Relations entre le nombre de classes et les formes modulaires

Mémoire

David Ayotte

Maîtrise en mathématiques - avec mémoire
Maître ès sciences (M. Sc.)

Québec, Canada

Relations entre le nombre de classes et les formes modulaires

Mémoire

David Ayotte

Sous la direction de:

Antonio Lei, directeur de recherche

Résumé

En 2010, Dummigan et Heim ont démontré deux résultats en lien avec le nombre de classes du corps quadratique $\mathbb{Q}(\sqrt{-p})$, dénoté $h(-p)$, et l'espace des formes cuspidales de poids k pour $\mathrm{SL}_2(\mathbb{Z})$, dénoté $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, où $p \equiv 3 \pmod 4$ est un premier et $k = (p+1)/2$. Ainsi, dans ce mémoire, on s'intéresse à présenter les démonstrations de Dummigan et Heim avec davantage de détails et de généraliser leurs résultats.

Tout d'abord, le premier résultat affirme que la trace de la fonction L carrée symétrique, un nombre rationnel qui dépend uniquement du poids de l'espace $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, possède un unique facteur de p au dénominateur si et seulement si $h(-p) > 1$. De plus, si $h(-p) = 1$, alors la trace ne contient aucun facteur de p. Ainsi, en utilisant les congruences de Kummer pour les nombres de Bernoulli, on démontre qu'il est possible de généraliser ce résultat pour l'espace $\mathcal{S}_{k'}(\mathrm{SL}_2(\mathbb{Z}))$ où $k' \equiv k \pmod{p-1}$. En rapport avec ce résultat, une conjecture est énoncée et des évidences numériques avec PARI/GP sont données.

Ensuite, Dummigan et Heim ont démontré, en utilisant la théorie des représentations galoisiennes, qu'il existe une forme cuspidale $f = \sum_{n \geq 1} a_n q^n$ de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ qui satisfait une congruence diédrale en p, c'est-à-dire $p \mid a_\ell$ pour tout premier ℓ tel que $(\frac{\ell}{p}) = -1$, si et seulement si $h(-p) > 1$. À l'aide de la famille d'Hida d'une forme modulaire et de la série d'Eisenstein de poids $p-1$, on démontre de deux façons que ce résultat est également vrai pour l'espace $\mathcal{S}_{k'}(\mathrm{SL}_2(\mathbb{Z}))$ où $k' \equiv k \pmod{p-1}$.

Table des matières

As conquerors, we search
interconnections through those
dimensions

The Axiom – Beyond Creation

Remerciements

Tout d'abord, je tiens à remercier profondément mon superviseur Antonio Lei. Grâce à ses conseils, sa patience infinie et son appui financier, il a su me guider tout au long de ma maîtrise. Ensuite, des remerciements sont dûs au Département de mathématiques et de statistique de l'Université Laval pour leur appui financier et pour m'avoir permis de travailler sur divers projets. Merci à tous les professeurs du département pour votre passion. En particulier, je remercie les professeurs Hugo Chapdelaine et Michael Lau avec qui j'ai suivi des cours très intéressants dans le domaine de l'algèbre et la théorie des nombres. Merci à Nicolas Simard de m'avoir aidé avec PARI/GP. Je remercie mes parents, Cathy et Bertrand, pour leur support moral. Finalement, je ne pourrai jamais remercier assez ma copine, Alexandra, qui a toujours été là pour moi.

Introduction

L'étude du nombre de classes d'un corps de nombres est un sujet encore d'actualité aujourd'hui en mathématiques. En effet, rappelons que le nombre de classes d'un corps de nombres est défini comme l'ordre du quotient du groupe des idéaux fractionnaires par le groupe des idéaux fractionnaires principaux de l'anneau des entiers. Le nombre de classes, qui est une quantité finie par la théorie de la géométrie des nombres de Minkowski, mesure si l'anneau des entiers est un domaine à factorisation unique ou non. Ainsi, une bonne compréhension du nombre de classes nous donne de l'information sur une propriété algébrique importante de notre corps de nombres. Le nombre de classes est une quantité qui possède encore des questions ouvertes. Par exemple, Gauss a conjecturé qu'il existe un nombre infini de corps quadratiques réels avec un nombre de classes de 1. Dans ce mémoire, on s'intéresse à généraliser deux résultats concernant le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$ et les formes modulaires de poids k pour le groupe modulaire $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$, où p est un premier congru à 3 modulo 4 et $k = (p+1)/2$.

Brièvement, une forme modulaire f de poids k pour $\Gamma(1)$ est une fonction holomorphe définie sur le demi-plan supérieur $\mathbb{H}$ qui satisfait une certaine condition de croissance à l'infinie et qui satisfait la condition d'invariance suivante :

$$f\Big(\frac{a\tau+b}{c\tau+d}\Big) = (c\tau+d)^k f(\tau), \text{ pour chaque } \tau \in \mathbb{H} \text{ et } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Cette propriété d'invariance implique que f possède un développement de Fourier de la forme $f(\tau) = \sum_{n\geq 0} a_n e^{2\pi i n\tau},\ a_n \in \mathbb{C}$. Si $a_0 = 0$, alors on dit que f est une forme cuspidale et l'espace des formes cuspidale de poids k pour $\Gamma(1)$ est dénoté $\mathcal{S}_k(\Gamma(1))$. On peut associer à une telle forme cuspidale une fonction L définie par $L(f,s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ pour $\Re(s) > k/2+1$. Si f est une fonction propre pour tous les opérateurs de Hecke, une suite d'opérateurs linéaires, et qu'elle est normalisée, c'est-à-dire le premier coefficient non nul de f est 1, alors la fonction $L(f,s)$ admet le produit eulérien suivant :

$$L(f,s) = \prod_q \frac{1}{(1-\alpha_q q^{-s})(1-\beta_q q^{-s})}$$

où α_q et β_q sont tels que $\alpha_q+\beta_q = a_q$ et $\alpha_q\beta_q = q^{k-1}$. La fonction $L(f,s)$ est en fait la fonction L associée à une représentation du groupe de Galois d'une clôture algébrique de $\mathbb{Q}$ qui peut

être définie à partir de f. Si $\mathrm{Sym}^2(f)$ est le carré symétrique de la représentation associée à f, alors la fonction la fonction L associée à $\mathrm{Sym}^2(f)$ est définie par

$$L(\mathrm{Sym}^2(f), s) := \prod_{\text{premier } q} \frac{1}{(1-\alpha_q^2 q^{-s})(1-\alpha_q\beta_q q^{-s})(1-\beta_q^2 q^{-s})},$$

pour $s \in \mathbb{C}$ et $\Re(s) > k$. Une propriété importante à noter de la fonction L carré symétrique est qu'elle admet un prolongement analytique sur tout le plan complexe. Une autre propriété est que les entiers $k, k+2, \ldots, 2k-2$ sont des points d'évaluation spéciaux de $L(\mathrm{Sym}^2(f), s)$. En effet, si s est un entier pair entre k et $2k-2$, alors la valeur de $L(\mathrm{Sym}^2(f), s)$ sera un facteur algébrique multiplié par certaine puissance de π et la norme de f. Ainsi, la trace de la fonction L carrée symétrique pour la valeur spéciale $s \in \{k, k+2, \ldots, 2k-2\}$ est définie comme étant la somme des facteurs algébriques par rapport à la base de formes propres normalisées de $\mathcal{S}_k(\Gamma(1))$. Cette trace a pour propriété d'être un nombre rationnel qui dépendra de k et du choix de la valeur spéciale, ce qui permettra de s'intéresser à des questions de p-divisibilité de la trace.

Dummigan et Heim ont démontré en 2010 [DH10, Theorems I et II] que la présence d'un unique facteur de p au dénominateur de la trace pour un espace de poids $k = (p+1)/2$ et pour le point spécial $s = 2k-2$ est équivalent au fait que $h(-p) > 1$. De plus, si le nombre de classes est 1, alors la trace ne contiendra aucun facteur de p. Pour parvenir à ce résultat, les deux auteurs ont obtenu une formule explicite de la trace en termes des nombres de Bernoulli en utilisant une formule de relèvement pour une série d'Eisenstein de Siegel de degré 2. Dans ce mémoire, nous allons démontrer qu'il est possible d'étendre en partie ce résultat pour des valeurs de poids k' telles que $k' \equiv k \pmod{p-1}$, en utilisant les congruences de Kummer des nombres de Bernoulli.

Le deuxième résultat de Dummigan et Heim [DH10, Theorem III] concerne les congruences diédrales en p des formes cuspidales de poids k et niveau 1. On dit que $f = \sum_{n=1}^{\infty} a_n q^n$ satisfait une *congruence diédrale en p* si $p \mid a_\ell$ pour tout premier ℓ tels que $(\ell/p) = -1$. En se servant de la théorie des représentations galoisiennes modulo p, les auteurs ont prouvé qu'il existe une forme propre normalisée satisfaisant une congruence diédrale en p si et seulement si $h(-p) > 1$. Par exemple, si $p = 23$, alors $k = 12$. La seule forme cuspidale propre normalisée de poids 12 est le discriminant modulaire

$$\begin{aligned}\Delta &:= q\prod_{n=1}^{\infty}(1-q^n)^{24} \\ &= \sum_{n=1}^{\infty}\tau(n)q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6049q^6 - 16744q^7 + \cdots .\end{aligned}$$

Observons que

$$\tau(5) = 4830 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \mathbf{23};$$
$$\tau(7) = -16744 = -2^3 \cdot 7 \cdot 13 \cdot \mathbf{23};$$
$$\tau(11) = 534612 = 2^2 \cdot 3 \cdot 13 \cdot \mathbf{23} \cdot 149;$$
$$\tau(17) = -6905934 = -2 \cdot 3 \cdot 7 \cdot \mathbf{23} \cdot 2383.$$

Ceci n'est pas une coïncidence, puisque que le nombre de classes de $\mathbb{Q}(\sqrt{-23})$ est 3. Dans ce mémoire, à l'aide des séries d'Eisenstein ainsi que de la théorie des familles d'Hida, nous allons donner deux démonstrations que le théorème de Dummigan et Heim, qui se concentre seulement en un poids k, est également vrai pour tous les poids k' tels que $k' \equiv k \pmod{p-1}$.

Le présent mémoire est séparé en cinq chapitres. Dans le premier chapitre, la fonction L carrée symétrique est définie et certaines de ses propriétés sont présentées. La trace est également définie dans le but d'énoncer précisément le premier théorème de Dummigan et Heim. Ensuite, le deuxième chapitre est une brève introduction à la théorie des formes modulaires de Siegel dans le but de comprendre certains outils qui seront utilisés, tels que l'opérateur de Siegel et l'expansion de Fourier. Le troisième chapitre est consacré à la démonstration du premier résultat de Dummigan et Heim et de sa généralisation. Aussi, une conjecture en lien avec la généralisation sera formulée. Dans le quatrième chapitre, une exposition de la théorie des représentations galoisienne est donnée afin d'expliquer la démonstration du deuxième résultat de Dummigan et Heim à propos des congruences diédrales. On retrouvera également dans ce chapitre quelques faits sur la théorie des familles d'Hida pour généraliser le deuxième résultat. Enfin, le chapitre 5 est une exposition des calculs numériques que l'on peut effectuer à l'aide de PARI/GP. Le but de ce chapitre est de présenter les fonctionnalités du logiciel en lien avec les formes modulaires. On y discutera également des résultats expérimentaux obtenus pour la conjecture énoncée au chapitre 3 et d'autres horizons qui auraient pu être étudiés.

Chapitre 1

La fonction L carrée symétrique d'une forme modulaire

Dans ce chapitre, nous définissons la fonction L carrée symétrique associée à une forme modulaire. Cette fonction L possède certaines propriétés fort utiles. En particulier, elle possède un lien avec la norme de Petersson d'une forme modulaire. À la fin du chapitre, nous allons définir la trace de la fonction L carrée symétrique. Cette trace est un nombre algébrique qui dépendra seulement du poids d'un espace de formes cuspidales. L'étude de la p-valuation de cette trace pour un poids fixe révèlera un lien avec le nombre de classes d'un corps quadratique.

1.1 Rappels sur les formes modulaires classiques

Dans cette section, nous faisons quelques rappels sur la théorie des formes modulaires classiques dans le but de fixer les définitions et la notation. Les démonstrations peuvent être trouvées dans plusieurs ouvrages de cette théorie par exemple dans [DS05], [Miy89] ou bien [Ser77]. Tout au long de cette section, $N \geq 1$ et k sont des entiers fixés.

Groupe modulaire, formes modulaires et caractères de Dirichlet

Soit $\mathrm{SL}_2(\mathbb{Z})$ l'ensemble des matrices carrées de dimension 2 à coefficients dans $\mathbb{Z}$ et de déterminant 1. On dénote par $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$ le *groupe modulaire* muni de son action par transformation de Mœbius sur le demi-plan supérieur $\mathbb{H} := \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$:

$$\gamma \cdot \tau := \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathbb{H}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Un sous-groupe $\Gamma \leqslant \Gamma(1)$ est dit de *congruence de niveau* N si N est le plus petit entier tel que Γ contient le groupe

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Par exemple, les sous-groupes suivants

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

et

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

sont des sous-groupes de congruences.

Le groupe des matrices carrées de dimension 2 à coefficients dans $\mathbb{R}$ et de déterminant positif, dénoté $\mathrm{GL}_2^+(\mathbb{R})$, agit sur l'ensemble des fonctions holomorphes $f : \mathbb{H} \to \mathbb{C}$ par le biais de l'opérateur de poids k :

$$f[\gamma]_k(\tau) := (\det(\gamma))^{k/2}(c\tau + d)^{-k} f(\gamma \cdot \tau).$$

où $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$. Si une fonction holomorphe f est invariante sous l'opérateur de poids k, c'est-à-dire que $f[\gamma]_k = f$ pour toute matrice γ dans un sous-groupe de congruence Γ, alors on dit que f est une *fonction modulaire de poids k*. Puisque la matrice $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ se trouve dans Γ, nous avons que f est N-périodique : $f(\tau + N) = f(\tau)$. Donc, f admet une série de Fourier

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n(f) q^n, \qquad q := e^{\frac{2\pi i \tau}{N}}.$$

Nous appellerons une telle expression la q-expansion d'une fonction modulaire. Si $a_n(f) = 0$ pour tout $n < 0$, nous disons que f est holomorphe à l'infinie.

Définition 1.1.1. Soit Γ un sous-groupe de congruence de niveau $N \geq 1$. Une fonction holomorphe $f : \mathbb{H} \to \mathbb{C}$ est appelée une *forme modulaire de poids k pour* Γ si pour toute matrice $\gamma \in \Gamma$ nous avons que

1. f est invariante sous l'opérateur de poids k ;
2. $f[\gamma]_k$ est holomorphe à l'infinie.

L'espace des formes modulaires de poids k pour Γ est noté $\mathcal{M}_k(\Gamma)$. Si le terme constant dans la q-expansion de $f|_k\gamma$ est nul pour toute matrice $\gamma \in \Gamma$, alors f est appelée une *forme cuspidale*. L'espace des formes cuspidales est noté $\mathcal{S}_k(\Gamma)$. Une forme modulaire est dite *normalisée* si son premier coefficient non nul est égal à 1.

Par la définition d'une forme modulaire, on voit que $\mathcal{M}_k(\Gamma)$ est un $\mathbb{C}$-espace vectoriel. En fait, il s'agit d'un espace de dimension fini. Il est également possible d'obtenir des formules qui dépendent de k pour calculer la dimension de $\mathcal{M}_k(\Gamma)$, ceci est fait dans [DS05, Chapitre 3].

Rappelons qu'un caractère de Dirichlet modulo N est un homomorphisme de groupe

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

Le plus petit $N' \mid N$ tel que χ est un caractère modulo N' est appelé le conducteur de χ, que nous noterons N_χ. On dit que χ est *primitif* s'il est un caractère modulo N_χ. De plus, notons qu'il est possible d'étendre le domaine de χ à $\mathbb{Z}$ en définissant

$$\chi(u) := \begin{cases} \chi(u \bmod N) & \text{si } (u, N) = 1; \\ 0 & \text{si } (u, N) = 0, \end{cases}$$

pour $u \in \mathbb{Z}$.

Si $\Gamma = \Gamma_1(N)$, alors il est possible de décomposer l'espace $\mathcal{M}_k(\Gamma_1(N))$ comme une somme directe

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(\Gamma_0(N), \chi),$$

où la somme est prise sur l'ensemble des caractères de Dirichlet modulo N et

$$\mathcal{M}_k(\Gamma_0(N), \chi) := \left\{ f \in \mathcal{M}_k(\Gamma_1(N)) : f[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]_k = \chi(d) f \quad \forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \right\}.$$

Dans la littérature, cet espace est parfois dénoté par $\mathcal{M}_k(N, \chi)$.

Un caractère de Dirichlet est dit *quadratique* si $\mathrm{Im}(\chi) = \{\pm 1\}$. Un exemple de caractère de Dirichlet quadratique qui nous sera utile est le symbole de Kronecker.

Définition 1.1.2. Soit $D \neq 1$ un entier qui est le discriminant d'un corps quadratique. On définit le *symbole de Kronecker* $(\frac{D}{\cdot})$ par les cinq propriétés suivantes.

1. $(\frac{D}{\cdot})$ est complètement multiplicatif, c'est-à-dire $(\frac{D}{ab}) = (\frac{D}{a})(\frac{D}{b})$, pour tout $a, b \in \mathbb{Z}$.
2. $(\frac{D}{0}) = 0$ et $(\frac{D}{1}) = 1$;
3. $(\frac{D}{p})$ est le symbole de Legendre pour tout premier impair p ;
4. $\left(\frac{D}{2}\right) = \begin{cases} 0, & \text{si } D \equiv 0 \pmod 2; \\ 1, & \text{si } D \equiv 1 \pmod 8; \\ -1, & \text{si } D \equiv 5 \pmod 8; \end{cases}$
5. $\left(\frac{D}{-1}\right) = \begin{cases} 1, & \text{si } D > 0; \\ -1, & \text{si } D < 0. \end{cases}$

Remarque 1.1.3. En fait, il existe une bijection entre l'ensemble des corps quadratiques et l'ensemble des caractères de Dirichlet quadratiques. Si K est un corps quadratique de discriminant D, alors on peut lui associer le symbole de Kronecker χ_D. Inversement, si χ est un caractère quadratique, alors il existe un entier D qui est le discriminant d'un corps quadratique tel que $\chi = (\frac{D}{\cdot})$.

Proposition 1.1.4 (Proposition 3.64 de [Shi94]). *Soit $N \geq 1$. Soit χ et ψ des caractères de Dirichlet primitifs modulo d_1 et d_2 respectivement où d_2 est un diviseur positif de N. Soit $f = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k(\Gamma_0(N), \psi)$, alors la forme*

$$f \otimes \chi := \sum_{n=1}^{\infty} \chi(n) a_n q^n$$

appartient à l'espace $\mathcal{S}_k(\Gamma_0(N'), \psi\chi^2)$ où $N' = \mathrm{ppcm}(N, d_1^2, d_1 d_2)$.

Exemple 1.1.5. Soit ψ un caractère de Dirichlet primitif modulo N et $f \in \mathcal{S}_k(\Gamma_0(N), \psi)$. Si χ est un caractère quadratique modulo N, alors $f \otimes \chi \in \mathcal{S}_k(\Gamma_0(N), \psi)$.

Opérateur de Hecke et produit de Petersson

Considérons maintenant le cas où $\Gamma = \Gamma_1(N)$. Pour chaque $n \geq 1$, il existe des opérateurs linéaires définis sur l'espace $\mathcal{M}_k(\Gamma_1(N))$:

$$\langle n \rangle, T_n : \mathcal{M}_k(\Gamma_1(N)) \longrightarrow \mathcal{M}_k(\Gamma_1(N)).$$

Les opérateurs $\langle n \rangle$ et T_n sont respectivement appelés les *opérateurs diamants* et les *opérateurs de Hecke*. On peut montrer que ces derniers préservent le sous-espace des formes cuspidales. De plus, leur polynômes caractéristiques sont définies sur $\mathbb{Q}$. Le lecteur est référé à [DS05, Chap. 5] pour la définition de ses opérateurs.

Considérons maintenant l'espace $\mathcal{S}_k(\Gamma_1(N))$. Nous munirons cet espace du produit scalaire de Petersson.

Définition 1.1.6. Le *produit scalaire de Petersson* est l'application $\mathbb{C}$-bilinéaire $\langle \cdot, \cdot \rangle : \mathcal{S}_k(\Gamma_1(N)) \times \mathcal{S}_k(\Gamma_1(N)) \to \mathbb{C}$ définie par

$$\langle f, g \rangle := \int_{\Gamma_1(N)\backslash\mathbb{H}} f(x+iy)\overline{g(x+iy)} y^{k-2} dx dy.$$

On notera la norme induite par le produit de Petersson par $\| \cdot \|$. On peut montrer que les opérateurs T_n et $\langle n \rangle$ commutent entre eux et sont normaux par rapport au produit de Petersson [DS05, Propositions 5.2.4 et 5.5.3]. Donc, par le théorème spectral, il existe une base orthogonale de formes modulaires dont chaque forme est simultanément une fonction propre pour chaque opérateur T_n. Une telle fonction sera appelée une *forme propre*. La base devient unique si chaque forme propre de la base est normalisée. Un intérêt pour les formes propres normalisées dans ce mémoire vient de ce théorème :

Théorème 1.1.7. *Si f est une forme propre normalisée dans $\mathcal{M}_k(\Gamma_1(N))$ ayant pour q-expansion $f = \sum_n a_n q^n$, alors ses coefficients sont des entiers algébriques. De plus, le corps $\mathbb{Q}(\{a_n : n \geq 0\})$ est une extension finie de $\mathbb{Q}$.*

Une démonstration de ce théorème est donnée dans les notes de Milne [Mil12, Proposition 5.27].

