \left(\frac{p}{q}\right) (\lambda_p + \mu_p)^2 - 1$$

Tout cela pour dire que les $\left(\frac{p}{q}\right) a_f(p^2)$ ne peuvent prendre qu'un nombre assez limité de valeurs. Une analyse très fine due à Serre ([5] Proposition 2.b, [12]) conduit en fait à :

$$\forall p \neq q, \left(\frac{p}{q}\right) a_f(p^2) \in \left\{-1, 0, 3, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$$

Cela permet d'établir la

Proposition 6.2 (Duke) *Soit $f \in N_1(q)$ de type icosahédral. Alors, pour $p \neq q$ premier on a :*

$$a_f(p^{12}) - a_f(p^8) - \left(\frac{p}{q}\right) a_f(p^2) = 1$$

Preuve. On note ε le symbole de Legendre modulo q dans le reste de la preuve et on rappelle qu'alors $\varepsilon^2 = 1$. Comme f est une forme propre de Hecke normalisée, on sait que pour $m, n \geq 1$:

$$a_f(n)a_f(m) = \sum_{d|(m,n)} \varepsilon(d) a_f(mnd^{-2})$$

Soit $p \neq q$ premier, on utilise la relation précédente pour le couple (p^2, p^{2n}) ce qui conduit à :

$$a_f(p^{2(n+1)}) = (a_f(p^2) - \varepsilon(p))a_f(p^{2n}) - a_f(p^{2(n-1)})$$

En multipliant cette relation par $\varepsilon(p)^{n+1}$ et en notant $x = \varepsilon(p)a_f(p^2)$ et $u_n = \varepsilon(p)^n a_f(p^{2n})$ on obtient alors :

$$u_{n+1} = (x-1)u_n - u_{n-1}$$

Avec les conditions initiales $u_0 = 1$ et $u_1 = x$. On peut alors calculer les premiers termes de la suite (u_n) par récurrence et remarquer que :

$$u_6 - u_4 - u_1 = x(x+1)(x-2)(x-3)(x^2-x-1)+1$$

Finalement, comme $x \in \{-1, 0, 3, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\}$ et par définition des (u_n) on trouve bien que :

$$a_f(p^{12}) - a_f(p^8) - \left(\frac{p}{q}\right) a_f(p^2) = 1$$

□

Notons que le cas octahédral donne une relation analogue. On pourrait aussi obtenir une relation beaucoup moins fine que celle-là et quand même obtenir une borne en $q^{1-\varepsilon}$ pour $|N_{\text{ico}}(q)|$ mais moins fine que celle de Duke. On peut enfin prouver le :

Théorème 6.3 (Duke) *On a, de manière uniforme en q :*

$$|N_{ico}(q)| \ll q^{11/12} \log^4 q$$

Preuve. On note que deux formes propres de Hecke normalisées distinctes sont orthogonales pour le produit de Petersson. C'est une conséquence du principe de multiplicité 1 et de la normalité des opérateurs de Hecke. Soit alors B est une base orthogonale de $S_1(q)$ contenant $N_{1,\text{ico}}(q)$. On applique l'inégalité de grand crible en utilisant la majoration $\langle f, f\rangle \ll q \log^3 q$:

$$\sum_{f \in N_{\text{ico}}(q)} \left| \sum_{n \le N} c_n a_f(n) \right|^2 \ll (q+N) \log^3 q \sum_{n \le N} |c_n|^2$$

On spécialise en $N = q$ avec les (c_n) choisis pour exploiter la relation exhibée précédemment:

$$c_n = \begin{cases} 1 & \text{si } n = p^{12} \le q, \\ -1 & \text{si } n = p^8, p \le q^{1/12}, \\ -\left(\frac{p}{q}\right) & \text{si } n = p^2, p \le q^{1/12}, \\ 0, & \text{sinon.} \end{cases}$$

On obtient alors :

$$|N_{\text{oct}}(q)| \cdot \pi(q^{1/12})^2 \ll q \log^3 q \pi(q^{1/12})$$

Où π est la fonction de comptage des nombres premiers. Par le théorème des nombres premiers, on a $\pi(q^{1/12}) \sim \frac{12q^{1/12}}{\ln q}$, d'où finalement :

$$|N_{\text{oct}}(q)| \ll q^{11/12} \log^4 q$$

□

7 Annexe B : Séries de Poincaré et Eisenstein

On va construire des formes cuspidales de type $(\Gamma_0(q), \chi)$. En quelque-sorte, les formes modulaires les plus simples auxquelles on peut penser sont les fonctions 1-périodique qui sont modulaires pour le groupe de translation $\Gamma_\infty = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\} = \langle T \rangle$ où $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ agit par $z \mapsto z+1$. C'est seulement un sous-groupe de $\Gamma_0(q)$ mais on va pouvoir construire des formes modulaires sur $\Gamma_0(q)$ grâce à elles.