Définition 1.1.8. Soit $N \geq 1$, $k \in \mathbb{Z}$ et $f \in \mathcal{M}_k(\Gamma(N))$ une forme propre normalisée ayant pour q-expansion $f = \sum_{n\geq 0}^{\infty} a_n q^n$. Le *corps des coefficients* de f est le corps $\mathbb{Q}_f := \mathbb{Q}(\{a_n : n \geq 0\})$.

Fonction L associée à une forme modulaire

Soit $f \in \mathcal{S}_k(\Gamma_1(N))$ ayant la q-expansion suivante

$$f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n, \quad a_n(f) \in \mathbb{C}.$$

Alors, on peut considérer formellement la série L suivante

$$L(f, s) := \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}.$$

Cette série converge absolument pour tout $s \in \mathbb{C}$ ayant une partie réelle strictement plus grande que $k/2 + 1$ [DS05, Proposition 5.9.1].

Théorème 1.1.9. *Soit $f \in \mathcal{S}_k(\Gamma_1(N))$. Alors, f est une forme propre normalisée si et seulement si la fonction L associée à f admet un produit eulérien :*

$$L(f, s) = \prod_{p \text{ premier}} \frac{1}{1 - a_p(f)p^{-s} + p^{k-1-2s}}.$$

pour $\Re(s) > k/2 + 1$.

Démonstration. Voir théorème 5.9.2 de [DS05]. □

Il est possible d'étendre analytiquement la fonction L associée à une forme modulaire sur tout le plan complexe. Pour $\Re(s) > k/2 + 1$, on pose

$$\Gamma(s) := \int_0^{\infty} x^{s-1} e^{-x} dx.$$

Ainsi, on définit la fonction $L(f, s)$ *complétée* par

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

L'utilité de cette dernière fonction est qu'elle satisfait une équation fonctionnelle :

Théorème 1.1.10. *La fonction $L^*(f, s)$ satisfait l'équation fonctionnelle suivante*

$$L^*(f, s) = \pm L^*(f, k - s).$$

En conséquence, la fonction L associée à f possède un prolongement analytique sur tout le plan $\mathbb{C}$.

Démonstration. Une démonstration de ce théorème est donnée dans [DS05, Theorem 5.10.2]. □

Remarquons que si α_p et β_p sont les racines du polynôme $X^2 - a_p(f)X + p^{k-1}$, alors on peut réécrire ce produit eulérien de cette manière :

$$L(f,s) = \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}.$$

Les nombres α_p et β_p sont appelés les *paramètres de Satake de* f. Par leur définition, ils satisfont les deux relations suivantes :

$$\alpha_p + \beta_p = a_p(f), \quad \alpha_p\beta_p = p^{k-1}.$$

1.2 Définition et propriétés de la fonction L carré-symétrique

Soit f une forme cuspidale propre normalisée de niveau N et de poids k. Considérons les paramètres de Satake α_p et β_p de f. Alors, la fonction L *carrée symétrique associée à* f est définie par

$$L(\mathrm{Sym}^2(f), s) := \prod_p \frac{1}{(1-\alpha_p^2 p^{-s})(1-\alpha_p\beta_p p^{-s})(1-\beta_p^2 p^{-s})}$$

pour $s \in \mathbb{C}$ avec $\Re(s) > k$. Cette fonction L satisfait la relation :

$$\zeta_N(2s+2-2k)\sum_{n=1}^{\infty}\frac{a_n(f)^2}{n^s} = \zeta_N(s+1-k)L(\mathrm{Sym}^2(f),s), \tag{1.1}$$

où ζ_N est la fonction ζ de Riemann à laquelle on enlève les facteurs où $p \mid N$ de son produit eulérien [Zag77, §1]. Cette relation peut se démontrer en comparant les facteurs d'Euler de chaque côté de l'égalité. Donc, l'équation (1.1) donne une méthode pour calculer numériquement des approximations des valeurs prises par la fonction L carrée symétrique.

Il est possible de compléter la fonction L carrée symétrique en utilisant la fonction Γ qui a été définie à la section précédente. Ainsi, en posant $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2)$ et $\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s}\Gamma(s)$, on définit la fonction L carrée symétrique complétée par

$$L^*(\mathrm{Sym}^2(f), s) := \Gamma_{\mathbb{R}}(s-k+2)\Gamma_{\mathbb{C}}(s)L(\mathrm{Sym}^2(f),s). \tag{1.2}$$

Cette fonction satisfait l'équation fonctionnelle suivante

$$L^*(\mathrm{Sym}^2(f), s, 2k-1-s) = L^*(\mathrm{Sym}^2(f), s). \tag{1.3}$$

Un théorème qui est démontré dans un article de Zagier [Zag77, Corollaire page 115] nous dit que pour certaines valeurs entières de s, l'image de la fonction L carrée symétrique possède une certaine forme déterminée. Voici son énoncé :

Théorème 1.2.1. *Soit f une forme cuspidale propre normalisée de niveau N et poids k. Alors, pour $s \in \{k, k+2, k+4, \ldots, 2k-2\}$, la valeur de $L(\mathrm{Sym}^2(f), s)$ est un multiple algébrique de $\pi^{2s-k+1} \times \|f\|^2$.*

Autrement dit, pour chacune de ces valeurs de s, nous avons que

$$L(\mathrm{Sym}^2(f), s) = (\text{facteur algébrique}) \times \pi^{2s-k+1} \times \|f\|^2.$$

Le facteur algébrique est connu dans le cas précis où $s = k$:

$$L(\mathrm{Sym}^2(f), k) = \left(\frac{4^k}{2N(k-1)!}\right) \times \pi^{k+1} \times \|f\|^2.$$

Cette dernière équation permet de calculer de la norme de Petersson. Il s'agit d'une méthode plus simple que celle basée sur la définition 1.1.6 pour calculer une approximation numérique de cette norme. Davantage de détails sur cette méthode sont donnés dans [Coh13].

En vertu du théorème 1.2.1, nous dénotons, pour $s \in \{k, k+2, k+4, \ldots, 2k-2\}$, la partie algébrique de la fonction $L^*(\mathrm{Sym}^2(f), s)$ par

$$L^*(\mathrm{Sym}^2(f), s)_{\mathrm{alg}} := \frac{L^*(\mathrm{Sym}^2(f), s)}{\pi^{s/2-k/2}\|f\|^2}.$$

Par exemple, pour $s = k$ et $N = 1$, nous avons que

$$L^*(\mathrm{Sym}^2(f), k)_{\mathrm{alg}} = 2^k k. \tag{1.4}$$

Terminons cette section en expliquant brièvement la notation $\mathrm{Sym}^2(f)$. Au chapitre 4, nous énoncerons un théorème de Deligne qui affirme qu'il est possible de définir une représentation de dimension deux du groupe des automorphismes de $\overline{\mathbb{Q}}$ qui fixent $\mathbb{Q}$, dénoté $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, à partir d'une forme cuspidale propre normalisée [Del71]. Ainsi, la notation $\mathrm{Sym}^2(f)$ désigne la représentation carrée symétrique de la représentation associée à une forme propre f. De ce fait, la fonction L carrée symétrique est la fonction L qui est associée à la représentation $\mathrm{Sym}^2(f)$. Plus généralement, il est possible de définir une fonction L associée à une représentation quelconque du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. La définition complète de cette fonction L est donnée dans [Del79, (1.2.2)]. Nous verrons davantage de détails sur les représentations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ à la section 4.1 du chapitre 4.

1.3 Définition de la trace et lien avec le nombre de classes

Dans cette section, nous allons définir un objet d'intérêt principal pour ce mémoire soit la trace de la fonction L carrée symétrique. Un intérêt pour cet objet vient du fait que la trace possède un lien avec le nombre de classes d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$ où p est un premier congru à 3 modulo 4. Rappelons que le nombre de classes d'un corps de

nombres K est défini comme l'ordre du quotient du groupe des idéaux fractionnaires de K par le groupe des idéaux fractionnaires principaux. Autrement dit, si on dénote l'ensemble des idéaux fractionnaires par

$$\mathcal{I}_K := \{\alpha_1\mathcal{O}_K + \alpha_2\mathcal{O}_K + \cdots + \alpha_m\mathcal{O}_K : m \geq 1,\ \alpha_i \in K \text{ et } \exists i, \alpha_i \neq 0\}$$

et l'ensemble des idéaux fractionnaires principaux par

$$\mathcal{P}_K := \{\alpha\mathcal{O}_K : \alpha \in K \setminus \{0\}\}$$

alors le nombre de classes de K est défini par

$$h(K) := |\mathcal{I}_K/\mathcal{P}_K|.$$

Il est à noter que $h(K) < \infty$. Ce fait non trivial découle de la théorie de Minkowski sur la géométrie des nombres [Neu99, Chap. I, Theorem 6.3]. Si $K = \mathbb{Q}(\sqrt{D})$ est un corps quadratique de discriminant D, autrement dit $D \equiv 1 \pmod 4$, alors nous allons noter le nombre de classes de K par $h(D)$.

Définition 1.3.1. Soit k un entier pair et soit $\mathcal{B}_k$ la base de formes propres normalisées pour $\mathcal{S}_k(\Gamma(1))$. La *trace de la fonction L carrée symétrique* associée à l'espace $\mathcal{S}_k(\Gamma(1))$ est définie par

$$\mathrm{Tr}_k(L(\mathrm{Sym}^2, s)) := \sum_{f\in\mathcal{B}_k} L^*(\mathrm{Sym}^2(f), s)_{\mathrm{alg}},$$

pour $s \in \{k, k+2, k+4, \ldots, 2k-2\}$.

Remarque 1.3.2. La trace est une quantité bien définie, étant donné que la base de formes propres normalisées de poids k et niveau 1 est unique. De plus, à partir du moment où la valeur de s est fixée, on peut voir la trace comme un objet qui dépend uniquement du poids de l'espace des formes cuspidales. Par exemple, si $s = k$, alors on déduit de l'équation (1.4) que

$$\mathrm{Tr}_k(L(\mathrm{Sym}^2, k)) = \sum_{f\in\mathcal{B}_k} 2^k k = 2^k k \dim \mathcal{S}_k.$$

La trace est un nombre algébrique par définition. Par conséquent, il est possible d'étudier des questions portant sur la valuation p-adique de celle-ci. Soit $p \equiv 3 \pmod 4$ un premier et $k := (p+1)/2$, le poids de l'espace des formes cuspidales $\mathcal{S}_k(\Gamma(1))$. Notons que si $p < 23$, alors $(p+1)/2 < 12$ et donc $\mathcal{S}_k(\Gamma(1)) = 0$. Cette dernière implication découle du fait que nous avons l'égalité $\dim_{\mathbb{C}} \mathcal{S}_k(\Gamma(1)) = 0$ pour $0 \leq k \leq 11$ [DS05, Theorem 3.5.2]. De plus, remarquons que le premier p est choisi de sorte que $-p$ soit le discriminant du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$. Dans leur article [DH10], Dummigan et Heim s'intéressent à une équivalence entre la p-valuation de $\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))$ et le nombre de classes de $\mathbb{Q}(\sqrt{-p})$. Leur résultat s'énonce comme suit :

Théorème 1.3.3 (Théorèmes 1 et 2 de [DH10]). *Soit $p \geq 23$ un premier congru à 3 modulo 4 et $k := (p+1)/2$, alors*

1. $v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) = -1$ *si et seulement si* $h(-p) > 1$;
2. *Si* $h(-p) = 1$, *alors* $v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) = 0$,

où v_p est la valuation p-adique.

Ce théorème, qui sera démontré au chapitre 3, provient d'un calcul explicite de la trace. En effet, Dummigan et Heim ont obtenu une formule de la trace qui s'exprime en fonction des *nombres de Bernoulli*, une suite de nombres possédant plusieurs propriétés arithmétiques intéressantes. Une étude approfondie de ces nombres démontre qu'ils sont en lien avec le nombre de classes de $\mathbb{Q}(\sqrt{-p})$.

Le théorème 1.3.3 se concentre seulement en une seule valeur de k, soit celle de $k = (p+1)/2$. Ainsi, un objectif de ce mémoire est de répondre à la question : peut-on obtenir un résultat similaire si l'on fait varier le poids k ? À la section 3.3 du chapitre 3, nous verrons qu'il existe une réponse affirmative à cette question. Pour ce faire, nous aurons besoin d'étudier la théorie des formes modulaire de Siegel afin de démontrer la formule de la trace.

Chapitre 2

Formes modulaires de Siegel

À la section 1.1, nous avons repassé rapidement sur la notion de formes modulaires dites *elliptiques*. En étudiant les formes quadratiques, le mathématicien Carl Ludwig Siegel a développé une généralisation de cette théorie pour des fonctions à plusieurs variables. Ainsi, les formes modulaires de Siegel peuvent être vues comme des formes modulaires à plusieurs variables. Pour des références sur le sujet des formes modulaires de Siegel, on réfère le lecteur au chapitre 1 du livre d'Andrianov [And09], au livre de Klingen [Kli90] ou bien aux notes de van der Geer [vdG08].

2.1 Le groupe modulaire et le demi-espace de degré n

Définition 2.1.1. Soit $n \geq 1$. Le *groupe modulaire de degré* n que l'on note $\Gamma^n(1)$ est formé de matrices de dimension $2n \times 2n$ à coefficients dans $\mathbb{Z}$ de la forme

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

où A, B, C et D sont des matrices de dimension $n \times n$ satisfaisant les trois relations suivantes :

1. $AB^t = BA^t$;
2. $CD^t = DC^t$;
3. $AD^t - BC^t = I_n$.

Soit $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^n(1)$ une telle matrice. Ainsi, par les propriétés 1, 2 et 3 nous avons que

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix} = \begin{pmatrix} AD^t - BC^t & BA^t - AB^t \\ CD^t - DC^t & DA^t - CB^t \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix}.$$

Donc, M est une matrice inversible et nous connaissons son inverse. Nous récapitulons ce calcul dans la proposition suivante :

Proposition 2.1.2. *Soit* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ *une matrice de dimension* $2n \times 2n$ *à coefficients entiers. Alors,* $M \in \Gamma^n(1)$ *si et seulement si* M *est inversible et*

$$M^{-1} = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix}$$

Remarque 2.1.3. Au lieu de multiplier M^{-1} à la droite de M, nous aurions pu la multiplier à la gauche de M et obtenir de nouvelles relations :

$$\begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} D^tA - B^tC & D^tB - B^tD \\ A^tC - C^tA & A^tD - C^tB \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix}.$$

Par conséquent, $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^n(1)$ si et seulement si ses coefficients sont entiers et qu'elle respecte les relations suivantes :

1. $C^tA = A^tC$;
2. $D^tB = B^tD$;
3. $D^tA - B^tC = I_n$.

On remarque immédiatement que le groupe modulaire de degré 1 est le même que le groupe modulaire classique défini à la section 1.1. Il s'agit donc bien d'une généralisation. Certains auteurs notent le groupe modulaire de degré n par $\mathrm{Sp}_{2n}(\mathbb{Z})$, car il s'agit en fait d'un groupe de matrices dites *symplectiques*.

Il existe également une généralisation du demi plan supérieur $\mathbb{H}$. Pour définir cette généralisation, nous avons besoin d'introduire la notion de matrice définie positive. Si $v \in \mathbb{C}^n$ est un vecteur, alors nous noterons par $\overline{v}$ le vecteur conjugué.

Définition 2.1.4. Soit Y une matrice de dimension $n \times n$. Alors Y est dite *semi-définie positive* si $\overline{v}^t Y v \geq 0$ pour tout vecteur $v \in \mathbb{C}^n$ et on note cette propriété par $Y \geq 0$. Si $\overline{v}^t Y v > 0$ pour tout vecteur $v \in \mathbb{C}^n \setminus \{0\}$, alors on dit que Y est *définie positive*. On note cette propriété par $Y > 0$.

Définition 2.1.5. Soit $n \geq 1$ un entier. Le *demi-espace supérieur de degré* n est défini par

$$\mathbb{H}_n := \{Z = X + iY : X, Y \in \mathrm{M}_n(\mathbb{R}), Z^t = Z \text{ et } Y > 0\}.$$

Notons que $\mathbb{H}_n \subset \mathrm{M}_n(\mathbb{C})$.

Soit $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^n(1)$ et $Z = X + iY \in \mathbb{H}_n$. Pour avoir une action de $\Gamma^n(1)$ sur $\mathbb{H}_n$ généralisant le cas $n = 1$, il est naturel de poser

$$M \cdot Z := (AZ + B)(CZ + D)^{-1}. \tag{2.1}$$

Cependant, il faut faire attention : nous devons vérifier que la matrice $CZ + D$ est bien inversible pour que l'action soit bien définie. Pour cela nous allons utiliser le lemme suivant :

Lemme 2.1.6. *Soit* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^n(1)$ *et* $Z = X + iY \in \mathbb{H}_n$, *alors*

1) $(C\overline{Z} + D)^t(AZ + B) - (A\overline{Z} + B)^t(CZ + D) = 2iY$;

2) $(CZ + D)^t(AZ + B) - (AZ + B)^t(CZ + D) = 0$.

Démonstration. Ce lemme découle d'un calcul direct en utilisant les relations de la définition 2.1.1 en plus des relations obtenues à la remarque 2.1.3. □

Pour montrer que la matrice $CZ + D$ est inversible, nous allons prouver que le système linéaire homogène $(CZ + D)v = 0$ possède l'unique solution $v = 0$. Soit v une telle solution. Alors, par l'équation 1 du lemme 2.1.6, nous avons que

$$\overline{v}^t Y v = \frac{1}{2i}\Big(\underbrace{\overline{v}^t(C\overline{Z} + D)^t}_{=0}(AZ + B)v - \overline{v}^t(A\overline{Z} + B)^t \underbrace{(CZ + D)v}_{=0} \Big) = 0$$

Par définition du demi-espace supérieur, nous avons que $Y > 0$ et donc $v = 0$. Par conséquent, l'application (2.1) est bien définie.

Vérifions maintenant qu'il s'agit bien d'une action de groupe. Nous devons vérifier que pour toutes paires de matrices M et M' dans $\Gamma^n(1)$ ainsi que pour toutes matrices Z dans $\mathbb{H}_n$ nous avons les deux conditions suivantes :

1. $M \cdot Z \in \mathbb{H}_n$;
2. $(MM') \cdot Z = M \cdot (M' \cdot Z)$.

Démontrons que $M \cdot Z \in \mathbb{H}_n$. Par l'équation 2 du lemme 2.1.6 on a que

$$(CZ + D)^t(M \cdot Z - (M \cdot Z)^t)(CZ + D) = (CZ + D)^t(AZ + B) - (AZ + B)^t(CZ + D) = 0.$$

Donc, $M \cdot Z - (M \cdot Z)^t = 0$ et $M \cdot Z$ est une matrice symétrique. Si $M \cdot Z = X' + iY'$, alors il reste à montrer que Y' est définie positive. Ceci découle du fait que

$$(C\overline{Z} + D)^t Y'(CZ + D) = Y.$$

Cette dernière égalité s'obtient par le lemme 2.1.6. On conclut donc que $M \cdot Z \in \mathbb{H}_n$.
Pour ce qui est de la condition 2, elle s'obtient par un calcul direct.

Domaine fondamental pour l'action de $\Gamma^n(1)$ sur $\mathbb{H}_n$

Il est possible de construire un domaine fondamental pour l'action de $\Gamma^n(1)$ sur $\mathbb{H}_n$. Pour cela, il faut définir la notion de matrice réduite au sens de Minkowski. Soit $Y = (y_{ij})$ une matrice de dimension $n \times n$ avec $y_{ij} \in \mathbb{R}$. Alors, Y est dite *réduite au sens de Minkowski* si

1. $v^t Y v \geq y_{ii}$ pour $1 \leq i \leq n$;
2. $y_{i,i+1} \geq 0$ pour $0 \leq i \leq n - 1$;

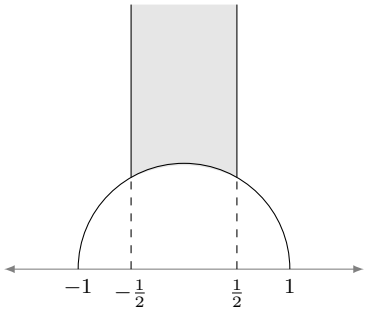
pour tout vecteur $v \in \mathbb{Z}^n$ ayant des coordonnées copremières.

Théorème 2.1.7. *Soit $n \geq 1$ un entier. Un domaine fondamental pour l'action de $\Gamma^n(1)$ sur $\mathbb{H}_n$ est donné par l'ensemble des matrices $Z = X + iY$ dans $\mathbb{H}_n$ telles que*

1. *Pour toutes matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ dans $\Gamma^n(1)$, on a que $|\det(CZ + D)| \geq 1$;*
2. *Y est réduite au sens de Minkowski.*
3. *Si $X = (x_{ij})$, alors $|x_{ij}| \leq 1/2$ pour tout indice i et j.*

Une démonstration de ce théorème peut être trouvée dans [And09, Theorem 1.16]. En guise d'exemple avec $n = 1$, le domaine fondamental de l'action de $\Gamma^1(1)$ sur $\mathbb{H}_1$ est donné par la région grise de la figure suivante :

FIGURE 2.1: Domaine fondamental de l'action de $\Gamma^1(1)$ sur $\mathbb{H}_1$



2.2 Définition d'une forme modulaire de Siegel

Nous donnons ici la définition d'une forme modulaire de Siegel. Soit $n \geq 1$ et $k \geq 1$ des entiers. Tout comme dans le cas classique, on définit l'opérateur de poids k d'une fonction $f : \mathbb{H}_n \to \mathbb{C}$ par

$$f[M]_k(Z) := \det(CZ + D)^{-k} f(M \cdot Z),$$

où $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ est dans $\Gamma^n(1)$ et Z est dans le demi-espace de Siegel.

Définition 2.2.1. Une *forme modulaire de Siegel de degré n et de poids k pour* $\Gamma^n(1)$ est une fonction holomorphe $f : \mathbb{H}_n \to \mathbb{C}$ telle que

$$f(M \cdot Z) = \det(CZ + D)^k f(Z),$$

pour toute matrice $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^n(1)$. De plus, si $n = 1$, on exige la condition d'être holomorphe à l'infinie. L'espace des formes modulaires de Siegel de degré n et de poids k pour $\Gamma^n(1)$ est noté $\mathcal{M}_k(\Gamma^n(1))$. Nous noterons par $\mathcal{M}^n$ l'algèbre graduée de toutes les formes modulaires de degré n :

$$\mathcal{M}^n := \bigoplus_{k=1}^{\infty} \mathcal{M}_k(\Gamma^n(1)).$$

Si $n = 1$, alors nous avons l'espace de toutes les formes modulaires classiques qui ont été définies à la section 1.1.

Remarque 2.2.2. Il aurait été possible de donner une définition plus générale. En effet, nous aurions pu considérer une fonction holomorphe $f : \mathbb{H}_n \to V$ où V est un $\mathbb{C}$-espace vectoriel de dimension fini. Ainsi, pour généraliser le facteur d'automorphie $\det(CZ + D)^k$, il faut considérer un homomorphisme continu $\rho : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}(V)$ et exiger que f satisfasse la condition suivante

$$f(M \cdot Z) = \rho(CZ + D)f(Z)$$

pour chaque matrice $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^n(1)$ et $Z \in \mathbb{H}_n$. Dans le cadre de la définition 2.2.1, nous avons que $V = \mathbb{C}$ et $\rho = (\det(\cdot))^k$. Cependant, nous n'aurons pas besoin d'un tel niveau de généralité. Cela a été précisé à titre informatif seulement.

À la définition 2.2.1, la fonction f peut être vue comme une fonction complexe à $n(n+1)/2$ variables. Donc, si f est holomorphe sur $\mathbb{H}_n$, cela revient à dire que f peut s'écrire comme une série entière à plusieurs variables autour de chaque point de $\mathbb{H}_n$. La condition sur l'holomorphie à l'infinie peut sembler un peu étrange, étant donné qu'elle s'applique seulement au cas $n = 1$. Cependant, il aurait été superflu de l'exiger pour $n > 1$, puisque cette condition sera toujours vérifiée dans ce cas. Ce fait correspond au théorème 1 de [vdG08].

2.3 Développement de Fourier et opérateur de Siegel

Nous allons étudier dans cette section le développement de Fourier d'une forme modulaire de Siegel. Cela nous permettra de définir un opérateur linéaire sur l'espace des formes modulaires de Siegel. Nous verrons qu'une propriété de cet opérateur est qu'il applique une forme de degré n vers une forme de degré $n - 1$. Ceci nous sera utile plus tard pour obtenir de l'information sur les coefficients de la q-expansion d'une forme modulaire de degré 2.

Définition 2.3.1. Une matrice symétrique A à coefficients rationnels et de dimension $n \times n$ est appelée *semi-entière* si A est sous la forme :

$$N = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \frac{a_{1n}}{2} \\ \frac{a_{12}}{2} & a_{22} & \cdots & \frac{a_{2n}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}}{2} & \frac{a_{2n}}{2} & \cdots & a_{nn} \end{pmatrix}$$

où les éléments a_{ij} sont des entiers.

Théorème 2.3.2 (Théoreme 1.23 de [And09])**.** *Soit $f \in \mathcal{M}_k(\Gamma^n(1))$. Alors, f possède un développement de la forme*

$$f(Z) = \sum_{\substack{N \text{ semi-entière} \\ N \geq 0}} c(N) e^{2\pi i \mathrm{Tr}(NZ)}, \qquad c(N) \in \mathbb{C}.$$

Cette série converge absolument sur $\mathbb{H}$ et uniformément sur tout sous-ensemble compact de la forme :

$$\mathbb{H}_n^{\varepsilon} := \{Z = X + iY \in \mathbb{H}_n : Y - \varepsilon I_n \geq 0\}, \quad \varepsilon > 0.$$

De plus, les coefficients $c(N)$ satisfont la relation

$$c(A^t N A) = (\det(A))^k c(N),$$

pour toute matrice inversible $A \in \Gamma^n(1)$ de dimension $n \times n$.

Pour une matrice Z' de dimensions $(n-1) \times (n-1)$, $n \geq 2$, et un nombre réel $y \in \mathbb{R}$, nous allons dénoter par Z'_y la matrice de dimension $n \times n$ définie par

$$Z'_y := \begin{pmatrix} Z' & 0 \\ 0 & iy \end{pmatrix}.$$

Proposition 2.3.3. *Soit $n \geq 2$, $f \in \mathcal{M}_k(\Gamma^n(1))$ et $Z' \in \mathbb{H}_{n-1}$. Alors, la limite suivante*

$$\Phi(f)(Z') := \lim_{y \to \infty} f\left(Z'_y\right)$$

existe. De plus, la fonction $F : \mathbb{H}_{n-1} \to \mathbb{C}$ définie par $Z' \mapsto \Phi(f)(Z')$ est une forme modulaire de Siegel de poids k pour $\Gamma^{n-1}(1)$.

Démonstration. Soit $f \in \mathcal{M}_k(\Gamma^n(1))$ admettant la q-expansion suivante

$$f(Z) = \sum_{\substack{N \text{ semi-entière} \\ N \geq 0}} c(N) e^{2\pi i \mathrm{Tr}(NZ)}. \tag{2.2}$$

Puisque cette série converge uniformément sur tout sous-ensemble de la forme $\mathbb{H}_n^{\varepsilon}$, alors nous avons

$$\lim_{y \to \infty} f\left(Z'_y\right) = \sum_{\substack{N \text{ semi-entière} \\ N \geq 0}} c(N) \lim_{y \to \infty} e^{2\pi i \mathrm{Tr}(NZ'_y)},$$

où $Z' \in \mathbb{H}_{n-1}$. Pour calculer cette limite, écrivons $N = \left(\begin{smallmatrix} N' & * \\ * & x_{nn} \end{smallmatrix}\right)$ où N' est une matrice $(n-1) \times (n-1)$ et $x_{nn} \in \mathbb{Q}$. On trouve

$$\begin{aligned} \lim_{y \to \infty} e^{2\pi i \mathrm{Tr}(NZ'_y)} &= \lim_{y \to \infty} e^{-2\pi y x_{nn}} e^{2\pi i \mathrm{Tr}(N'Z')} \\ &= \begin{cases} e^{2\pi i \mathrm{Tr}(N'Z')} & \text{si } x_{nn} = 0; \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Donc, puisque N est semi-définie positive, on déduit que

$$\lim_{y \to \infty} f\left(Z'_y\right) = \sum_{\substack{N' \text{ semi-entière} \\ N' \geq 0}} c\left(\begin{pmatrix} N' & 0 \\ 0 & 0 \end{pmatrix}\right) e^{2\pi i \mathrm{Tr}(N'Z')}. \tag{2.3}$$

Cette dernière série est une série partielle du développement de Fourier (2.2). On en conclut que la limite converge comme il est souhaité.

Montrons maintenant que $Z' \to \Phi(f)(Z')$ est une forme modulaire de Siegel de poids k pour $\Gamma^{n-1}(1)$. Par l'équation (2.3), il reste seulement à démontrer que $\Phi(f)$ est $\Gamma^{n-1}(1)$-invariante. Soit $M' = \left(\begin{smallmatrix} A' & B' \\ C' & D' \end{smallmatrix}\right) \in \Gamma^{n-1}(1)$. Considérons la matrice

$$M := \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

où

$$A = \begin{pmatrix} A' & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} B' & 0 \\ 0 & 0 \end{pmatrix},$$
$$C = \begin{pmatrix} C' & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} D' & 0 \\ 0 & 1 \end{pmatrix}.$$

Notons que $M \in \Gamma^n(1)$. De plus, remarquons que $(M' \cdot Z')_y = M \cdot Z'_y$ et que $\det(CZ'_y + D) = \det(C'Z' + D')$. Alors, on observe que $\Phi(f)$ est invariante sous l'opérateur de poids k par le calcul suivant

$$\begin{aligned} \Phi(f)[M']_k(Z') &= \det(C'Z' + D')^{-k} \lim_{y\to\infty} f((M' \cdot Z')_y) \\ &= \det(CZ'_y + D)^{-k} \lim_{y\to\infty} f(M \cdot Z'_y) \\ &= \Phi(f[M]_k)(Z') \\ &= \Phi(f)(Z'). \end{aligned}$$

□

Remarques 2.3.4.

1. Dans le cas où $n = 1$, alors on définit $\Phi : \mathcal{M}_k(\Gamma(1)) \to \mathbb{C}$ par

$$\Phi(f) := \lim_{n\to\infty} f(iy).$$

   Cet opérateur est bien défini, car il s'agit du coefficient $a_0(f)$ dans la q-expansion de f.

2. La démonstration du théorème précédent montre que nous avons une injection

$$\begin{aligned} \Gamma^{n-1}(1) &\hookrightarrow \Gamma^n(1) \\ \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} &\longmapsto \begin{pmatrix} A' & 0 & B' & 0 \\ 0 & 1 & 0 & 0 \\ C' & 0 & D' & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Corollaire 2.3.5. *Soit $f \in \mathcal{M}_k(\Gamma^n(1))$, $n \geq 2$, ayant pour q-expansion*

$$f(Z) = \sum_{\substack{N \in \Gamma^n(1) \text{ semi-entière} \\ N \geq 0}} c(N) e^{2\pi i \mathrm{Tr}(NZ)}, \quad Z \in \mathbb{H}_n.$$

Alors, la q-expansion de la forme modulaire $\Phi(f)$ est donnée par

$$\Phi(f)(Z') = \sum_{\substack{N' \in \Gamma^{n-1} \text{ semi-entière} \\ N' \geq 0}} c\left(\begin{pmatrix} N' & 0 \\ 0 & 0 \end{pmatrix}\right) e^{2\pi i \mathrm{Tr}(N'Z')}, \quad Z' \in \mathbb{H}_{n-1}.$$

Définition 2.3.6. L'opérateur linéaire

$$\begin{aligned} \Phi : \mathcal{M}_k(\Gamma^n(1)) &\longrightarrow \mathcal{M}_k(\Gamma^{n-1}(1)) \\ f &\longmapsto \Phi(f) \end{aligned}$$

est appelé l'*opérateur de Siegel.*

La proposition 2.3.3 nous dit que

$$\Phi(\mathcal{M}_k^n(\Gamma(1))) \subset \mathcal{M}_k^{n-1}(\Gamma(1)).$$

Il est conjecturé qu'il s'agit d'un opérateur surjectif pour les valeurs paires de k. Ce fait a été démontré pour des valeurs paires de k telles que $k > 2n$ [vdG08, Corollary 3]. Cependant, il ne s'agit pas d'un opérateur injectif. Ceci nous permet donc de généraliser l'espace des formes cuspidales pour des degrés supérieurs. En effet, rappelons que, dans le cas où $n = 1$, on dit qu'une forme modulaire f est cuspidale si elle s'annule à l'infinie. Autrement dit, si la limite $\lim_{y\to\infty} f(iy)$ est égale à 0.

Définition 2.3.7. L'espace des *formes cuspidales de poids k pour* $\Gamma^n(1)$ est le noyau de $\Phi|_{\mathcal{M}_k^n(\Gamma(1))}$. Cet espace est dénoté par $\mathcal{S}_k(\Gamma^n(1))$.

2.4 Séries d'Eisenstein

Dans cette section, nous allons étudier un exemple important de forme modulaire, les séries d'Eisenstein. Nous porterons notre intérêt à ces dernières principalement pour les coefficients de leur q-expansions.

2.4.1 Les séries d'Eisenstein classiques et les nombres de Bernoulli

Pour un entier pair $k \geq 4$, on définit la *série d'Eisenstein normalisée de poids k* par :

$$E_k(\tau) := \frac{1}{2} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty^+ \backslash \Gamma(1)} \frac{1}{(cz+d)^k} = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \mathrm{pgcd}(c,d)=1}} \frac{1}{(c\tau+d)^k},$$

où

$$\Gamma_\infty^+ := \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}.$$

Cette série est absolument convergente pour tout $\tau \in \mathbb{H}$. De plus, il s'agit d'une forme modulaire de poids k pour $\Gamma(1)$ qui possède la q-expansion suivante :

$$E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

où B_k est le k-ième nombre de Bernoulli et $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$. Ce qui est intéressant avec les séries d'Eisenstein c'est que les nombres de Bernoulli sont présents dans leur q-expansion. Ces nombres respectent certaines propriétés arithmétiques fort utiles. En effet, grâce aux nombres de Bernoulli, nous serons capables de lier la trace de la fonction L carrée symétrique avec le nombre de classes d'un corps quadratique imaginaire. Rappelons que le *k-ième nombre de Bernoulli* est défini comme étant le nombre B_k de sorte que

$$\frac{te^t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Notons que B_k est un nombre rationnel et que $B_k = 0$ si $k \geq 3$ est impair.

Il existe une généralisation des nombres de Bernoulli pour les caractères de Dirichlet. Ainsi, on définit le *k-ième nombre de Bernoulli généralisé pour le caractère primitif* χ par le nombre $B_{k,\chi}$ tel que

$$\sum_{u=1}^{N_\chi} \frac{\chi(u) t e^{ut}}{e^{f_\chi t} - 1} = \sum_{k=0}^{\infty} B_{k,\chi} \frac{t^k}{k!}.$$

Les nombres de Bernoulli sont en lien avec les valeurs spéciales de la fonction ζ de Riemann. En effet, nous avons que

$$\zeta(1-k) = \frac{-B_k}{k}, \quad k \geq 2. \tag{2.4}$$

Ce résultat est classique et peut être trouvé dans plusieurs livres de référence, par exemple dans [Neu99, Chap. VII, Theorem 1.8].

Il existe une généralisation de l'égalité (2.4) pour les séries L de Dirichlet associée à un caractère de Dirichlet χ. Rappelons que la série L associées à χ, un caractère de Dirichlet primitif de conducteur N_χ, est définie par

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \Re(s) > 1.$$

Proposition 2.4.1. *Soit $k \geq 2$, alors $L(1-k, \chi) = \frac{-B_{k,\chi}}{k}$.*

Démonstration. Voir [Neu99, Chap VII, Theorem 2.9]. □

Ainsi, nous sommes maintenant prêts à énoncer la formule pour calculer la trace de la fonction L carrée symétrique.

Théorème 2.4.2. *Soit $k \geq 4$ un entier pair. Alors,*

$$\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2)) = c_k \left(B_{k-1,(\frac{-4}{\cdot})} + 2B_{k-1,(\frac{-3}{\cdot})} + B_{2k-2}\left(1 + \frac{k}{B_k}\right)\right).$$

où

$$c_k := 2^{2k-1}\frac{(\frac{k}{2}-1)!}{(k-1)!}.$$

Grâce à cette formule, le calcul de la trace est grandement simplifié. Son écriture en termes de nombres de Bernoulli nous permet de déduire des résultats de divisibilité sur la trace en lien avec le nombre de classes d'un corps quadratique imaginaire. Pour démontrer le théorème 2.4.2, nous avons besoin de définir les séries d'Eisenstein de degré supérieur. Nous verrons au prochain chapitre qu'elles sont reliées aux séries d'Eisenstein classiques par une formule.

2.4.2 Les séries d'Eisenstein de degré supérieur

Dans cette sous-section, nous étudierons un exemple important de forme modulaire de Siegel. Considérons le sous-groupe suivant de $\Gamma^n(1)$:

$$\Gamma_\infty^n := \left\{ \begin{pmatrix} I_n & N \\ 0 & I_n \end{pmatrix} : N^t = N \right\}.$$

Définition 2.4.3. Soit $n \geq 1$ et $k > n+1$ deux entiers avec k pair. On définit la *série d'Eisenstein de Siegel de degré n et de poids k* par

$$E_k^n(Z) := \sum_{M \in \Gamma_\infty^n \backslash \Gamma^n(1)} \frac{1}{\det(CZ+D)^k}, \quad M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right),\ Z \in \mathbb{H}_n.$$

On peut montrer que cette série est bien définie et qu'elle converge absolument et uniformément sur $\mathbb{H}_n$ [Kli90, p. 63]. Par sa définition, on constate qu'elle est invariante sous l'opérateur de poids k pour $\Gamma^n(1)$. Ainsi, E_k^n est une forme modulaire de Siegel de poids k et degré n. Notons que les séries d'Eisenstein de degré supérieur ne sont pas des formes cuspidales. Ceci s'explique par le prochain résultat :

Proposition 2.4.4. $\Phi(E_k^n) = E_k^{n-1}$.

Une démonstration de la dernière proposition est donnée dans la preuve de la proposition 8 de la section 5 du livre [Kli90]. Par exemple, si $n = 2$, alors $\Phi(E_k^2) = E_k$.

Par le théorème 2.3.2, la séries E_k^2 possède un développement de Fourier de la forme

$$E_k^2(Z) = \sum_{\substack{N \text{ semi-entière} \\ N \geq 0}} A_k^2(N) e^{2\pi i \mathrm{Tr}(NZ)}, \qquad A_k^2(N) \in \mathbb{C}. \tag{2.5}$$

Il existe une formule explicite pour les coefficients de cette série. Afin d'écrire cette formule, nous avons besoin d'introduire un peu de notation. Tout d'abord, les matrices semi-entières en indice dans le développement de Fourier (2.5) seront de la forme

$$N = \begin{pmatrix} a & r/2 \\ r/2 & b \end{pmatrix}.$$

Pour dénoter les matrices semi-entières N, nous utiliserons (a, r, b) comme notation. Ensuite, Cohen a introduit dans son article [Coh75] une fonction $H(r, D)$ où $r \geq 1$ et D sont des entiers positifs. Si $D \equiv 1 \pmod 4$, alors la fonction H de Cohen a comme propriété

$$H(k-1, D) = L(2-k, (\tfrac{-D}{\cdot})).$$

Nous aurons uniquement besoin de cette propriété pour ce qui suit. On réfère le lecteur à la définition 2.2 de l'article de Cohen pour la définition complète de la fonction H.

Proposition 2.4.5. *Les coefficients pour le développement de Fourier de la série d'Eisenstein E_k^2 sont donnés par*

$$A_k^2(a, r, b) := A_k^2(N) = \frac{2}{\zeta(1-k)\zeta(3-2k)} \sum_{d \mid \mathrm{pgcd}(a,r,b)} d^{k-1} H\left(k-1, \frac{4ab-r^2}{d^2}\right)$$

Cette formule a été initialement démontrée par Maass dans [Maa64] et [Maa72]. Une autre démonstration de cette formule est donnée par Zagier dans [Zag81].

Supposons que les entiers a, r et b satisfont

$$\mathrm{pgcd}(a, r, b) = 1 \quad \text{et} \quad D := 4ab - r^2 \equiv 1 \pmod 4.$$

Ainsi, on a que

$$A_k^2(a, r, b) = \frac{2L(2-k, \left(\frac{-D}{\cdot}\right))}{\zeta(1-k)\zeta(3-2k)}. \tag{2.6}$$

Donc, par les valeurs spéciales de la fonction L et de la fonction ζ aux entiers négatifs, on peut simplifier l'équation (2.6) :

$$A_k^2(a, r, b) = \frac{-4kB_{k-1,\left(\frac{-D}{\cdot}\right)}}{B_k B_{2k-2}}.$$

Chapitre 3

Calcul de la trace de $L(\mathrm{Sym}^2(\cdot), s)$

3.1 Formule de relèvement d'une Série d'Eisenstein de Siegel de degré 2

Commençons par introduire un concept appelé le relèvement d'une forme modulaire de Siegel. Soit $n \geq 2$ un entier que l'on décompose en une partition $\eta = (n_1, n_2, \ldots, n_r)$,

$$n = n_1 + n_2 + \cdots + n_r,\ n_i \in \mathbb{Z}_{\geq 1}.$$

Ainsi, nous avons une injection $\mathbb{H}_{n_1} \times \mathbb{H}_{n_2} \times \cdots \times \mathbb{H}_{n_r} \hookrightarrow \mathbb{H}_n$ donnée par le plongement diagonal

$$(N_1, N_2, \ldots, N_r) \longmapsto \begin{pmatrix} N_1 & 0 & \ldots & 0 \\ 0 & N_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & N_r \end{pmatrix},$$

où chaque bloc N_i est dans $\mathbb{H}_{n_i}$. Nous dénotons l'image de $\mathbb{H}_{n_1} \times \mathbb{H}_{n_2} \times \cdots \times \mathbb{H}_{n_r}$ sous cette injection par $\mathbb{H}_\eta$.

Définition 3.1.1. Soit $n \geq 2$, $f \in \mathcal{M}_k(\Gamma^n(1))$ et $\eta = (n_1, \ldots, n_r)$ une partition de n. Alors, le *relèvement de f pour la partition η* est la fonction $f|_{\mathbb{H}_\eta}$.

Cette notion nous amène à énoncer une formule initialement démontrée par Garrett dans [Gar84, Theorem §5] pour calculer le relèvement de la série d'Eisenstein de poids k et de degré 2 pour la partition $(1, 1)$.

Théorème 3.1.2. *Soit $k \geq 4$ un entier pair et $\mathcal{B}_k$ la base de formes cuspidales propres normalisées de poids k et de niveau 1. Alors, pour $z, w \in \mathbb{H}$, le relèvement de E_k^2 pour la partition $\eta = (1, 1)$ est égal à*

$$E_k^2|_{\mathbb{H}_\eta} = E_k(z)E_k(w) + \sum_{f \in \mathcal{B}_k} \mu_f f(z) f(w),$$

où

$$\mu_f = \frac{-2^{5-2k}k!}{(\frac{k}{2}-1)!} \times \frac{1}{B_k B_{2k-2}} \times L^*(\mathrm{Sym}^2(f), 2k-2)_{\mathrm{alg}}.$$

Ainsi, dans cette formule, nous voyons les séries d'Eisenstein classiques apparaître et le terme $L^*(\mathrm{Sym}^2(f), 2k-2)_{\mathrm{alg}}$. Ceci nous permettra d'obtenir la formule de la trace de la fonction L carrée symétrique.