Voyons comment construire des formes modulaires plus générales à partir d'un sous-groupe dans un cas simple. Soit χ un morphisme de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{C}^\times$ pour un certain $n \geq 1$ et f une fonction n-périodique. On va chercher à construire g une fonction telle que $g(x+i) = \chi(i)g(x)$ pour tout x i.e $g(T \cdot) = \chi(T)g$. On part de :

$$\mathbb{Z} = \bigsqcup_{i=0}^{n-1} n\mathbb{Z} + i$$

Choisissons g sous forme de moyenne pondérée par χ sur les classes : $g = \sum_{i=0}^{p-1} \chi^{-1}(i) f \circ T^i$. On a alors :

$$g \circ T = \sum_{i=0}^{p-1} \chi^{-1}(i) \cdot f \circ T^i \circ T = \sum_{i=0}^{p-1} \chi^{-1}(T^{-1}i) \cdot f \circ T^i = \chi(T)g$$

Suivant la même idée, à partir de fonctions 1-périodiques, c'est-à-dire automorphes pour Γ_∞ on va construire des séries en moyennant sur les classes $\Gamma_\infty \backslash \Gamma_0(q)$, qui seront modulaires de type $(\Gamma_0(q), \chi)$.

Définition 7.1 (Séries de Poincaré) *Soit $m \geq 0$, $q \geq 1$ et χ un caractère de Dirichlet modulo q. La m-ème série de Poincaré (de poids $k \geq 3$, pour le caractère χ) est définie par :*

$$P_m(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(q)} \overline{\chi(\gamma)} j_\gamma(z)^{-k} e(m\gamma z)$$

Illustrons formellement pourquoi cette série est modulaire de type $(\Gamma_0(q), \chi)$. Soit donc $\lambda \in \Gamma_0(q)$, on a :

$$\begin{aligned}
(P_m)_{|\lambda}(z) = j_\lambda(z)^{-k} P_m(\lambda z) &= j_\lambda(z)^{-k} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(q)} \overline{\chi(\gamma)} j_\gamma(\lambda z)^{-k} e(m\gamma\lambda z) \\
&= \sum_{\omega \in \Gamma_\infty \backslash \Gamma_0(q)} \overline{\chi(w\lambda^{-1})} j_{\omega\lambda^{-1}}(\lambda z)^{-k} j_\lambda(z)^{-k} e(m\omega z) \quad \text{où : } \omega = \gamma\lambda \\
&= \chi(\lambda) \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(q)} \overline{\chi(\gamma)} j_{\gamma\lambda^{-1}}(\lambda z)^{-k} j_\lambda(z)^{-k} e(m\gamma z) \\
&= \chi(\lambda) P_m(z) \quad \text{en utilisant deux fois 1.2}
\end{aligned}$$

Pour les propriétés analytiques, on pourra regarder [8] chapitre 3. On résume cela par la :

Proposition 7.2 *Si $k \geq 3$ et $m \geq 1$ alors $P_m \in \mathcal{S}_k(\Gamma_0(q), \chi)$. Les séries de Poincaré $(P_m)_{m \geq 1}$ engendrent l'espace des formes cuspidales. On a aussi, toujours pour $k \geq 3$, $P_0 \in \mathcal{M}_k(\Gamma_0(q), \chi)$.*