3.2 Démonstration de la formule de la trace

Cette section se consacre à présenter avec plus de détails la démonstration de Dummigan et Heim du théorème 2.4.2. Rappelons que ce dernier stipule que, pour $k \geq 4$ pair, nous avons la formule

$$\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2)) = c_k\Big(B_{k-1,\chi_{-4}} + 2B_{k-1,\chi_{-3}} + B_{2k-2}(1 + \frac{k}{B_k})\Big), \tag{3.1}$$

où

$$c_k := 2^{2k-1}\frac{(\frac{k}{2}-1)!}{(k-1)!}.$$

L'idée de la démonstration est de comparer les coefficients de la q-expansion de chaque côté de l'égalité de la formule de relèvement de E_k^2 pour la partition $\eta = (1,1)$ donnée dans le théorème 3.1.2. D'une part, le côté gauche a pour q-expansion

$$E_k^2|_{\mathbb{H}_\eta} = \sum_{N=(a,r,b)\geq 0} A_k^2(N)e^{2\pi i(az+bw)}, \quad A_k^2(N) \in \mathbb{C}, \quad (a,r,b) = \begin{pmatrix} a & r/2 \\ r/2 & b \end{pmatrix}$$

et d'autre part, les premiers termes de la q-expansion du membre de droite sont

$$\begin{aligned} &E_k(z)E_k(w) + \sum_{f\in\mathcal{B}_k} \alpha_f f(z)f(w) \\ &\qquad = 1 - \frac{2k}{B_k}e^{2\pi iz} - \frac{2k}{B_k}e^{2\pi iw} + \left[\left(\frac{2k}{B_k}\right)^2 + \sum_{f\in\mathcal{B}_k}\mu_f\right]e^{2\pi i(z+w)} + \cdots \end{aligned}$$

Nous allons nous intéresser au coefficient devant le terme $e^{2\pi i(z+w)}$. Ainsi, les matrices symétriques semi-définies positives N pour lesquelles $\mathrm{Tr}(NZ) = z+w$ sont

$$(1,0,1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (1,\pm 1,1) = \begin{pmatrix} 1 & \pm 1/2 \\ \pm 1/2 & 1 \end{pmatrix}, \quad (1,\pm 2,1) = \begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix}.$$

De plus, étant donné que nous avons les deux relations suivantes

$$\begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1/2 \\ -1/2 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

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

alors par la relation sur les coefficients de la q-expansion d'une forme modulaire de Siegel on a que $A_k^2(1,1,1) = A_k^2(1,-1,1)$ et $A_k^2(1,2,1) = A_k^2(1,-2,1)$. Donc, en comparant les coefficients devant le terme $e^{2\pi i(z+w)}$ nous obtenons l'équation

$$A_k^2(1,0,1) + 2A_k^2(1,1,1) + 2A_k^2(1,2,1) = \left(\frac{2k}{B_k}\right)^2 + \sum_{f\in\mathcal{B}_k} \mu_f. \tag{3.2}$$

Notons que la trace apparait dans la dernière formule grâce à cette égalité

$$\sum_{f\in\mathcal{B}_k} \mu_f = \frac{-2^{5-2k}k!}{(\frac{k}{2}-1)!} \times \frac{1}{B_k B_{2k-2}} \times \mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2)).$$

Il nous reste donc à calculer explicitement tous les termes de chaque côté de l'équation (3.2) et de simplifier le tout. Par la formule des coefficients de la série d'Eisenstein de degré 2 qui a été donné à la section 2.4, on en retient que

$$A_k^2(1,0,1) = \frac{-4kB_{k-1,(\frac{-4}{\cdot})}}{B_k B_{2k-2}}, \quad \text{et} \quad A_k^2(1,1,1) = \frac{-4kB_{k-1,(\frac{-3}{\cdot})}}{B_k B_{2k-2}}. \tag{3.3}$$

Calculons maintenant le coefficient $A_k^2(1,2,1)$. Pour cela, nous allons plutôt utiliser le fait que $\Phi(E_k^2) = E_k$. Tout d'abord, remarquons que nous avons

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

et donc $A_k^2(1,2,1) = A_k^2(1,0,0)$. Ensuite, par le corollaire 2.3.5 sur la q-expansion de l'image d'une forme modulaire sous l'opérateur Φ appliqué à E_k^2, on a que le coefficient $A_k^2(1,0,0)$ doit être égal au coefficient $-2k/B_k$ de la série d'Eisenstein de degré 2. Enfin, pour obtenir la formule de la trace escomptée, il reste tout simplement à remplacer la dernière égalité et les deux relations (3.3) dans l'équation (3.2) et d'isoler la trace.

3.3 p-valuation de la trace et le nombre de classes d'un corps quadratique imaginaire

Rappelons que notre but est d'obtenir de l'information sur le nombre de classe d'un corps quadratique imaginaire avec la valuation p-adique de la trace de la fonction L carré-symétrique. Ainsi, nous étudierons quelques résultats préliminaires sur des propriétés arithmétiques des nombres de Bernoulli. Les démonstrations des prochaines propriétés peuvent être trouvées dans le livre [AIK14]. Tout d'abord, le théorème de Von-Staudt-Clausen nous permet de déterminer les premiers dans les dénominateurs des nombres de Bernoulli :

Lemme 3.3.1 (Von-Staudt-Clausen). *Pour $k = 1$ et pour tout entier $k \geq 2$ pair, nous avons que*

$$B_k + \sum_{\substack{p \text{ premier} \\ p-1|k}} \frac{1}{p} \in \mathbb{Z}.$$

Remarque 3.3.2. Ce résultat nous permet de dire que le dénominateur de B_k est exactement le produit des premiers p tels que $(p-1) \mid k$. Par exemple, pour $k = 24$ nous avons que

$$B_{24} = \frac{-236364091}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13}.$$

Lemme 3.3.3 ([Car59]). *Soit χ un caractère de Dirichlet primitif modulo m.*

1. *Si $f = 4$, alors*

$$\frac{B_{n,\chi}}{n} \equiv \begin{cases} 1/2 \pmod{\mathbb{Z}} & (n \text{ impair}); \\ 0 \pmod{\mathbb{Z}} & (n \text{ pair}). \end{cases}$$

2. *Si $m = p$ est un premier impair, alors $B_{n,\chi}/n$ est un entier algébrique sauf s'il existe un élément $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que*

$$\mathfrak{p} = (p, 1 - \chi(g)) \neq (1).$$

et que g est une racine primitive p^r-ième de l'unité pour tout $r \geq 1$. Dans ce cas, on a que $pB_{n,\chi} \equiv p - 1 \pmod{\mathfrak{p}^{n+1}}$.

Ensuite, rappelons les congruences de Kummer.

Lemme 3.3.4. *Soit p un nombre premier impair.*

(a) Si k est un nombre pair non divisible par $p-1$, alors le dénominateur de B_k/k n'est pas divisible par p.

(b) Soit k et k' deux entiers pairs positifs non divisibles par $p-1$ qui sont congrus modulo $p-1$. Alors, nous avons que

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod{p}.$$

Démonstration. Voir théorème 3.2 de [AIK14] □

L'intérêt que nous portons pour les nombres de Bernoulli provient du fait qu'ils sont en lien avec le nombre de classes du corps quadratique $\mathbb{Q}(\sqrt{-p})$, que nous dénotons $h(-p)$ (le lecteur est référé à la page 11 pour la définition). Plus précisément, nous avons une congruence suivante :

Lemme 3.3.5. *Si $p > 3$ est un premier tel que $p \equiv 3 \pmod 4$ et $k = (p+1)/2$, alors nous avons la congruence suivante*

$$h(-p) \equiv -2B_k \pmod{p}.$$

Une démonstration détaillée de ce lemme peut être trouvée dans le livre [AIK14, Theorem 7.1]. Cette congruence sera la clé qui établira le lien entre la trace et le nombre de classes de $\mathbb{Q}(\sqrt{-p})$.

Par la suite, nous aurons également besoin d'une borne classique sur le nombre de classe d'un corps quadratique imaginaire.

Lemme 3.3.6. *Soit K un corps quadratique imaginaire de discriminant D. Alors*

$$h(D) \leq \sqrt{|D|}\log|D|.$$

Démonstration. Par la formule analytique du nombre de classes appliquée à un corps quadratique imaginaire, on a que

$$h(D) = \frac{w\sqrt{|D|}}{2\pi}L(1,\chi_D) \overset{(*)}{\leq} \sqrt{|D|}\log|D|.$$

L'inégalité $(*)$ est un résultat classique de théorie analytique des nombres. Une démonstration peut être trouvée dans [Lou01, Theorem 1]. □

Corollaire 3.3.7. *Si $p \equiv 3 \pmod 4$ et $k = (p+1)/2$, alors B_k est inversible modulo p.*

Démonstration. Par le lemme 3.3.6, on a que $h(-p) \leq \sqrt{p}\log p < p$. Donc $h(-p)$ est inversible modulo p. Le corollaire découle de la congruence du lemme 3.3.5. □

Enfin, un théorème important qui sera utile est le théorème d'Heegner-Stark [Sta67]. Ce théorème classifie complètement les corps quadratiques imaginaires ayant un nombre de classes égal à 1.

Théorème 3.3.8 (Heegner, Stark)**.** *Soit D un entier négatif libre de carré. Alors $h(D) = 1$ si et seulement si*

$$D \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}.$$

Théorème 3.3.9 (Dummigan, Heim)**.** *Soit $p \geq 23$ un premier congru à 3 modulo 4 et $k := (p+1)/2$, alors*

1. *$v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) = -1$ si et seulement si $h(-p) > 1$;*
2. *Si $h(-p) = 1$, alors $v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) = 0$,*

où v_p est la valuation p-adique.

Démonstration. La démonstration consiste à directement calculer la p-valuation en utilisant la formule

$$\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2)) = c_k\left(B_{k-1,(\frac{-4}{\cdot})} + 2B_{k-1,(\frac{-3}{\cdot})} + B_{2k-2}\left(1+\frac{k}{B_k}\right)\right), \tag{3.4}$$

où

$$c_k = 2^{2k-1}\frac{(k/2-1)!}{(k-1)!}.$$

Soit $p \equiv 3 \pmod 4$ un premier et $k = (p+1)/2$. Nous obtenons l'équation

$$\begin{aligned} &v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) \\ &\quad = v_p(c_k) + \min\left\{v_p(B_{k-1,(\frac{-4}{\cdot})} + 2B_{k-1,(\frac{-3}{\cdot})}), v_p(B_{2k-2}(1+\frac{k}{B_k}))\right\}. \end{aligned} \tag{3.5}$$

Tout d'abord, par la définition de c_k, nous avons $v_p(c_k) = 0$. Ensuite, la première partie du lemme 3.3.3 nous permet de déduire que $v_p(B_{k-1,(\frac{-4}{\cdot})}) \geq 0$. La deuxième partie nous donne la même affirmation avec le nombre $B_{k-1,(\frac{-3}{\cdot})}$. Donc, nous avons

$$v_p(B_{k-1,(\frac{-4}{\cdot})} + 2B_{k-1,(\frac{-3}{\cdot})}) \geq 0.$$

Maintenant, puisque $2k - 2 = p - 1$, on déduit par le théorème de Von-Staudt-Clausen que $v_p(B_{2k-2}) = -1$. Ainsi, par le lemme 3.3.5 et le corollaire 3.3.7, on obtient que

$$1 + \frac{k}{B_k} = 1 + \frac{p-1}{2B_k} \equiv 1 - h(-p)^{-1} \pmod{p}.$$

Par conséquent, nous avons deux cas : si $h(-p) > 1$ ou si $h(-p) = 1$.

1. Si $h(-p) > 1$, alors $1 + \frac{1}{B_k} \not\equiv 0 \pmod{p}$, autrement dit, $v_p(1 + \frac{1}{B_k}) = 0$. En conséquence, l'unique présence de p^{-1} dans la factorisation de la trace provient de B_{2k-2}, c'est-à-dire que
$$v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) = -1.$$
2. Si $h(-p) = 1$, alors le théorème d'Heegner-Stark nous dit que nous avons seulement un nombre fini de cas à vérifier. Par notre hypothèse que $p \geq 23$, nous avons les trois possibilités suivante : $p = 43, 67$ ou 163. Des calculs explicites de la trace à l'aide de PARI/GP nous permettent effectivement de vérifier que
$$v_p(\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))) = 0$$
pour ces trois valeurs de p. On réfère le lecteur au chapitre 5 pour les méthodes numériques.

□

Le dernier théorème nous donne de l'information pour seulement un poids fixé de l'espace des formes cuspidales. Cependant, il est possible de généraliser ce résultat pour une infinité de poids en utilisant les congruences de Kummer pour les nombres de Bernoulli.

Théorème 3.3.10. *Soit $p \geq 23$ un premier congru à 3 modulo 4 et $k := (p+1)/2$. Soit k' un entier tel que $k' \equiv k \pmod{p-1}$. Alors,*

1. $v_p(\mathrm{Tr}_{k'}(L(\mathrm{Sym}^2, 2k'-2))) = v_p(c_{k'}) - 1$ *si et seulement si* $h(-p) > 1$;
2. *Si* $h(-p) = 1$, *alors* $v_p(\mathrm{Tr}_{k'}(L(\mathrm{Sym}^2, 2k'-2))) \geq v_p(c_{k'})$;

où

$$c_{k'} = 2^{2k'-1} \frac{(k'/2-1)!}{(k'-1)!}.$$

Démonstration. Ce théorème découle de l'équation (3.5). En effet, toujours par le lemme 3.3.3 nous avons que

$$v_p(B_{k'-1,\chi_{-4}} + 2B_{k'-1,\chi_{-3}}) \geq 0.$$

Aussi, par la congruence de Kummer pour les nombres de Bernoulli et le lemme 3.3.5, nous obtenons la nouvelle congruence

$$1 + \frac{k'}{B_{k'}} \equiv 1 - h(-p)^{-1} \pmod{p}.$$

Ce qu'il reste à vérifier est que $v_p(B_{2k'-2}) = -1$. Soit $m \in \mathbb{Z}$ tel que $k' = k + m(p-1)$. Alors, nous avons que $2k' - 2 = (2m+1)(p-1)$. Donc, par le théorème de Von-Staudt Clausen, la p-valuation de $B_{2k'-2}$ est de -1. Par conséquent, si $h(-p) > 1$, alors

$$\begin{aligned} v_p(\mathrm{Tr}_{k'}(L(\mathrm{Sym}^2, 2k'-2))) &= v_p(c_{k'}) + \min\left\{ v_p(B_{k'-1,\chi_{-4}} + 2B_{k'-1,\chi_{-3}}), v_p(B_{2k'-2}(1 + \frac{k'}{B_{k'}})) \right\} \\ &= v_p(c_{k'}) - 1. \end{aligned}$$

Maintenant, si $h(-p) = 1$, alors les quantités dans le minimum du calcul précédent sont toutes plus grandes ou égales à 0. On en conclut donc que $v_p(\mathrm{Tr}_{k'}(L(\mathrm{Sym}^2, 2k'-2))) \geq v_p(c_{k'})$. □

Ce théorème est une généralisation du théorème 3.3.9 pour une infinité de poids de l'espace des formes cuspidales. En effet, si $k' = k$, alors on retrouve quasiment le théorème de Dummigan et Heim. La seule différence est que le numéro 2 du théorème 3.3.10 nous dit que la p-valuation de la trace est plus grande ou égale à 0, alors que le théorème de Dummigan et Heim nous donne une égalité. Rappelons que la méthode de Dummigan et Heim pour obtenir cette égalité était d'utiliser le théorème d'Heegner-Stark et de vérifier numériquement tous les cas possibles. Cette idée se généralise difficilement dans le cas général puisque nous avons une infinité de poids, donc une infinité de cas à vérifier. À l'aide de calculs numériques, nous avons observé qu'il s'agit d'une égalité dans beaucoup de cas, sauf pour certains cas précis. Par ces observations, nous avons formulé cette conjecture :

Conjecture 3.3.11. *Soit $p = 43, 67$ ou 163. et $k := (p+1)/2$. Soit $m \geq 0$ et $k' := k + m(p-1)$. Alors,*

$$v_p(\mathrm{Tr}_{k'}(L(\mathrm{Sym}^2, 2k'-2))) = \begin{cases} v_p(c_{k'}) + 1 & \text{si } p \mid 2m+1; \\ v_p(c_{k'}) & \text{sinon.} \end{cases}$$

Cette conjecture a été vérifiée pour les valeurs de m entre 0 et 300 (voir chapitre 5). Il y a donc évidence de croire que cette conjecture est vraie. Une meilleure compréhension de la valuation p-adique des nombres de Bernoulli pourrait certainement aider à résoudre ce problème.

Pour terminer, faisons la remarque que la p-valuation du facteur $c_{k'}$ est relativement simple à calculer. En effet, rappelons que ce dernier est définie par

$$c_{k'} = 2^{2k'-1} \frac{(k'/2-1)!}{(k'-1)!}.$$

Par conséquent, le calcul de $v_p(c_{k'})$ est réduit au calcul de la p-valuation d'une factorielle, qui est connue par la formule de Legendre :

$$v_p(x!) = \sum_{k=1}^{\infty} \left\lfloor \frac{x}{p^k} \right\rfloor, \quad x \in \mathbb{Z}_{\geq 1}.$$

Chapitre 4

Congruences diédrales pour les formes cuspidales

Dans ce chapitre, nous étudions un autre lien entre les formes modulaires et le nombre de classes d'un corps quadratique. Plus précisément, si $p \equiv 3 \pmod 4$ et $k = (p+1)/2$ Dummigan et Heim [DH10, Theorem III] ont démontré qu'il existe une forme modulaire de poids k qui satisfait une congruence diédrale en p si et seulement si le nombre de classes est strictement plus grand que 1. Pour ce faire, ils ont eu recours aux représentations galoisiennes modulo p. Cet outil permet de construire des formes modulaires à partir de caractères sur des groupes de Galois. De plus, pour établir un lien entre les congruences sur les formes modulaires et le nombre de classes, Dummigan et Heim se sont servis d'un résultat sur la théorie des corps de classe. Ainsi, dans un premier temps, nous donnerons la démonstration de Dummigan et Heim avec davantage de détails et, dans un deuxième temps, nous généraliserons leur résultat pour des poids k' tels que $k' \equiv k \pmod{p-1}$.

4.1 Représentations galoisiennes

La théorie des représentations galosiennes est l'étude des représentations du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Cette théorie intervient dans la théorie des formes modulaires grâce à un théorème que Deligne a démontré [Del71]. Brièvement, ce théorème stipule que, pour une forme modulaire donnée, il est possible de construire une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Serre [Ser87] a conjecturé une réciproque à ce théorème pour les formes modulaires réduites modulo p. Cette conjecture, qui a été démontrée par Khare et Wintenberger ([KW09a] et [KW09b]), nous permettra de construire une forme modulaire qui satisfait une congruence diédrale.

4.1.1 Rappels sur la ramification

Les résultats mentionnés dans cette sous-section peuvent être trouvés dans le chapitre 1 de [Neu99]. Soit $K/\mathbb{Q}$ un corps de nombres et $\mathcal{O}_K$ l'anneau des entiers algébriques associé. Les

idéaux de $\mathcal{O}_K$ admettent une factorisation unique [Neu99, Chap. I, Theorem 3.3]. Plus précisément, si $0 \neq \mathfrak{a} \subsetneq \mathcal{O}_K$ est un idéal, alors il existe des idéaux premiers uniques $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$ et des entiers uniques $e_1, e_2, \ldots, e_g \in \mathbb{Z}_{\geq 1}$ tels que

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}.$$

En particulier, si $K/\mathbb{Q}$ est une extension de Galois et p est un premier rationnel, alors l'idéal principal $(p) = p\mathcal{O}_K$ admet une factorisation de la forme

$$(p) = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g)^e,$$

où $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_K$, g et e sont des entiers [Neu99, Chap. I, §9]. Les idéaux $\mathfrak{p}_i$ sont appelés les *premiers de K au-dessus de p*. Nous dénoterons par $k_{\mathfrak{p}_i}$ le corps résiduel $\mathcal{O}_K/\mathfrak{p}_i$. Il s'agit bien d'un corps, parce que les idéaux premiers non-nuls de $\mathcal{O}_K$ sont maximaux [Neu99, Chap. I, Theorem 3.1]. Si $f = [k_{\mathfrak{p}_i} : \mathbb{F}_p]$ (notons que f est indépendant de i), alors nous avons cette formule

$$[K : \mathbb{Q}] = efg.$$

Les trois quantités e, f et g dépendent évidemment de p et sont respectivement nommées le *degré de ramification*, le *degré d'inertie* et l'*indice de décomposition*.

Définition 4.1.1. Soit p un premier rationnel admettant la factorisation

$$(p) = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g)^e, \quad f = [k_{p_i} : \mathbb{F}_p].$$

Alors, p est dit *ramifié* si $e > 1$ et *non ramifié* autrement. Si $g = 1$ et $f = 1$, alors on dit que p est *totalement ramifié*. Si $e = 1$ et $f = 1$, alors on dit que p est *totalement décomposé*. Enfin, si $e = 1$ et $g = 1$, alors on dit que p est *inerte dans K*, c'est-à-dire que (p) est un idéal premier de $\mathcal{O}_K$.

Exemple 4.1.2. Si $K/\mathbb{Q}$ est un corps quadratique de discriminant D, alors la factorisation de (p) est complètement déterminée en termes du symbole de Legendre. En effet, si $(D/p) = 1$, alors il existe deux premiers distincts $\mathfrak{p}$ et $\mathfrak{q}$ au dessus de p tels que $(p) = \mathfrak{pq}$. Ensuite, si $(D/p) = -1$, alors p est inerte dans K, autrement dit il existe un unique premier $\mathfrak{p}$ au dessus de p tel que $(p) = \mathfrak{p}$. Enfin, si $(D/p) = 0$, alors p est totalement ramifié dans K, autrement dit $(p) = \mathfrak{p}^2$ pour un premier $\mathfrak{p}$ au dessus de p. Cela découle de la proposition 8.5 de [Neu99, Chap. I] et du fait que p est ramifié dans K si et seulement si p divise D [Neu99, Chap. III, Corollary 2.12]. Nous résumons cette discussion par la formule suivante :

$$(p) = \begin{cases} \mathfrak{pq}, & \text{si } (D/p) = 1; \\ \mathfrak{p}, & \text{si } (D/p) = -1; \\ \mathfrak{p}^2, & \text{si } (D/p) = 0. \end{cases}$$

Il est important de noter que le groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$ agit transitivement sur les premiers au-dessus de p de manière naturelle : $\sigma \cdot \mathfrak{p} := \sigma(\mathfrak{p})$ [Neu99, Proposition 9.1].

Définition 4.1.3. Le *groupe de décomposition* de $\mathfrak{p}$ est le sous-groupe de $\mathrm{Gal}(K/\mathbb{Q})$ suivant

$$D_{\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma \cdot \mathfrak{p} = \mathfrak{p}\}.$$

Le *groupe d'inertie* de $\mathfrak{p}$ est défini par

$$I_{\mathfrak{p}} := \{\sigma \in D_{\mathfrak{p}} : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{p},\ \forall \alpha \in \mathcal{O}_K\}.$$

Remarque 4.1.4. Si p est un premier totalement décomposé, alors il découle de la définition du groupe de décomposition et du fait que l'action de $\mathrm{Gal}(K/\mathbb{Q})$ est transitive sur les premiers au-dessus de p que $D_{\mathfrak{p}} = \{1\}$.

Proposition 4.1.5.

1. *$D_{\mathfrak{p}}$ est un sous-groupe d'ordre ef et d'indice g dans* $\mathrm{Gal}(K/\mathbb{Q})$ *;*
2. *$I_{\mathfrak{p}}$ est un sous-groupe d'ordre e ;*
3. *Nous avons la suite exacte courte suivante*

$$1 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) \longrightarrow 1.$$

Le groupe de Galois $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$ est un groupe cyclique d'ordre f qui est engendré par l'*automorphisme de Frobenius* :

$$\begin{aligned} \sigma_p : k_{\mathfrak{p}} &\longrightarrow k_{\mathfrak{p}} \\ \alpha &\longmapsto \alpha^p. \end{aligned}$$

De la proposition 4.1.5, on déduit que $D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \langle \sigma_p \rangle$.

Définition 4.1.6. Un *élément de Frobenius*, dénoté $\mathrm{Frob}_{\mathfrak{p}}$, dans $\mathrm{Gal}(K/\mathbb{Q})$ est un choix d'une préimage de σ_p de l'application surjective $D_{\mathfrak{p}} \twoheadrightarrow \langle \sigma_p \rangle$. Si $\mathfrak{p}$ est non ramifié, alors $I_{\mathfrak{p}} = \{1\}$ et donc $\mathrm{Frob}_{\mathfrak{p}}$ est unique.

De cette définition, on remarque qu'un élément de Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ satisfait la propriété

$$\mathrm{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^p \bmod \mathfrak{p},\ \forall \alpha \in \mathcal{O}_K.$$

Si $\mathfrak{p}' = \sigma \cdot \mathfrak{p}$ est un premier conjugué à $\mathfrak{p}$, alors nous avons les relations suivantes

$$D_{\mathfrak{p}'} = \sigma^{-1} D_{\mathfrak{p}} \sigma, \quad I_{\mathfrak{p}'} = \sigma^{-1} I_{\mathfrak{p}} \sigma, \quad \text{et} \quad \mathrm{Frob}_{\mathfrak{p}'} = \sigma^{-1} \mathrm{Frob}_{\mathfrak{p}} \sigma.$$

La dernière de ces trois relations nous sera utile plus tard, car nous aurons à calculer la trace de la représentation d'un élément de Frobenius dans un groupe de transformations linéaires. En

particulier, la valeur de cette trace ne dépendra pas du choix de l'idéal premier au-dessus d'un certain premier rationnel et sera donc bien définie. Dans le cas où p est un nombre premier inerte dans K, alors on écrira tout simplement D_p, I_p et Frob_p.

Le choix d'un idéal premier $\mathfrak{p}$ au-dessus de p et la factorisation unique des idéaux de $\mathcal{O}_K$ nous permettent de définir une valuation sur K. En effet, pour $x \in K$, on définit $v_\mathfrak{p}(x)$ comme étant l'entier satisfaisant

$$(x) = x\mathcal{O}_K = \mathfrak{p}^{v_\mathfrak{p}(x)}\mathfrak{a},.$$

où $\mathfrak{a} \subset \mathcal{O}_K$ est un idéal tel que $\mathfrak{p} \nmid \mathfrak{a}$. La complétion de K par rapport à la valuation $v_\mathfrak{p}$ sera dénotée par $K_\mathfrak{p}$. Le corps $K_\mathfrak{p}$ est une extension finie de Galois du corps des nombres p-adique $\mathbb{Q}_p$. Plus précisément, on a

$$\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \cong D_\mathfrak{p}.$$

En particulier, si p est totalement décomposé, alors $K_\mathfrak{p} = \mathbb{Q}_p$.

Le sous-groupe d'inertie $I_\mathfrak{p}$ peut être vu comme un élément d'une suite décroissante de sous-groupe.

Définition 4.1.7. Soit $i \geq -1$ un entier. Alors, le *i-ième groupe de ramification* de $K/\mathbb{Q}$ associé à $\mathfrak{p}$ est défini par

$$G_i := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : v_\mathfrak{p}(\sigma(\alpha) - \alpha) \geq i + 1,\ \forall \alpha \in \mathcal{O}_K\}.$$

Remarques 4.1.8.

1. Nous avons que $G_{-1} = \mathrm{Gal}(K/\mathbb{Q})$ et $G_0 = I_\mathfrak{p}$.
2. Le groupe $R_\mathfrak{p} := G_1$ est appelé le *groupe de ramification* de $\mathfrak{p}$.

4.1.2 Le groupe de Galois absolu de $\mathbb{Q}$

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et $\overline{\mathbb{Z}}$ la clôture intégrale de $\mathbb{Z}$ dans $\overline{\mathbb{Q}}$. L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ est de degré infini et son groupe d'automorphisme $G_\mathbb{Q} := \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ est appelé le *groupe de Galois absolu de* $\mathbb{Q}$. Notons que si $K/\mathbb{Q}$ est une extension galoisienne (et donc de degré fini), alors $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ est un quotient de $G_\mathbb{Q}$. Pour avoir une bonne théorie de Galois pour $G_\mathbb{Q}$, nous avons besoin de le munir d'une topologie.

Définition 4.1.9. Soit $\sigma \in G_\mathbb{Q}$. Alors, l'ensemble

$$\left\{\sigma\mathrm{Aut}(\overline{\mathbb{Q}}/K) : K/\mathbb{Q} \text{ est galoisienne finie}\right\}$$

forme une base de voisinages ouverts de σ. Ces voisinages engendrent ce que l'on appelle la *topologie de Krull pour* $G_\mathbb{Q}$.

Proposition 4.1.10. *Le groupe de Galois absolu de $\mathbb{Q}$ muni de la topologie de Krull est compact et totalement discontinue.*

Démonstration. Voir [Neu99, Chap. IV, proposition 1.1]. □

Définition 4.1.11. Une extension algébrique de corps L/K est dite *galoisienne* ou de *Galois* si L/K est séparable et normale. Nous dénotons le groupe des automorphismes qui fixent le corps de base K par $\mathrm{Gal}(L/K)$.

Remarque 4.1.12. Cette définition est une bonne généralisation, puisque, dans le cas où l'extension L/K est finie, alors le fait d'être normale et séparable est équivalent au fait que $|\mathrm{Aut}(L/K)| = \#[L : K]$.

Il y a aussi une généralisation du théorème fondamentale de Galois. Cependant, dans le cas infini, les sous-extensions $K \subseteq K' \subseteq L$ ne correspondent pas exactement à tous les sous-groupes de $\mathrm{Gal}(L/K)$. En effet, il y a plus de sous-groupes que de sous-extensions. Il faut donc se restreindre aux sous-groupes fermés pour la topologie de Krull.

Théorème 4.1.13. *Soit L/K une extension de Galois. Alors, nous avons une bijection entre les deux ensembles suivants*

$$\begin{aligned} \{K' : K \subseteq K' \subseteq L\} &\longleftrightarrow \{H \leqslant \mathrm{Gal}(L/K) : H \textit{ est fermé}\} \\ K' &\longmapsto \mathrm{Gal}(L/K') \\ L^H &\longleftarrow\!\shortmid H. \end{aligned}$$

Dans le cas où l'extension L/K est de degré fini, alors le groupe de Galois est aussi fini. Ainsi, ce dernier sera muni de la topologie discrète. On retrouve donc le théorème fondamental de la théorie de Galois pour les extensions finies. Une bonne introduction à la théorie de Galois infinie est donnée dans [Neu99, Chap. IV §1].

Tout comme à la section précédente, il est également possible de définir les sous-groupes de décomposition et d'inertie de $G_{\mathbb{Q}}$. Soit p un nombre premier rationnel et $\mathfrak{p} \subset \overline{\mathbb{Z}}$ un idéal maximal au-dessus de p. Notons que, si $\mathcal{O}$ est l'anneau des entiers d'un corps de nombres, alors $\mathfrak{p} \cap \mathcal{O}$ sera un idéal premier de $\mathcal{O}$. On pose

$$D_{\mathfrak{p}} := \{\sigma \in G_{\mathbb{Q}} : \sigma \cdot \mathfrak{p} = \mathfrak{p}\}$$

et

$$I_{\mathfrak{p}} := \{\sigma \in D_{\mathfrak{p}} : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}}\ \forall \alpha \in \overline{\mathbb{Z}}\}.$$

De manière analogue à la proposition 4.1.5, si $G_{\mathbb{F}_p} := \mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, nous avons une suite exacte

$$1 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow G_{\mathbb{F}_p} \longrightarrow 1.$$

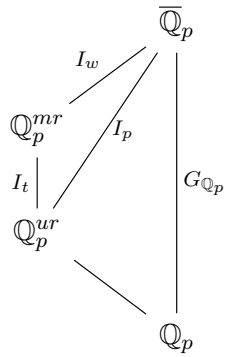
Ainsi, un *élément de Frobenius dans* $G_{\mathbb{Q}}$, dénoté $\mathrm{Frob}_{\mathfrak{p}}$, est un choix d'une pré-image dans $D_{\mathfrak{p}}$ de l'automorphisme de Frobenius $\sigma_p \in G_{\mathbb{F}_p}$. Si $K/\mathbb{Q}$ est un corps de nombres de Galois, alors la restriction de $\mathrm{Frob}_{\mathfrak{p}}$ à K donnera un élément de Frobenius dans $\mathrm{Gal}(K/\mathbb{Q})$.

L'idéal premier $\mathfrak{p}$ de $\overline{\mathbb{Z}}$ définit une valuation sur $\overline{\mathbb{Q}}$. La complétion de la clôture algébrique de $\mathbb{Q}$ par rapport à cette valuation donne $\overline{\mathbb{Q}}_p$, une clôture algébrique de $\mathbb{Q}_p$. L'extension infinie $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ est de Galois infinie et l'on écrit $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Ce groupe de Galois est un sous-groupe de $G_{\mathbb{Q}}$ qui est isomorphe à $D_{\mathfrak{p}}$.

Le groupe $G_{\mathbb{Q}_p}$ possède des sous-groupes importants. Soit $\mathbb{Q}_p^{ur}$ l'extension maximale non ramifiée de $\mathbb{Q}_p$ et $\mathbb{Q}_p^{mr}$ l'extension maximale modérément ramifiée de $\mathbb{Q}_p^{ur}$. On définit

$$I_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{ur}), \quad I_w := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{mr}), \quad I_t := \mathrm{Gal}(\mathbb{Q}_p^{mr}/\mathbb{Q}_p^{ur}).$$

Voici un diagramme à avoir en tête pour bien visualiser les dernières définitions :



Le sous-groupe I_p est appelé le *sous-groupe d'inertie de* $G_{\mathbb{Q}_p}$ et il est isomorphe à $I_{\mathfrak{p}}$. Pour terminer, une exposition de la théorie de ramification pour les extension galoisienne infinie est faite dans [Neu99, Chap. II].

4.1.3 Représentation galoisienne p-adique

Définition 4.1.14. Soit p un premier et $\mathfrak{p}$ un premier d'un corps de nombres K au-dessus de p. Une *représentation galoisienne* $\mathfrak{p}$*-adique de dimension* d est un homomorphisme continu

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

où V est un $K_{\mathfrak{p}}$-espace vectoriel de dimension $d < \infty$. Deux représentions galoisiennes ρ_1 et ρ_2 sont dites *équivalentes* s'il existe une transformation linéaire $\gamma \in \mathrm{GL}(V)$ telle que

$$\rho_2(\sigma) = \gamma^{-1}\rho_1(\sigma)\gamma, \quad \forall \sigma \in G_{\mathbb{Q}}.$$

Remarque 4.1.15. Si V est de dimension $d < \infty$, alors, nous avons l'isomorphisme de groupe $\mathrm{GL}(V) \cong \mathrm{GL}_d(K_{\mathfrak{p}})$. Cet isomorphisme n'est pas canonique, puisqu'il dépend d'un choix de base de V. Aussi, une représentation galoisienne nous donne en fait une action à gauche du groupe $G_{\mathbb{Q}}$ sur l'espace vectoriel V. En effet, pour $g \in G_{\mathbb{Q}}$ et $v \in V$, alors on pose $g \cdot v := \rho(g)(v)$. Par conséquent, une représentation p-adique de dimension d est aussi appelée un $G_{\mathbb{Q}}$*-module de dimension* d.

Sous les mêmes notations que la définition précédente, soit $\ell \in \mathbb{Q}$ un premier rationnel et $\mathfrak{l} \subset \mathcal{O}_K$ un premier au-dessus de ℓ. Soit $\mathrm{Frob}_\mathfrak{l} \in G_\mathbb{Q}$ un élément de Frobenius. Nous avons vu à la section 4.1.1 que si $\mathfrak{l}'$ est un autre premier au-dessus de ℓ, alors il existe un automorphisme $\sigma \in G_\mathbb{Q}$ tel que $\mathfrak{l}' = \sigma \cdot \mathfrak{l}$. De plus, on a que $\mathrm{Frob}_{\mathfrak{l}'} = \sigma^{-1}\mathrm{Frob}_\mathfrak{l}\sigma$. Du fait que ρ est un homomorphisme on obtient que

$$\mathrm{Tr}(\rho(\mathrm{Frob}_{\mathfrak{l}'})) = \mathrm{Tr}(\rho(\sigma^{-1}\mathrm{Frob}_\mathfrak{l}\sigma)) = \mathrm{Tr}(\rho(\mathrm{Frob}_\mathfrak{l})).$$

En d'autres mots, la trace d'un élément de Frobenius est indépendante du choix du premier au-dessus de ℓ. Nous dénoterons donc une telle trace tout simplement par $\mathrm{Tr}(\rho(\mathrm{Frob}_\ell))$.

Définition 4.1.16. Soit ℓ un nombre premier et I_ℓ son groupe de ramification associé. Une représentation galoisienne p-adique ρ est dite *non-ramifiée en* ℓ si $\rho(I_\ell) = \{1\}$.

Proposition 4.1.17. *Soit $\rho : G_\mathbb{Q} \to \mathrm{GL}(V) \cong \mathrm{GL}_d(K_\mathfrak{p})$ une représentation galoisienne $\mathfrak{p}$-adique de dimension d. Alors, ρ est équivalente (par conjugaison) à une représentation $\rho' : G_\mathbb{Q} \to \mathrm{GL}_d(\mathcal{O}_\mathfrak{p})$, où $\mathcal{O}_\mathfrak{p}$ est l'anneau des entiers de $K_\mathfrak{p}$.*

Démonstration. Voir proposition 9.3.5 de [DS05]. □

En vertu de la proposition précédente, nous pouvons considérer des *représentations galoisiennes modulo p*, c'est-à-dire, des homomorphismes continus

$$\overline{\rho} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p),$$

où $\overline{\mathbb{F}}_p = \cup_{n\geq 1}\mathbb{F}_{p^n}$. Nous donnons ici à $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$ la topologie discrète. Ceci implique que $\ker(\overline{\rho}) = \overline{\rho}^{-1}(\{\mathrm{id}_d\})$ est ouvert et compact, où id_d est la matrice identité $d \times d$. Donc, $\ker\overline{\rho}$ est d'indice fini dans $G_\mathbb{Q}$ et, par le premier théorème d'isomorphisme, l'image de $\overline{\rho}$ est finie. Par conséquent, il existe un entier $n \geq 1$ tel que $\mathrm{Im}(\overline{\rho}) \subset \mathrm{GL}_d(\mathbb{F}_{p^n})$.

Exemple 4.1.18. Soit p un nombre premier et $\mathbb{Q}(\mu_{p^\infty}) := \cup_{m\geq 1}\mathbb{Q}(\mu_{p^m})$ où

$$\mu_{p^m} := \{\zeta \in \mathbb{C} : \zeta^p = 1\}.$$

Alors, on a l'inclusion $\mathbb{Q}(\mu_{p^\infty}) \subset \overline{\mathbb{Q}}$. De ce fait, nous avons une surjection

$$\pi_p : G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}).$$

Par l'isomorphisme de groupe suivant

$$\chi_p : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times,$$

nous avons le *caractère cyclotomique p-adique* $\omega_p := \chi_p \circ \pi_p$ aussi appelé le caractère de Teichmüller. Le caractère cyclotomique p-adique défini un $\mathbb{Z}_p[G_\mathbb{Q}]$-module, disons W. Par

conséquent, le $G_{\mathbb{Q}}$-module $V := \mathbb{Q}_p \otimes_{\mathbb{Z}_p[G_{\mathbb{Q}}]} W$ sera une représentation galoisienne p-adique de dimension 1 sur $\mathbb{Q}_p$.

Le *caractère cyclotomique modulo* p, dénoté $\overline{\omega}_p$, est la réduction modulo p de ω_p. Ainsi, il s'agit d'un caractère de $G_{\mathbb{Q}}$ à image dans $\mathbb{F}_p^\times$. Supposons que $p \equiv 3 \pmod 4$ et considérons le symbole de Kronecker $(\frac{-p}{\cdot})$. Alors, il existe une relation entre $\overline{\omega}_p$ et $(\frac{-p}{\cdot})$:

$$\left(\frac{-p}{\cdot}\right) = \overline{\omega}_p^{\frac{p-1}{2}}. \tag{4.1}$$

En effet, si ζ est une racine primitive p-ième de l'unité, alors $\overline{\omega}_p$ peut être vu comme un caractère de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Ce groupe de Galois est isomorphe au groupe $\mathbb{F}_p^\times$ et ce dernier possède l'unique sous-groupe d'indice 2 suivant

$$H = \left\{ x \in \mathbb{F}_p^\times : \left(\frac{-p}{x}\right) = 1 \right\}.$$

Alors, par le théorème fondamental de la théorie de Galois, H correspond à une extension quadratique $L/\mathbb{Q}$. Du fait que le seul premier qui est ramifié dans $\mathbb{Q}(\zeta)$, on déduit que le seul premier qui se ramifie dans L est p. Donc, $L = \mathbb{Q}(\sqrt{-p})$, puisqu'il s'agit du seul corps quadratique qui est uniquement ramifié en p (car $\mathrm{disc}(\mathbb{Q}(\sqrt{-p})) = p$). Autrement dit, le corps quadratique $\mathbb{Q}(\sqrt{-p})$ est inclus dans le corps cyclotomique $\mathbb{Q}(\zeta)$. Cela implique que $(\frac{-p}{\cdot})$ peut être vu comme un caractère de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Ceci démontre la relation (4.1).

Définition 4.1.19. Soit c la conjugaison complexe. Une représentation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(K_{\mathfrak{p}})$ est dite *impaire* si $\det(\rho(c)) = -1$ où c et *pair* sinon.

4.1.4 Représentations galoisiennes associées à une forme modulaire

Soit $k \geq 2$ et N deux entiers et soit ε un caractère de Dirichlet primitif modulo N. Rappelons que si $f \in \mathcal{S}_k(\Gamma_0(N), \varepsilon)$ est une forme propre normalisée, alors f possède une q-expansion de la forme $f = \sum_{n=1}^{\infty} a_n q^n$, $q = e^{2\pi i z}$, $z \in \mathbb{H}$. De plus, les a_n sont des entiers algébriques et l'extension $\mathbb{Q}_f = \mathbb{Q}(\{a_n : n \geq 1\})$ est un corps de nombre. Aussi surprenant que cela puissent paraître, il est possible d'associer à une telle forme f une représentation galoisienne de dimension 2. Ce lien a été établi par Deligne dans son article [Del71]. Voici l'énoncé du théorème.

Théorème 4.1.20 (Deligne)**.** *Soit $k \geq 2$ et ε un caractère de Dirichlet modulo N. Soit $f \in \mathcal{S}_k(\Gamma_0(N), \varepsilon)$ une forme propre normalisée avec corps de nombres $\mathbb{Q}_f$ et p un nombre premier. Pour tout premier $\mathfrak{p}$ de $\mathbb{Q}_f$ au-dessus de p, il existe une représentation galoisienne p-adique de dimension 2 irréductible*

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_{f,\mathfrak{p}})$$

qui est non ramifiée en chaque premier ℓ qui ne divisent pas pN. Pour un tel premier ℓ, nous avons que

$$\mathrm{Tr}(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) = a_\ell \quad \text{et} \quad \det(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) = \varepsilon(\ell)\ell^{k-1}. \tag{4.2}$$

Remarque 4.1.21. À partir des relations (4.2), il est possible de montrer que $\det(\rho_f) = \varepsilon\omega_p^{k-1}$.