La série de Poincaré de poids 0 est appelée **série d'Eisenstein** de poids k. Dans le cas $q = 1$, la série de Poincaré de poids $k \geq 3$ pair, notée E_k, est un élément de $\mathcal{M}_k$. On a une description simple des classes de $\mathrm{SL}_2(\mathbb{Z})$ modulo Γ_∞ : $\Gamma_\infty A = \Gamma_\infty B$ si et seulement si A et B ont même ligne inférieure. Ainsi, on a un ensemble de représentants en choisissant les entiers $(c, d) \neq (0, 0)$ premiers entre-eux. On a donc la formule explicite :

$$E_k(z) = \sum_{\substack{(n,m) \neq (0,0) \\ (m,n)=1}} (nz+m)^{-k}$$

Annexe C : Domaine Fondamental pour $\mathrm{SL}_2(\mathbb{Z})$

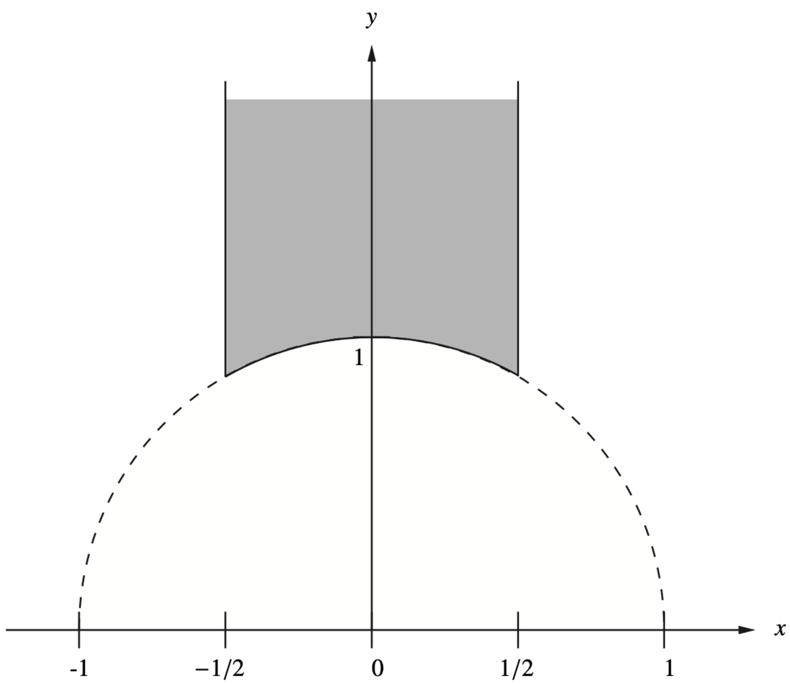

Figure 1: Domaine fondamental pour $\mathrm{SL}_2(\mathbb{Z})$, illustration tirée de [6]

Bibliographie

[1] Shubhrajit Bhattacharya and Reginald Simpson. *The Pólya-Vinogradov inequality*. URL: https://personal.math.ubc.ca/~gerg/teaching/613-Winter2023/PVI.pdf.

[2] Pierre Deligne and Jean-Pierre Serre. "Formes modulaires de poids 1". In: Annales scientifiques de l'É.N.S n°4 7 (1974). URL: http://www.numdam.org/article/ASENS_1974_4_7_4_507_0.pdf.

[3] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Vol. 228. Graduate Texts in Mathematics. Springer Verlag, 2005.

[4] Gabriel Dospinescu. *Introduction rapide aux formes modulaires*. URL: http://perso.ens-lyon.fr/gabriel.dospinescu/formes%20modulaires.pdf.

[5] W. Duke. "The dimension of the space of cusp forms of weight one". In: International Mathematics Research Notices 2 (1995). URL: https://arxiv.org/pdf/math/9411212.

[6] Philipp Fleig. *Eisenstein series and automorphic representations*. 2016. URL: https://arxiv.org/pdf/1511.04265.

[7] Paul Garrett. *Basic Rankin-Selberg*. URL: https://www-users.cse.umn.edu/~garrett/m/v/basic_rankin_selberg.pdf.

[8] Henryk Iwaniec. *Topics in Classical Automorphic Forms*. Vol. 17. Graduate Studies in Mathematics. American Mathematical Society, 2005.

[9] Svetlana Katok. *Fuchsian Groups*. Vol. 17. Chicago Lectures in Mathematics. The University of Chicago Press, 1992.

[10] Daniel A. Marcus. *Number Fields*. Universitext. Springer, 2018.

[11] Jürgen Neukirch. *Algebraic Number Theory*. A Series of Comprehensive Studies in Mathematics. Springer Berlin, 1999.

[12] Jean-Pierre Serre. "Modular forms of weight one and Galois representations". In: Oeuvres - Collected Papers III (1977).