Définition 4.1.22. Une représentation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{\mathfrak{p}})$ est dite *modulaire* s'il existe une forme propre normalisée f de sorte que ρ est équivalente à $\rho_{f,\mathfrak{p}}$. De manière similaire, une représentation galoisienne $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ modulo p est dite *modulaire* s'il existe une forme propre normalisée f telle que $\overline{\rho}$ est équivalente à $\overline{\rho}_{f,\mathfrak{p}}$

Exemple 4.1.23. Soit $f \in \mathcal{S}_k(\Gamma_0(N), \varepsilon)$ une forme propre normalisée et $\rho_{f,\mathfrak{p}}$ la représentation associée. Alors, $\rho_{f,\mathfrak{p}}$ correspond à un $G_{\mathbb{Q}}$-module V de dimension 2. Pour $m \geq 1$, on pose

$$\mathrm{Sym}^m(f) := V^{\otimes m}/\{v_1 \otimes v_2 \otimes \cdots \otimes v_m - v_{\pi(1)} \otimes v_{\pi(2)} \otimes \cdots \otimes v_{\pi(m)} : v_i \in V, \pi \in S_m\}.$$

où S_m est le groupe des permutations de $\{1, 2, \ldots, m\}$. Alors, $\mathrm{Sym}^m(f)$ est une représentation $\mathfrak{p}$-adique de $G_{\mathbb{Q}}$ de dimension $m+1$.

Il existe une réciproque au théorème 4.1.20. En effet, il s'agit d'une conjecture de Serre qui a été énoncée en 1973 [Ser87]. Cette conjecture a été démontrée partiellement en 2005 par Khare [Kha06] et entièrement en 2008 par Khare en travail conjoint avec Wintenberger. La démonstration complète se trouve dans [KW09a] et [KW09b]. Brièvement, la conjecture de Serre stipule qu'une représentation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ qui est *impaire* et *irréductible* est forcément modulaire. Afin de formuler cette conjecture, Serre a associé trois quantités à une telle représentation : un niveau $N(\rho)$, un poids $k(\rho)$ et un caractère $\varepsilon(\rho) : (\mathbb{Z}/N(\rho)\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$. Voici l'énoncé de cette conjecture qui est maintenant un théorème.

Théorème 4.1.24 (Khare-Wintenberger)**.** *Soit*

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

une représentation galoisienne modulo p qui est irréductible et impaire. Alors, il existe une forme propre cuspidale f de poids $k(\rho)$, de niveau $N(\rho)$ et de caractère $\varepsilon(\rho)$ à coefficients dans $\overline{\mathbb{F}}_p$ telle que $\rho \sim \overline{\rho}_{f,p}$.

Dans ce qui suit, p est un nombre premier fixé et

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

est une représentation galoisienne modulo p où V est un $\overline{\mathbb{F}}_p$-espace vectoriel de dimension 2. Notre but est de définir le niveau $N(\rho)$ et le poids $k(\rho)$ de la représentation ρ. Étant donné que seul le cas $N(\rho) = 1$ sera nécessaire pour la démonstration du théorème de Dummigan et Heim sur les congruences diédrales, nous ne donnerons pas la définition du caractère $\varepsilon(\rho)$. Les constructions complètes de ces quantités sont données dans [Ser87].

4.1.5 Le niveau $N(\rho)$

Commençons par définir l'entier $N(\rho)$. Soit $\ell \neq p$ un premier et $\mathfrak{l} \subset \overline{\mathbb{Z}}$ un premier au-dessus de ℓ. Considérons la suite G_i, $i \geq 0$, des groupes de ramification associés à $v_{\mathfrak{l}}$. Soit $V_i := V^{G_i}$ le sous-espace des éléments de V qui sont fixés par l'action de G_i. Définissons la quantité suivante :

$$n(\ell, \rho) := \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim V/V_i.$$

Proposition 4.1.25. *La quantité $n(\ell, \rho)$ est un entier positif. De plus, $n(\ell, \rho) = 0$ si et seulement si ρ est non ramifiée en ℓ.*

Définition 4.1.26. Le *niveau* de ρ est défini par

$$N(\rho) := \prod_{\ell \neq p} \ell^{n(\ell, \rho)}.$$

Remarque 4.1.27. Par la proposition 4.1.25, si ρ est non ramifiée en ℓ pour tout premier $\ell \neq p$, alors $N(\rho) = 1$.

4.1.6 Le poids $k(\rho)$

Maintenant, nous allons définir le poids $k(\rho)$. L'entier $k(\rho)$ dépend uniquement de la *localisation* de ρ en p. Cette dernière est la représentation ρ_p de $G_{\mathbb{Q}_p}$ que l'on obtient à partir de ρ. Considérons $\rho_p|_{I_p}$, la restriction de ρ_p au groupe d'inertie associé à p. On définit la *semi-simplification de* $\rho_p|_{I_p}$, dénoté $\rho_p|^{ss}_{I_p}$, comme étant la somme directe des sous-quotients irréductibles de $\rho_p|_{I_p}$. Autrement dit, si W est le $\overline{\mathbb{F}}_p$-espace vectoriel sur lequel I_p agit, alors la semi-simplification de W est définie par

$$W^{ss} := \bigoplus_{i \geq 1} W_{i+1}/W_i$$

où $(W_i)_{i \geq 1}$ est une suite de sous-modules de W tels que $W_i \subset W_{i+1}$ et W_{i+1}/W_i est irréductible. On peut montrer que le module W^{ss} est bien défini à isomorphisme près. Notons que si $\rho_p|_{I_p}$ est irréductible, alors $\rho_p|^{ss}_{I_p} = \rho_p|_{I_p}$, car une représentation irréductible est semi-simple.

Il est connu par un article de Serre que $\rho_p|^{ss}_{I_p}(I_w) = \{1\}$ (voir [Ser72, Proposition 4]) où I_w est le groupe défini à la fin de la section 4.1.2. Ainsi, $\rho_p|^{ss}_{I_p}$ se factorise sur I_t. Puisque I_t est un groupe abélien, alors la restriction $\rho_p^{ss}|_{I_t}$ est diagonalisable et donc elle est de la forme suivante :

$$\rho_p^{ss}|_{I_t} \sim \begin{pmatrix} \phi & 0 \\ 0 & \phi' \end{pmatrix},$$

où $\phi, \phi' : I_t \to \overline{\mathbb{F}}_p^{\times}$ sont des caractères. Ensuite, la proposition 2 de [Ser72] stipule que

$$I_t \cong \varprojlim \mathbb{F}_{p^n}^{\times}.$$

Donc, nous disons qu'un caractère $\varphi : I_t \to \overline{\mathbb{F}}_p^\times$ est de *niveau* n si n est le plus petit entier tel que nous avons le diagramme commutatif suivant :

$$\begin{array}{ccc} I_t & \xrightarrow{\quad\varphi\quad} & \overline{\mathbb{F}}_p^\times. \\ & \searrow \quad \nearrow & \\ & \mathbb{F}_{p^n}^\times & \end{array}$$

Les caractères $I_t \to \mathbb{F}_{p^n}^\times \to \overline{\mathbb{F}}_p^\times$ qui sont induits par les plongements $\mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$ sont appelés les *caractères fondamentaux de niveau* n. Il y a n caractères fondamentaux, car $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. La définition de l'entier $k(\rho)$ dépend du niveau de ϕ et ϕ' et de la restriction de ρ_p à I_w. La prochaine proposition nous indique qu'il n'y a pas beaucoup de cas possibles.

Proposition 4.1.28 (No. 2.3 de [Ser87])**.**

1. *Les caractères ϕ et ϕ' sont de niveau* 1 *ou* 2.
2. *Si ϕ et ϕ' sont de niveau* 1 *et $\rho_p|_{I_w}$ est trivial, alors il existe des entiers a et b tels que $0 \leq a \leq b \leq p-2$ et*
$$\rho_p|_{I_p} \sim \begin{pmatrix} \omega_p^a & 0 \\ 0 & \omega_p^b \end{pmatrix},$$
où ω_p est le caractère cyclotomique p-adique.

Définition 4.1.29. Dans le cadre du numéro 2 de la proposition 4.1.28, on définit le poids de ρ comme étant

$$k(\rho) := \begin{cases} 1 + pa + b & \text{si } (a,b) \neq (0,0); \\ p & \text{sinon.} \end{cases}$$

4.1.7 Représentation induite

Pour terminer cette section, nous allons étudier la représentation induite d'une représentation dans un cas particulier. Soit K un corps quadratique. Alors, $H := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ est un sous-groupe d'indice 2 de $G_{\mathbb{Q}}$. Considérons un $\overline{\mathbb{F}}_p^\times$-caractère de H :

$$\tau : H \longrightarrow \overline{\mathbb{F}}_p^\times.$$

Ainsi, τ définit un $\overline{\mathbb{F}}_p[H]$-module de dimension 1 que nous allons noter $V = \langle v \rangle$. Pour obtenir un $\overline{\mathbb{F}}_p[G_{\mathbb{Q}}]$-module, nous posons

$$W := \overline{\mathbb{F}}_p[G_{\mathbb{Q}}] \otimes_{\overline{\mathbb{F}}_p[H]} V.$$

La représentation Galosienne modulo p associée à W sera dénotée $\mathrm{Ind}_K^{\mathbb{Q}}\tau$ et s'appelle *la représentation induite de K à $\mathbb{Q}$.*

Puisque H est d'indice 2 dans $G_{\mathbb{Q}}$, nous avons la décomposition en somme directe suivante

$$\overline{\mathbb{F}}_p[G_{\mathbb{Q}}] = \overline{\mathbb{F}}_p[H] \oplus \sigma\overline{\mathbb{F}}_p[H],$$

où σ est conjugaison dans $\mathrm{Gal}(K/\mathbb{Q})$. Par conséquent, nous avons que

$$W \cong V \oplus V^{\sigma}$$

où $V^{\sigma} := \{\sigma \otimes \lambda v : \lambda \in \overline{\mathbb{F}}_p\}$. Donc, $\mathrm{Ind}_K^{\mathbb{Q}}\tau$ sera une représentation de dimension 2 admettant la base suivante

$$\mathcal{B} = \{1 \otimes v, \sigma \otimes v\}.$$

Décrivons maintenant l'action de $G_{\mathbb{Q}}$ sur W. Notons que H est un sous-groupe normal de $G_{\mathbb{Q}}$ et σ est une involution, donc $\sigma H \sigma = H$. Soit $g \in G_{\mathbb{Q}} = H \sqcup \sigma H$. Il y a deux cas de figure possibles : $g \in H$ ou bien $g \in \sigma H$.

1. Si $g \in H$, alors

$$g(1 \otimes v) = g \otimes v = 1 \otimes \tau(g)v,$$

et

$$g(\sigma \otimes v) = g\sigma \otimes v = \sigma^2 g\sigma \otimes v = \sigma \otimes \tau(\sigma g \sigma)v.$$

Donc, la matrice représentative de g dans la base $\mathcal{B}$ est donnée par

$$\mathrm{Ind}_K^{\mathbb{Q}}\tau(g) = \begin{pmatrix} \tau(g) & 0 \\ 0 & \tau(\sigma g \sigma) \end{pmatrix}.$$

2. Si $g \in \sigma H$, alors

$$g(1 \otimes v) = g \otimes v = \sigma^2 g \otimes v = \sigma \otimes \tau(\sigma g)v,$$

et

$$g(\sigma \otimes v) = g\sigma \otimes v = 1 \otimes \tau(g\sigma)v.$$

Donc, la matrice représentative de g dans la base $\mathcal{B}$ est donnée par

$$\mathrm{Ind}_K^{\mathbb{Q}}\tau(g) = \begin{pmatrix} 0 & \tau(g\sigma) \\ \tau(\sigma g) & 0 \end{pmatrix}.$$

Par exemple, pour $g = \sigma$, nous sommes dans le deuxième cas et on a

$$\mathrm{Ind}_K^{\mathbb{Q}}\tau(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

donc $\det(\sigma) = -1$. Autrement dit, $\mathrm{Ind}_K^{\mathbb{Q}}\tau$ est une représentation galoisienne impaire.

4.2 Congruences sur les formes modulaires

Pour ce qui suivra, nous fixons deux plongements $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ et $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Rappelons que que, par le théorème 1.1.7, les coefficients d'une forme propre normalisée f sont des entiers algébriques. Il est donc pertinent de faire la définition suivante :

Définition 4.2.1. Soit $f = \sum_{n\geq 1} a_n q^n$ une forme cuspidale propre normalisée de poids k et niveau 1. Soit p un nombre premier et $\mathfrak{p}$ un premier de $\overline{\mathbb{Q}}$ au-dessus de p. La *réduction modulo* $\mathfrak{p}$ *de* f est la forme

$$\overline{f} = \sum_{n\geq 1} \overline{a}_n q^n,$$

où $a_n \equiv \overline{a}_n \pmod{\mathfrak{p}}$. Si f' est une autre forme de poids k' qui possède la même réduction modulo $\mathfrak{p}$ que f, alors on écrira $f \equiv f' \pmod{\mathfrak{p}}$.

Remarque 4.2.2. Les formes f et f' de la définition précédente possèdent la même représentation galoisienne modulo p, d'après le théorème de Deligne. De ce fait, nous avons que

$$\det(\rho_{f,\mathfrak{p}}) \equiv \det(\rho_{f',\mathfrak{p}}) \pmod{p}.$$

Il découle de la remarque 4.1.21 que $\overline{\omega}_p^{k-1} \equiv \overline{\omega}_p^{k'-1}$, où k et k' sont les poids de f et f' respectivement. Par conséquent, $k - 1 \equiv k' - 1 \pmod{p-1}$. Ceci nous donne la proposition suivante :

Proposition 4.2.3. *Soit f et f' deux formes propres cuspidales normalisées de poids k et k' respectivement. Soit p un nombre premier et $\mathfrak{p}$ un premier de $\overline{\mathbb{Q}}$ au-dessus de p. Supposons que $f \equiv f' \pmod{\mathfrak{p}}$. Alors, $k \equiv k' \pmod{p-1}$.*

Définition 4.2.4. Soit $f = \sum_{n=1}^{\infty} a_n q^n$ une forme cuspidale propre normalisée de niveau 1 et p un nombre premier. Nous disons que f satisfait une *congruence diédrale en p* s'il existe un premier $\mathfrak{p}$ de $\mathbb{Q}_f$ au-dessus de p tel que la condition suivante soit satisfaite :

$$a_\ell \equiv 0 \pmod{\mathfrak{p}} \text{ pour tout premier } \ell \text{ tel que } \left(\frac{\ell}{p}\right) = -1.$$

Théorème 4.2.5 (Dummigan-Heim)**.** *Soit k un entier pair tel que $p = 2k - 1$ est premier. Alors, $h(-p) > 1$ si et seulement s'il existe une forme propre cuspidale normalisée f de poids k et niveau 1 qui satisfait une congruence diédrale en p.*

L'idée de la démonstration pour faire intervenir le nombre de classes est d'utiliser un résultat provenant de la théorie globale des corps de classes. Cette théorie a pour but de classifier les extensions abéliennes d'un corps de nombres.

Théorème 4.2.6 (Corps de classes d'Hilbert)**.** *Soit K un corps de nombres tel que son groupe de classes d'idéaux $\mathrm{Cl}(K)$ est non trivial. Alors, il existe une extension maximale abélienne non ramifiée partout E/K telle que*

$$\mathrm{Gal}(E/K) \cong \mathrm{Cl}(K).$$

Remarque 4.2.7. Le corps E est appelé le *corps de classe d'Hilbert*. Une bonne introduction à la théorie des corps de classe est donnée dans [Neu99, Chap. IV, V et VI].

Commençons par montrer la réciproque du théorème 4.2.5.

Proposition 4.2.8. *Soit p un premier congru à 3 modulo 4 et $k = (p+1)/2$. Supposons qu'il existe une forme propre normalisée de poids k et niveau 1 qui admet une congruence diédrale en p. Alors $h(-p) > 1$.*

Démonstration. Soit f une forme telle que dans l'énoncé. Par hypothèse, f est une forme de niveau 1, donc $\overline{\rho}_f$ est non-ramifiée aux premiers qui ne divisent pas p. Montrons que la restriction de $\overline{\rho}_f$ au groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, $K = \mathbb{Q}(\sqrt{-p})$, dénotée $\overline{\rho}_f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}$, est non-ramifiée au premier au dessus de p. Soit $\mathfrak{p}$ le premier au-dessus de p et $I_{\mathfrak{p}}$ son sous-groupe d'inertie associé. Supposons que l'action de $I_{\mathfrak{p}}$ est non triviale. D'après le travail de Serre dans [Ser73a, Section 3.2] et dans [Ser72], l'image de $\overline{\rho}_f(G_{\mathbb{Q}})$ dans $\mathrm{PGL}_2(\overline{\mathbb{F}}_{\mathrm{p}}) := \mathrm{GL}_2(\overline{\mathbb{F}}_p)/\overline{\mathbb{F}}_p^{\times}$ est diédrale et l'action sera induite par un caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{ur}(\sqrt{-p}))$. Donc, l'image $\overline{\rho}_f(I_{\mathfrak{p}})$ sera diédrale. En particulier, celle-ci sera un groupe non abélien. Cependant, la représentation locale $\overline{\rho}_{f,p} = \overline{\rho}_f|_{G_{\mathbb{Q}_p}}$ est irréductible et donc semi-simple. Par conséquent, $\overline{\rho}_{f,p}|_{I_{\mathfrak{p}}}$ sera diagonale, ce qui est impossible, car l'action est non-abélienne. Ceci démontre que $\overline{\rho}_f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}$ est forcément non-ramifiée partout. En particulier, le sous-groupe d'inertie $I_{\mathfrak{p}}$ est inclus dans le noyau, et donc il existe une extension non triviale E/K qui est non-ramifiée partout. Par le théorème 4.2.6, on doit avoir que $h(-p) > 1$. □

Démonstration du théorème 4.2.5. Supposons que $h(-p) > 1$. Ainsi, par le théorème 4.2.6, il existe une extension non ramifiée L de $K := \mathbb{Q}(\sqrt{-p})$ qui n'est pas triviale. Soit

$$\tau : \mathrm{Gal}(E/K) \longrightarrow \overline{\mathbb{F}}_p^{\times}$$

un caractère d'ordre $[E : K]$. Considérons la représentation induite $\rho := \mathrm{Ind}_K^{\mathbb{Q}}\tau$. Puisque K est une extension de degré 2, nous avons que ρ est une représentation modulo p de degré 2 du groupe $\mathrm{Gal}(E/\mathbb{Q})$. Donc, cela nous donne une représentation galoisienne modulo p de degré 2 qui est irréductible, que nous allons également noter ρ :

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p).$$

La représentation ρ est impaire et continue. Donc, par le théorème 4.1.24, nous avons que ρ provient d'une forme propre cuspidale f. Puisque $\mathrm{disc}(K/\mathbb{Q}) = p$, le seul premier ramifié de $K/\mathbb{Q}$ est p. De plus, E/K est non-ramifiée. Donc, par la définition du niveau de ρ, nous obtenons que $N(\rho) = 1$.

Déterminons maintenant le poids de ρ. Soit ρ_p la représentation de $G_{\mathbb{Q}_p}$ provenant de ρ. Par le fait que E/K est non-ramifiée, l'action de $\rho_p|_{I_p}$ sur $\mathrm{Gal}(E/K)$ est triviale. Ensuite,

l'action de $\rho_p|_{I_p}$ sur le groupe d'ordre deux $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q})/\mathrm{Gal}(E/K)$ est non triviale, puisque p est ramifiée dans K. Donc, l'action de $\rho_p|_{I_p}$ sur $\mathrm{Gal}(K/\mathbb{Q})$ est donnée par le caractère quadratique $(\frac{-p}{\cdot})$. Ainsi, la représentation $\rho_p|_{I_p}$ est équivalente à

$$\rho_p|_{I_p} \sim \begin{pmatrix} \mathbf{1} & 0 \\ 0 & (\frac{-p}{\cdot}) \end{pmatrix}, \tag{4.3}$$

où $\mathbf{1}$ est le caractère trivial. Soit $\omega_p : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1}$ le caractère cyclotomique p-adique, alors nous avons que $\mathbf{1} = \omega_p^0$ et, par l'équation (4.1) de l'exemple 4.1.18, $(\frac{-p}{\cdot}) = \omega_p^{(p-1)/2}$. Ceci nous donne $a = 0$ et $b = (p-1)/2$ par la proposition 4.1.28. Donc, le poids de ρ est

$$k(\rho) = 1 + pa + b = \frac{p+1}{2} = k.$$

Montrons maintenant que f satisfait une congruence diédrale en p. Étant donné que

$$a_\ell \equiv \mathrm{Tr}(\rho(\mathrm{Frob}_\ell^{-1})) \pmod{\mathfrak{p}},$$

il suffit de montrer que $\mathrm{Tr}(\rho(\mathrm{Frob}_\ell^{-1})) = 0$. Soit $\mathfrak{p}$ un premier de $\mathbb{Q}_f$ au-dessus de p. Soit ℓ un premier tel que $(\frac{\ell}{p}) = -1$. En particulier, ℓ est inerte dans K par l'exemple 4.1.2. Donc, $K_\ell/\mathbb{Q}_\ell$ est une extension de degré deux. Si $\mathfrak{l}$ est un premier de E au-dessus de ℓ, alors on a que $\mathrm{Gal}(E_\mathfrak{l}/\mathbb{Q}_\ell)$ est cyclique engendré par Frob_ℓ. De cela, il découle que Frob_ℓ n'agit pas trivialement sur K et donc $\mathrm{Frob}_\ell \notin \mathrm{Gal}(E_\mathfrak{l}/K_\ell)$. Par les calculs sur la représentation induite effectués à la section 4.1.7 nous avons que

$$\rho(\mathrm{Frob}_\ell^{-1}) \sim \begin{pmatrix} 0 & \tau(\mathrm{Frob}_\ell^{-1}\sigma) \\ \tau(\sigma\mathrm{Frob}_\ell^{-1}) & 0 \end{pmatrix}.$$

Donc, $\mathrm{Tr}(\rho(\mathrm{Frob}_\ell^{-1})) = 0$.

La réciproque est donnée par la proposition 4.2.8. Une autre démonstration moins conceptuelle consiste tout simplement à calculer tous les cas possibles. Cela peut effectivement être fait, puisque, par le théorème d'Heegner-Stark, il existe seulement un nombre fini de premiers p tels que $h(-p) = 1$. Nous référons le lecteur au chapitre 5 pour les exemples de calculs numériques. □

4.3 Congruences diédrales pour des poids supérieurs

Dans cette section, notre but est de généraliser le deuxième théorème de Dummigan et Heim en lien avec le nombre de classes d'un corps quadratique imaginaire. Voici l'énoncé de ce théorème :

Théorème 4.3.1. *Soit k un entier tel que $p = 2k - 1$ est premier. Soit k' un entier qui est congru à k modulo $p - 1$. Alors, $h(-p) > 1$ si et seulement s'il existe une forme propre cuspidale normalisée f de poids k' et niveau 1 qui satisfait une congruence diédrale en p.*

Nous allons donner deux démonstrations de l'implication directe de ce théorème, c'est-à-dire de l'affirmation que $h(-p) > 1$ implique qu'il existe une forme propre cuspidale normalisée $f \in \mathcal{S}_{k'}(\Gamma(1))$, où $k' \equiv k \pmod{p-1}$, qui satisfait une congruence diédrale en p. La première consiste à utiliser un argument de congruence sur les séries d'Eisenstein de poids $p-1$. La deuxième démonstration, qui est un peu plus sophistiquée, consiste à appliquer la théorie des formes modulaires Λ-adiques à la forme qui a été construite dans la démonstration du théorème 4.2.5.

Pour ce qui est de la réciproque, celle-ci découle de la proposition 4.2.3. En effet, soit f une forme propre cuspidale normalisée de poids k' et niveau 1 qui satisfait une congruence diédrale en p. Ainsi, la réduction modulo p de f définie une forme de poids k modulo $p-1$ par la proposition 4.2.3. Donc, cette nouvelle forme est de poids $k = (p+1)/2$ et satisfait une congruence diédrale par hypothèse. On en déduit que $h(-p) > 1$ par le théorème 4.2.5.

4.3.1 Séries d'Eisenstein de poids $p-1$

À la section 2.4, nous avons défini les séries d'Eisentein de poids $k \geq 4$. Rappelons que ces dernières possèdent la q-expansion suivante

$$E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Si $p \geq 5$ est un premier, alors $v_p(B_{p-1}) = -1$ par le théorème de Von-Staudt-Clausen. Donc,

$$v_p\Big(\frac{p-1}{B_{p-1}}\Big) = v_p(p-1) + 1 \geq 1.$$

De cela, il découle que $E_{p-1} \equiv 1 \pmod{p}$. Cette idée nous permettra de faire varier le poids d'une forme modulaire sans faire varier les congruences sur les coefficients.

Proposition 4.3.2. *Soit f une forme propre normalisée de poids k. Soit $p \geq 5$ un premier et $\mathfrak{p}$ un premier de $\mathbb{Q}_f$ au dessus de p. Alors, pour tout entier $m \geq 0$, $fE_{m(p-1)}$ est une forme de poids $k' = k + m(p-1)$ qui est congrue à f modulo $\mathfrak{p}$.*

Démonstration. Tout d'abord, la forme $fE_{m(p-1)}$ est bien de poids $k' = k + m(p-1)$, puisque la multiplication de deux formes modulaires de poids k_1 et k_2 donne une forme de poids $k_1 + k_2$. Ensuite, par le théorème de Von-Staudt-Clausen, nous avons que

$$v_p\Big(\frac{m(p-1)}{B_{m(p-1)}}\Big) = v_p(m(p-1)) + 1 \geq 1.$$

Ainsi, on obtient que $E_{m(p-1)} \equiv 1 \pmod{p}$ et donc $f \equiv fE_{m(p-1)} \pmod{\mathfrak{p}}$. □

L'implication directe du théorème 4.3.1 découle de la dernière proposition. Soit $p \equiv 3 \pmod{4}$ tel que $h(-p) > 1$ et $k = (p+1)/2$. Alors, par le théorème 4.2.5, il existe une forme de poids k qui satisfait une congruence diédrale en p. Ainsi, pour tout $m \geq 0$, la forme $fE_{m(p-1)}$ est de poids $k + m(p-1)$ et satisfait une congruence diédrale en p tel que désiré.

4.3.2 Formes modulaires Λ-adiques

La théorie des formes modulaires Λ-adique découle de l'étude des congruences sur les séries d'Eisenstein par Serre et de sa définition des formes modulaires p-adique [Ser73b]. Brièvement, une forme modulaire Λ-adique peut être vue comme une famille de formes modulaires satisfaisant des propriétés de congruences. Fixons p un nombre premier impair et $F/\mathbb{Q}_p$ une extension finie avec $\mathcal{O}_F$ comme anneau de valuation. La théorie qui suit est basée sur le chapitre 7 de [Hid93].

Définition 4.3.3. Soit $\psi = \omega_p^a$ où $a \geq 1$ et $M \geq 1$ un entier. Une famille *analytique p-adique* est un ensemble infini de formes modulaires $\{f_k\}_{k \geq M}$ satisfaisant les trois propriétés suivantes :

1. $f_k \in \mathcal{M}_k(\Gamma_0(p), \psi\omega_p^{-k})$;
2. $a_n(f_k) \in \overline{\mathbb{Q}}$ pour tout n ;
3. pour tout $n \geq 0$, il existe une série formelle $A_n(X) \in \mathcal{O}_F[[X]]$ telle que

$$a_n(f_k) = A_n((1+p)^k - 1)$$

pour tout $k \geq M$.

Définition 4.3.4. Soit $\Lambda := \mathcal{O}_F[[X]]$ et soit $\psi = \omega_p^a$ où $a \geq 1$. Une *forme modulaire Λ-adique*, aussi appelée *famille d'Hida*, est une série formelle

$$f_\infty(X, q) = \sum_{n=0}^{\infty} A_n(X) q^n \in \Lambda[[q]],$$

telle que l'évaluation $f_k := f_\infty((1+p)^k - 1, q)$ donne la q-expansion d'une forme modulaire dans $\mathcal{M}_k(\Gamma_0(p), \psi\omega_p^{-k})$. La forme modulaire f_k est appelée la *spécialisation de f_∞ en k*.

Remarque 4.3.5. Soit $f_\infty = \sum_{n=0}^{\infty} A_n(X) q^n$ une forme modulaire Λ-adique avec $A_n(X) = \sum_{n=0}^{\infty} \lambda_n X^n$. Alors, pour tout k, nous avons que

$$\begin{aligned} A_n((1+p)^k - 1) &= \sum_{n=0}^{\infty} \lambda_n ((1+p)^k - 1)^n \\ &\equiv \lambda_0 \pmod{p}. \end{aligned}$$

Par conséquent, chaque spécialisation de la famille d'Hida sont deux à deux congruentes modulo p. Cela veut donc dire que si f_k et $f_{k'}$ sont deux spécialisations, alors les deux formes possèdent la même représentation galoisienne modulo p.

Exemple 4.3.6. Soit $k \geq 2$ un entier pair. La série d'Eisenstein

$$G_k(\tau) := -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

nous donne un exemple de famille analytique p-adique. Plus précisément, la série d'Eisenstein modifiée suivante

$$G_k^{(p)}(\tau) := G_k(\tau) - p^{k-1}G_k(p\tau),$$

est la spécialisation en k d'une forme modulaire Λ-adique

$$G_\infty = \sum_{n=0}^{\infty} A_n(X)q^n \in \Lambda[[q]], \text{ où } \Lambda = \mathbb{Z}_p[[X]].$$

Pour montrer cette affirmation, il faut interpoler p-adiquement les coefficients de la q-expansion de $G_k^{(p)}$, qui sont donnés par

$$G_k^{(p)}(\tau) = \frac{\zeta^{(p)}(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}^{(p)}(n)q^n,$$

où

$$\zeta^{(p)}(1-k) := (1-p^{k-1})\zeta(1-k), \qquad \sigma_{k-1}^{(p)}(n) := \sum_{\substack{0<d|n \\ \text{pgcd(d,p)=1}}} d^{k-1}.$$

Par exemple, pour le terme constant, on doit utiliser la version p-adique de la fonction ζ de Riemann, qui a été construite par Kubota et Leopoldt [KL64]. Les détails de la construction de la série d'Eisenstein Λ-adique G_∞ sont donnés dans le livre de Hida [Hid93, Proposition 1, page 198].

Un théorème important qui est dû à Hida stipule que, si f est une forme propre de poids k et de niveau p qui satisfait la propriété d'être *p-ordinaire*, alors f est la spécialisation d'une unique famille d'Hida en k ([Hid86b] et [Hid86a]). Pour définir la notion d'être p-ordinaire, nous aurons besoin d'introduire deux nouveaux opérateurs.

Définition 4.3.7. Soit $f = \sum_{n=0}^{\infty} a_n q^n$ la q-expansion d'une forme modulaire de niveau N. Alors, on définit les opérateurs U_p et V_p par

$$U_p f := \sum_{n=0}^{\infty} a_{np} q^n, \quad V_p f := \sum_{n=0}^{\infty} a_n q^{np}.$$

Proposition 4.3.8. *Si T_p est le p-ième opérateur de Hecke et $f \in \mathcal{M}_k(\Gamma_0(N))$, alors*

$$T_p f = \begin{cases} U_p f, & \text{si } p \mid N; \\ U_p f + p^{k-1} V_p f & \text{si } p \nmid N. \end{cases}$$

De plus, si $p \nmid N$, alors U_p envoie une forme de niveau N vers une forme de niveau pN.

Rappelons nous que nous avons fixé un plongement $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Donc, les coefficients d'une forme cuspidale propre normalisée f peuvent être vus comme des éléments de $\mathcal{O}_{f,\mathfrak{p}} := \mathcal{O}_{\mathbb{Q}_{f,\mathfrak{p}}}$, où $\mathbb{Q}_{f,\mathfrak{p}}$ la complétion de $\mathbb{Q}_f$ par rapport à un premier $\mathfrak{p}$ au-dessus de p.

Définition 4.3.9. Soit $f = \sum_{n=0}^{\infty} a_n q^n$ une forme propre normalisée de poids k et de niveau N et p un premier. Soit $\mathfrak{p}$ un premier de $\mathbb{Q}_f$ au-dessus de p. Alors f est dite $\mathfrak{p}$-*ordinaire* si $U_p(f) = a_p f$ où a_p est une unité $\mathfrak{p}$-adique, c'est-à-dire $a_p \in (\mathcal{O}_{f,\mathfrak{p}})^\times$. On dénote par $\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(N))$ et $\mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(N))$ les espaces engendrés par les formes $\mathfrak{p}$-ordinaires.

Soit α_p et β_p les paramètres de Satake d'une forme propre $f \in \mathcal{M}_k(\Gamma_0(N))$. Supposons que $\mathfrak{p} \nmid a_p(f)$. Rappelons-nous que $\alpha_p + \beta_p = a_p(f)$ et $\alpha_p \beta_p = p^{k-1}$. Ainsi, on peut supposer sans perte de généralité que α_p est une unité p-adique et que $\mathfrak{p} \mid \beta_p$. Ceci nous amène donc à définir la p-*stabilisation* de f comme étant la forme modulaire suivante

$$f^{(p)}(\tau) := f(\tau) - \beta_p f(p\tau) = f(\tau) - \beta_p V_p f.$$

Par conséquent, $f^{(p)}$ sera une forme de poids k pour $\Gamma_0(pN)$ qui est $\mathfrak{p}$-ordinaire.

Théorème 4.3.10 (Hida)**.** *Soit $k \geq 2$ un entier et p un premier. Soit $f \in \mathcal{S}_k(\Gamma_0(pN))$ une forme propre normalisée qui est $\mathfrak{p}$-ordinaire. Alors il existe une unique forme modulaire Λ-adique f_∞ qui se spécialise à f en k.*

Pour démontrer l'implication directe du théorème 4.3.1, nous allons montrer que la forme cuspidale produite dans la démonstration du théorème de Dummigan et Heim sur les congruences diédrales est $\mathfrak{p}$-ordinaire. Pour ce faire, nous allons appliquer un théorème qui est dû à Fontaine, dont la démonstration peut être trouvée dans [Edi92, Theorem 2.6]. Voici l'énoncé :

Proposition 4.3.11. *Soit p un premier et f une forme propre cuspidale de poids k, de niveau N et de caractère ε avec $2 \leq k \leq p-1$. Supposons que $a_p(f) \equiv 0 \pmod{\mathfrak{p}}$. Alors $\rho_{f,\mathfrak{p}}$ est irréductible et*

$$\rho_{f,\mathfrak{p}}|_{I_p} = \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix}$$

où ψ et ψ' sont les caractères fondamentaux de niveau 2.

Proposition 4.3.12. *Soit k un entier tel que $p = 2k-1$ est premier. Si $h(-p) > 1$, alors, pour tout entier pair positif k', il existe une forme propre cuspidale normalisée $f \in \mathcal{S}_{k'}(\Gamma_0(p), \omega_p^{k-k'})$ qui satisfait une congruence diédrale en p.*

Démonstration. Supposons que $h(-p) > 1$. Par le théorème 4.2.5, nous savons qu'il existe une forme modulaire propre et normalisée f de poids k et de niveau 1 qui satisfait une congruence diédrale en p. Notre but est de montrer que f provient d'une famille d'Hida.

Tout d'abord, le p-ième coefficient de f n'est pas divisible par p. Cela découle de la ligne (4.3). En effet, nous avons vu que $\rho_{f,p}|_{I_p}$ est donné par deux caractères de niveau 1. Cependant, le théorème 4.3.11 nous dit que si $p \mid a_p(f)$, alors $\rho_{p,f}|_{I_p}$ serait donnée par deux caractères de niveau deux.

Ensuite, pour pouvoir utiliser le théorème d'Hida, nous devons avoir une forme de niveau divisible par p qui est une forme propre pour l'opérateur U_p. On pose alors $f_k := f^{(p)}$. Par le théorème 4.3.10, la forme f_k est la spécialisation d'une unique famille d'Hida f_∞. La remarque 4.3.5 nous dit que chaque spécialisation

$$f_{k'} := f_\infty((1+p)^{k'} - 1, q) \in \mathcal{S}_k(\Gamma_0(p), \omega_p^{k-k'}),$$

sont deux à deux congrues modulo p. Cela veut donc dire qu'elles satisfont toutes les propriétés d'être diédrale en p. □

Dans la proposition précédente, nous avons construit une forme de poids k', niveau p et caractère $\omega_p^{k-k'}$ qui satisfait une congruence diédrale en p. Si l'on suppose que $k' \equiv k \pmod{p-1}$, alors le caractère devient trivial :

$$\mathcal{S}_k(\Gamma_0(p), \omega_p^{k-k'}) = \mathcal{S}_k(\Gamma_0(p)).$$

Ensuite, pour terminer la démonstration de l'implication directe de 4.3.1, on utilise ce lemme :

Lemme 4.3.13. *Soit p un premier, χ un caractère de Dirichlet de conducteur m tel que $p \nmid m$. Si $p \mid N$ et $k \geq 3$, alors nous avons l'isomorphisme de $\mathbb{C}$-espace vectoriel suivant :*

$$\mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(N), \chi) \cong \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^{-1}N), \chi).$$

Démonstration. Soit $f \in \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(N), \chi)$ une forme telle que

$$f \notin \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^{-1}N), \chi).$$

Le p-ième coefficient de f satisfait

$$N_{\mathbb{Q}_f/\mathbb{Q}}(a_p(f)) = p^{(k-2)}.$$

Ce fait est démontré dans [Miy89, Theorem 4.6.17]. Par conséquent, si $k \geq 3$, alors f ne sera pas p-ordinaire. □

Corollaire 4.3.14. *Soit k un entier tel que $p = 2k-1$ est premier et k' un entier congru à k modulo $p-1$. Si $h(-p) > 1$, alors il existe une forme propre cuspidale normalisée $f \in \mathcal{S}_{k'}(\Gamma(1))$ qui satisfait une congruence diédrale en p.*

Démonstration. Par le lemme 4.3.13, on a que $\mathcal{S}_{k'}^{\mathrm{ord}}(\Gamma_0(p)) \cong \mathcal{S}_{k'}^{\mathrm{ord}}(\Gamma(1))$. En particulier, la forme $f_{k'} \in \mathcal{S}_{k'}^{\mathrm{ord}}(\Gamma_0(p))$ définie dans la proposition 4.3.12 correspondra, sous l'isomorphisme mentionné plus haut, à une forme de niveau 1 qui satisfait une congruence diédrale en p. □

4.3.3 Congruences dans des espaces de formes de niveau supérieur

L'idée derrière la démonstration du théorème 4.3.12 provient de la preuve d'un résultat se trouvant dans un article de Brown et Ghate [BG02, Theorem 2.11]. Leur résultat est en fait une généralisation d'un théorème initialement démontré par Hida [Hid98, Theorem 1].

Théorème 4.3.15 (Brown et Ghate). *Soit D un entier tel que $D \equiv 1 \pmod 4$ et $D = D_1 D_2$ avec $D_1 > 0$ et $D_1 \neq 1$. Soit p un premier tel que $\operatorname{pgcd}(p, 2D) = 1$. Soit $k \geq 2$ un entier tel que $(p-1) \nmid (k-1)$ et supposons que $p \neq 3$ si $k = 2$. Supposons également les trois hypothèses suivantes :*

(H1) p se décompose dans le corps quadratique réel $\mathbb{Q}(\sqrt{D_1})$;

(H2) Pour tout premier $q \mid D_2$, q se décompose dans $\mathbb{Q}(\sqrt{D_1})$;

(H3) $p \mid N_{\mathbb{Q}(\sqrt{D_1})/\mathbb{Q}}(\varepsilon_+^{k-1} - (-1)^a)$,

où ε_+ est une unité fondamentale de $\mathbb{Q}(\sqrt{D_1})$ telle que $\sigma(\varepsilon_+) > 0$ pour tout plongement $\sigma : \mathbb{Q}(\sqrt{D_1}) \hookrightarrow \mathbb{R}$ et l'entier a est le nombre de premiers qui divisent D_2 et qui satisfont une certaine condition technique énoncée dans [BG02, 2.10]. Alors, pour tout premier $\mathfrak{p}$ de $\overline{\mathbb{Q}}$ au-dessus de p, il existe une forme propre normalisée $f \in \mathcal{S}_k(|D|, (\frac{D}{\cdot}))$ telle que f est $\mathfrak{p}$-ordinaire, la représentation galoisienne modulo $\mathfrak{p}$ associée à f est irréductible et f satisfait la congruence suivante

$$f \equiv f \otimes \left(\frac{D}{\cdot}\right) \pmod{\mathfrak{p}}. \tag{4.4}$$

La réciproque de ce long théorème est également vraie [BG02, Theorem 2.1]. On peut voir le théorème de Dummigan et Heim comme un résultat similaire au théorème 4.3.15. En effet, soit p un premier et $\mathfrak{p}$ un premier au-dessus de p. Soit f une forme modulaire. Au sens de Dummigan et Heim, si $p \equiv 3 \pmod 4$, la condition d'être diédrale en p est

$$a_\ell(f) \equiv 0 \pmod{\mathfrak{p}}, \text{ pour tout premier } \ell \text{ tel que } \left(\frac{\ell}{p}\right) = -1. \tag{DH}$$

Pour ce qui est du théorème 4.3.15, si $D \equiv 1 \pmod 4$ et $\operatorname{pgcd}(p, 2D) = 1$, la congruence 4.4 nous dit que

$$a_\ell(f) \equiv 0 \pmod{\mathfrak{p}}, \text{ pour tout premier } \ell \text{ tel que } \left(\frac{D}{\ell}\right) = -1. \tag{BG}$$

Ainsi, on en déduit que les deux congruences sont très similaires. Par conséquent, le théorème de Brown et Ghate peut être vu comme un analogue du théorème de Dummigan et Heim, mais pour les formes de niveau $|D|$ et caractères $(\frac{D}{\cdot})$. Si $f \in \mathcal{S}_k(\Gamma_0(|D|), (\frac{D}{\cdot}))$ satisfait la condition (BG), nous dirons également que f satisfait une *congruence diédrale en p*.

Exemple 4.3.16. Considérons l'espace $\mathcal{S}_2(\Gamma_0(53), (\frac{53}{\cdot}))$. Alors, $D = D_1 = 53$ et donc $a = 0$. le premier $p = 7$ se décompose dans le corps $\mathbb{Q}(\sqrt{53})$, car $(53/7) = 1$. On peut également vérifier que nous avons la décomposition en idéaux premiers suivants

$$(7) = \left(\frac{-5 - \sqrt{53}}{2}\right)\left(\frac{5 - \sqrt{53}}{2}\right).$$

Ensuite, une unité fondamentale totalement positive de $\mathbb{Q}(\sqrt{53})$ est donnée par

$$\varepsilon_+ = \frac{51 - 7\sqrt{53}}{2}.$$

Ainsi, $N_{\mathbb{Q}(\sqrt{53})/\mathbb{Q}}(\varepsilon_+ - 1) = 7$. Par conséquent, pour tout premier $\mathfrak{p}$ de $\overline{\mathbb{Q}}$, il existe une forme propre normalisée $f \in \mathcal{S}_2(\Gamma_0(53), (\frac{53}{\cdot}))$ telle que f est $\mathfrak{p}$-ordinaire, la représentation galoisienne modulo $\mathfrak{p}$ associée à f est irréductible et f satisfait une congruence diédrale en $\mathfrak{p}$.

Pour conclure, la démonstration de Brown et Ghate [BG02, Theorem 2.11] utilise une autre méthode que celle de Dummigan et Heim pour produire une forme qui satisfait la congruence (4.4). Rappelons que la démonstration de Dummigan et Heim consistait à construire une représentation galoisienne modulo p à partir de la représentation induite d'un caractère d'un groupe de Galois et d'utiliser le théorème de Khare et Winterberger. Pour ce qui est de la démonstration de Brown et Ghate, on construit un *caractère de Hecke* et on considère la *série thêta* qui lui est associée. De manière heuristique, un caractère de Hecke peut être vu comme une généralisation des caractères de Dirichlet. Pour un certain type de caractère de Hecke, on peut définir une série thêta qui sera en fait une forme cuspidale. Les détails de la construction de cette série thêta sont donnés dans le livre de Miyake [Miy89, Théorèmes 4.8.2 et 4.8.3]. Ainsi, il aurait été possible de construire explicitement la forme cuspidale en utilisant cette méthode pour démontrer le théorème 4.2.5.

Chapitre 5

Calculs numériques avec PARI/GP

Dans ce chapitre, nous présenterons des exemples de calculs numériques en lien avec les deux théorèmes démontrés. Les calculs ont été effectués à l'aide du logiciel de calcul formel PARI/GP [PAR18]. Ce logiciel est en fait une union de deux composantes distinctes : PARI et GP. La composante PARI est une bibliothèque écrite en C, un langage de programmation, alors que GP est le langage de script permettant l'usage des fonctions de PARI. L'utilisation de ses deux composantes se fait à partir d'un interpréteur en ligne de commande appelé gp.

L'installation de PARI/GP se fait à partir du site internet :

`https://pari.math.u-bordeaux.fr/`.

Une fois le logiciel installé, alors il suffit d'exécuter le fichier `gp.exe`, qui se trouvera généralement dans le dossier d'installation. Cela aura pour effet de lancer l'interpréteur en ligne de commande gp. Il est conseillé d'utiliser la fonctionnalité d'aide du logiciel et de lire le guide d'introduction. Ces ressources sont très bien détaillées. Dans ce qui suivra, des exemples de calculs sont exposés pour permettre au lecteur de se familiariser avec le logiciel et de reproduire les démarches. L'ensemble des fonctions qui sont présentées plus bas sont disponibles à l'adresse suivante :

`https://github.com/DavidAyotte/Sym2-Dihedral.git`.

5.1 p-valuation de la trace et des nombres de Bernoulli

Dans cette section, nous allons nous intéresser à calculer explicitement la trace de la fonction L carrée symétrique qui est définie par :

$$\mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2)) = \sum_{f \in \mathcal{B}_k} L^*(\mathrm{Sym}^2(f), 2k-2)_{\mathrm{alg}}.$$

où $\mathcal{B}_k$ est la base de formes cuspidales propres normalisées de poids k et niveau 1. Considérant que la valeur spéciale $2k-2$ est fixée pour le calcul de la trace, nous écrirons $\mathrm{Tr}(k) := \mathrm{Tr}_k(L(\mathrm{Sym}^2, 2k-2))$.

À la section 3.2, nous avons vu qu'il existe une formule relativement simple pour calculer cette trace :

$$\mathrm{Tr}(k) = c_k\Big(B_{k-1,(\frac{-4}{\cdot})} + 2B_{k-1,(\frac{-3}{\cdot})} + B_{2k-2}(1+\frac{k}{B_k})\Big), \quad c_k = 2^{2k-1}\frac{(\frac{k}{2}-1)!}{(k-1)!}.$$

Le problème du calcul de la trace est donc réduit à celui du calcul des nombres de Bernoulli. Dans PARI/GP, le k-ième nombre de Bernoulli est donné par la fonction `bernfrac(k)` et le k-ième polynôme de Bernoulli est donné par `bernpol(k)`. Il est à noter que PARI/GP possède aussi la fonction `bernreal(k)`. Cette dernière retourne l'expansion décimale de B_k, alors que `bernfrac(k)` retourne B_k sous sa forme rationnelle. Dans PARI/GP, il n'y a pas de fonction pour calculer directement les nombres de Bernoulli généralisés associés à un caractère de Dirichlet χ. Cependant, le calcul de peut être fait à l'aide de la formule suivante

$$B_{k,\chi} = f^{k-1}\sum_{a=1}^{f}\chi(a)B_k(\frac{a}{f}),$$

où f est le conducteur de χ. Pour calculer le symbole de Kronecker $(\frac{D}{x})$, on écrit `kronecker(D,x)`. Voici la fonction qui a été écrite pour calculer la trace :

```
traceLsym2(k) = {
  if (k%2 != 0, error("k doit etre pair"));
  ck = 2^(2*k-3)*(k/2 - 1)!/(k-1)!;
  bernoullipol = bernpol(k-1); \\polynome de Bernoulli

  \\Nombre de Bernoulli generalises
  berngen4 = 4^(k-2)*sum(i = 1, 4, kronecker(-4, i)*subst(bernoullipol, x, i/4));
  berngen3 = 3^(k-2)*sum(i = 1, 3, kronecker(-3, i)*subst(bernoullipol, x, i/3));

  return(ck*(berngen4 + 2*berngen3 + bernfrac(2*k-2)*(1+k/bernfrac(k))));
}
```

Exemple 5.1.1. Dans la session PARI/GP suivante, on calcule la quantité Tr(12) et ensuite on montre qu'il y a un seul facteur de $p = 23$ au dénominateur.

```
gp > \r "trace.gp" \\importation du script contenant la fonction traceLsym2(k)
gp > tr = traceLsym2(12)

%1 = 1761607680/15893

gp > valuation(tr, 23)

%2 = -1
```

Étudions maintenant la conjecture 3.3.11 qui a été énoncée à la section 3.3. Cette conjecture est à propos de la p-valuation de la trace et elle stipule que

$$v_p(\mathrm{Tr}(k')) = \begin{cases} v_p(c_{k'}) + 1 & \text{si } p \mid 2m+1; \\ v_p(c_{k'}) & \text{sinon,} \end{cases}$$

où $p = 43, 67$ ou 163, $k = (p+1)/2$ et $k' = k + m(p-1)$. Par exemple, si $m = 21$, alors $2m+1 = 43$ et $k' = 904$. On peut vérifier à l'aide de la fonction `traceLsym2` que

$$v_{43}(\mathrm{Tr}(904)) = -10 \quad \text{et} \quad v_{43}(c_{904}) = -11.$$

Tel que mentionné à la fin de la section 3.3 du chapitre 3, la p-valuation du facteur $c_{k'}$ est facile à calculer, étant donné qu'il est défini par un quotient de factorielles. Toutefois, remarquons que la conjecture est indépendante de $c_{k'}$. En effet, si on définit

$$b(k') := B_{k'-1,\chi_{-4}} + 2B_{k'-1,\chi_{-3}} + B_{2k'-2}(1 + \frac{k'}{B_{k'}}),$$

alors la conjecture est équivalente à

$$v_p(b(k')) = \begin{cases} 1 & \text{si } p \mid 2m+1; \\ 0 & \text{sinon.} \end{cases}$$

Ce phénomène a été vérifié pour toutes les valeurs de m inférieures ou égales à 300. Les valeurs de m et de p pour lesquelles $v_p(b(k')) = 1$ ont été compilées dans le tableau 5.1. les valeurs de m et de p qui n'apparaissent pas dans le tableau sont celles pour lesquelles $v_p(b(k')) = 0$.

m	p	$2m+1$
21	43	43
33	67	67
64	43	$3 \cdot 43$
81	163	163
100	67	$3 \cdot 67$
107	43	$5 \cdot 43$
150	43	$7 \cdot 43$
167	67	$5 \cdot 67$
193	43	$9 \cdot 43$
234	67	$7 \cdot 67$
236	43	$11 \cdot 43$
244	163	$3 \cdot 163$
279	43	$13 \cdot 43$

Tableau 5.1: vérifications numériques de la conjecture 3.3.11

Ce qui complique le calcul de la p-valuation de la trace pour un ordinateur, est que, contrairement aux dénominateurs, la structure des numérateurs des nombres de Bernoulli est toujours inconnue. De plus, les numérateurs deviennent relativement énormes. Par exemple, pour

$m = 300$ et $p = 167$ nous devons calculer le nombre de Bernoulli suivant

$$B_{49884} = -\frac{17050\ldots50813}{68094390}.$$

Dans cet exemple, le numérateur de B_{49884} contient 172 884 chiffres et le dénominateur correspond au produit des premiers p tels que $p - 1 \mid 49884$ (par le théorème de Von-Staudt et Clausen). Ainsi, la grandeur des nombres des Bernoulli explique en partie la difficulté à calculer leur p-valuation.

À ce jour, l'algorithme de PARI/GP pour calculer le k-ième nombre de Bernoulli est basé sur la formule suivante

$$B_k = (-1)^{1-k/2}\frac{2 \cdot k!}{(2\pi)^k}\zeta(k).$$

C'est une méthode relativement rapide et efficace. Une description détaillée de l'algorithme est présentée dans [Ste07, Algorithm 2.45]. Cependant, cette méthode, contrairement à la p-valuation de la factorielle à l'aide de la formule de Legendre, n'offre pas de moyen pour calculer $v_p(B_k)$ rapidement. Ainsi, une étude plus approfondie de la p-valuation des nombres de Bernoulli permettrait de mieux comprendre la p-valuation de la trace. Cependant, cette étude pourrait s'avérer être difficile, étant donné que les nombres de Bernoulli possèdent plusieurs liens avec le nombre de classes d'un corps de nombre. Donc, comprendre les nombres de Bernoulli revient d'une certaine façon à comprendre le nombre de classes, qui est lui-même un objet encore mystérieux.

Les nombres de Bernoulli et le nombre de classes

L'intérêt de mieux comprendre la structure des nombres de Bernoulli ne vient pas que de la conjecture 3.3.11. En effet, à la section 3.3, nous avons énoncé que si $p \equiv 3 \pmod 4$, alors

$$h(-p) \equiv -2B_{\frac{p+1}{2}} \pmod p.$$

Il existe aussi une congruence similaire pour les premiers $p \equiv 1 \pmod 4$.

Proposition 5.1.2. *Soit p un premier congru à 1 modulo 4 et $\varepsilon = \frac{t+u\sqrt{p}}{2}$ une unité qui engendre le groupe $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]^\times/\{\pm 1\}$. Alors,*

$$\frac{u}{t}h(p) \equiv B_{\frac{p-1}{2}} \pmod p.$$

Cette congruence a été démontrée par Ankeny, Artin et Chowla en 1952 [AAC52, Theorem IV]. Les trois auteurs ont également énoncé une conjecture qu'ils ont vérifiée numériquement pour plusieurs valeurs.

Conjecture 5.1.3 (AAC). $u \not\equiv 0 \pmod p$.

Par la proposition 5.1.2, la conjecture AAC est équivalente au fait que $p \nmid B_{\frac{p-1}{2}}$. Par conséquent, une meilleure connaissance des propriétés de divisibilité des nombres de Bernoulli pourrait amener à la résolution de la conjecture 5.1.3.

Il y a également une autre conjecture en lien avec la p-divisibilité des nombres de Bernoulli.

Définition 5.1.4. Un premier p est dit *régulier* si p ne divise par le numérateur des nombres de Bernoulli suivant

$$B_2, B_4, \ldots, B_{p-3}.$$

Sinon, p est dit *irrégulier*.

Il est conjecturé qu'il existe un nombre infini de premiers réguliers. Pour les premiers irréguliers, il est connu qu'il y en a une infinité (voir [Was97, Theorem 5.17]). Un premier régulier p est en fait relié avec le nombre de classes du p-ième corps cyclotomique $\mathbb{Q}(\zeta_p)$.

Proposition 5.1.5 (Théorème 5.16 de [Was97])**.** *Un premier p est régulier si et seulement si $p \nmid h(\mathbb{Q}(\zeta_p))$.*

Par ce qui précède, on peut voir les nombres de Bernoulli comme un outil qui nous permettrait de mieux comprendre le nombre de classes pour certains corps de nombres.

5.2 Exemples de congruences diédrales

Depuis le mois de mai 2018, un module sur les formes modulaires a été intégré au logiciel PARI/GP. Ce module possède une multitude de fonctionnalités permettant de réaliser des calculs avec les formes modulaires. Par exemple, pour initialiser l'espace des formes cuspidales $\mathcal{S}_k(\Gamma_0(N))$, alors on écrit `mfinit([N, k], 1)`.

Exemple 5.2.1.

```
gp > S = mfinit([23, 24],1);
gp > mfdim(S) \\calcul de la dimension

%1 = 45

gp > B = mfbasis(S); f = B[5]; \\calcul d'une base de S
gp > mfcoefs(f, 6) \\affichage des 6 premiers coefficients de f

%2 = [0, 41, -4096, -346108, 159383552, -49902092]
```

Exemple 5.2.2. Dans cet exemple, nous allons montrer que si $p = 43$ et $k = (p+1)/2 = 22$, alors l'espace $\mathcal{S}_{22}(\Gamma(1))$ n'admet pas de forme satisfaisant une congruence diédrale en p, tel que prévu par le théorème 4.2.5. Autrement dit, pour chaque forme propre normalisée f, il faut exhiber un premier ℓ tel que $(\frac{\ell}{53}) = -1$, mais $53 \nmid a_\ell(f)$. Voici les commandes PARI/GP que l'on peut exécuter pour y parvenir :

```
gp > S = mfinit([1, 22], 1); \\initialisation de l'espace des formes cuspidales
gp > mfdim(S)

%1 = 1

gp > B = mfeigenbasis(S); f = B[1];
gp > mfcoefs(f, 10)

%2 = [0, 1, -288, -128844, -2014208, 21640950, 37107072, -768078808, 1184071680,
    6140423133, -6232593600]

gp > kronecker(2,43)

%3 = -1

gp > mfcoef(f, 2) % 43 \\on montre que 43 ne divise pas a_2(f)

%4 = 13
```

La même suite de calculs peut être réalisée pour les cas $p = 67$ et $p = 163$. Toutefois, il est à noter que la fonction `mfeigenbasis` ne retourne pas exactement tous les éléments de la base de formes propres normalisée. En effet, pour l'espace $\mathcal{S}_{34}(\Gamma(1))$ qui est de dimension 2, la fonction retourne uniquement la forme propre suivante

$$f = q + (-144\alpha - 60768)q^2 + (44928\alpha + 18937476)q^3 + \cdots$$

où α est une racine du polynôme $X^2 - X - 589050$. Pour trouver la deuxième forme propre normalisée, il faut remplacer α par sa racine conjuguée α^σ :

$$f^\sigma = q + (-144\alpha^\sigma - 60768)q^2 + (44928\alpha^\sigma + 18937476)q^3 + \cdots .$$

Par conséquent, $\{f, f^\sigma\}$ sera la base de formes propres normalisée de $\mathcal{S}_{32}(\Gamma(1))$.

Dans les exemples précédents, nous avons porté notre intérêt à la vérification qu'une forme modulaire n'est pas diédrale en p. Il est également possible de vérifier expérimentalement qu'une forme satisfait une congruence diédrale en p. Toutefois, cette vérification n'est pas mathématiquement rigoureuse, puisqu'elle consiste à vérifier que la condition d'être diédrale est vraie pour un nombre fini de coefficients. De ce fait, il faut spécifier un seuil maximal de coefficients lors de calculs numériques. La fonction qui a été écrite pour vérifier la condition d'être diédrale en p est la suivante :

```
mfisdihedral(f, nf, p, primeover, {D = 1}, {maxcoefs=150}) = {
        if(D == 1, D = p; chiD(q) = kronecker(q, D), chiD(q) = kronecker(D, q));
        forprime(q = 1, maxcoefs,
                if (chiD(q) == -1,
                        cf = mfcoef(f, q);
                        if (nfeltreduce(nf, cf, primeover) != 0, return(0));
                );
        );
        return(1);
};
```

Voici une description des paramètres de cette fonction :

- `f` : une forme cuspidale propre normalisée ;
- `nf` : un corps de nombres ;
- `p` : un nombre premier rationnel ;
- `primeover` : un premier de `nf` au dessus de `p` ;
- `D` : un entier congru à 0 ou 1 (mod 4). Par défaut, ce paramètre est initialisé à 1. Dans ce cas, la fonction vérifie si la forme est diédrale en `p` au sens de Dummigan et Heim (condition DH). Si $\texttt{D} > 1$, alors la fonction vérifie si `f` satisfait une congruence diédrale en `p` au sens de Brown et Ghate (condition BG) pour le caractère de Dirichlet $(\frac{\texttt{D}}{\cdot})$.
- `maxcoefs` : nombre maximal de coefficients à vérifier la congruence. Ce paramamètre est initialisé par défaut à 150.

Exemple 5.2.3. À l'exemple 4.3.16, nous avons vérifié qu'il existe une forme modulaire qui satisfait une congruence l'espace $\mathcal{S}_2(\Gamma_0(53), (\frac{53}{\cdot}))$. Il est possible avec PARI/GP de trouver une telle forme modulaire. Voici les commandes PARI/GP que l'on peut exécuter pour y parvenir :

```
gp > \r "dihedral.gp"
gp > S = mfinit([53, 2, 53], 0); \\espace des newforms de poids 2, niveau 53 et \
     caractere (53/.)
gp > corps = mffields(S);
gp > B = mfeigenbasis(S);
gp > length(B)

%1 = 1

gp > f = B[1];
gp > corps_de_f = nfinit(mffields[1]); \\creation du corps de nombres associe a f
gp > Pr = idealprimedec(corps_de_f, 7); \\liste des premiers au-dessus de p
gp > Nb_prem = #Pr \\nombre de premiers au-dessus de p

%2 = 3

gp > for(i, 1, Nb_prem, print(mfisdihedral(f, corps_de_f, 7, idealhnf(Pr[i]), 53)))

0
1
0

gp > coeff = mfcoefs(f, 50); \\calcul des 50 premiers coefficients
gp > norm(coeff)%7

%3 = [0, 1, 0, 0, 1, 0, 0, 4, 0, 0, 0, 2, 0, 0, 0, 0, 4, 4, 0, 0, 0, 0, 0, 0, 0, 0,
     0, 0, 4, 4, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 4, 2, 0, 0, 1, 0, 2, 0]
```

Plus précisément, la forme cuspidale de la session PARI/GP précédente est

$$\begin{aligned} f = q \ + \ & \alpha q^2 + (-\alpha^3 - 4\alpha)q^3 + (\alpha^2 + 2)q^4 + (\alpha^3 + 3\alpha)q^5 + (2\alpha^2 + 7)q^6 \\ & + (-\alpha^2 - 5)q^7 + (\alpha^3 + 4\alpha)q^8 + (-3\alpha^2 - 11)q^9 + (-3\alpha^2 - 7)q^{10} + (3\alpha^2 + 9)q^{11} - \alpha q^{12} \\ & + (-2\alpha^2 - 5)q^{13} + (-\alpha^3 - 5\alpha)q^{14} + (\alpha^2 + 7)q^{15} - 3q^{16} - 3q^{17} + (-3\alpha^3 - 11\alpha)q^{18} \\ & - 3\alpha q^{19} + (-\alpha^3 - \alpha)q^{20} + (3\alpha^3 + 13\alpha)q^{21} + (3\alpha^3 + 9\alpha)q^{22} + \alpha q^{23} + (3\alpha^2 + 14)q^{24} \\ & + \cdots \end{aligned}$$

où α est une racine de $X^4 + 6X^2 + 7$.

Pour conclure, nous venons de voir qu'il est possible à l'aide du logiciel PARI/GP d'effectuer des calculs numériques sur les formes modulaires. Il est à noter que nous avons survolé qu'une petite partie de l'ensemble des fonctionnalités de ce logiciel. En effet, ce dernier possède aussi des fonctions sur les courbes elliptiques, les corps de nombres et plus encore. Cependant, ce n'est pas le seul logiciel que l'on peut utiliser pour réaliser ces calculs. Un autre logiciel réputé pour ses fonctionnalités avec les formes modulaires est Sagemath [Sag]. Ce logiciel est libre de droit, ce qui signifie que quiconque peut y contribuer. Sagemath a pour avantage d'avoir une interface simple qui est basée sur le language de programmation Python. Au final, le choix d'un logiciel pour effectuer des calculs numériques est principalement préférentiel. Nous avons donc choisi PARI/GP dans ce mémoire dans le but de le rendre plus accessible et de présenter ses nouvelles fonctionnalités avec les formes modulaires.

Conclusion

Le but du présent mémoire était de détailler et de généraliser deux résultats de Dummigan et Heim mettant en lien le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$, où $p \equiv 3 \pmod 4$, avec les formes modulaires de poids $k = (p+1)/2$ et de niveau 1.

Dans un premier temps, nous avons montré que la trace de la fonction L carrée symétrique pour une base de formes propres normalisées de poids k et niveau 1 possède une p-valuation de -1 si et seulement si $h(-p) > 1$. Pour ce faire, nous avons étudié les formes modulaires de Siegel afin d'utiliser une formule de relèvement pour une série d'Eisenstein de degré 2. Nous avons également étudier des propriétés arithmétiques des nombres de Bernoulli qui nous ont permis de comprendre le lien entre la trace et le nombre de classe du corps quadratique $\mathbb{Q}(\sqrt{-p})$. À l'aide des congruences de Kummer, nous avons réussi à généraliser en partie ce lien pour une infinité de poids k' tels que $k' \equiv k \pmod{p-1}$. Bien que la valeur de la p-valuation de la trace change en fonction de k', notre généralisation démontre que le comportement de la p-valuation de la trace ne dépend pas uniquement de l'espace $\mathcal{S}_k(\Gamma(1))$, mais d'une infinité d'espace $\mathcal{S}_{k'}(\Gamma(1))$. Cette généralisation nous a mené à énoncer une conjecture, à laquelle nous avons certaines évidences numériques, mais une démonstration est toujours manquante.

Dans un deuxième temps, nous avons montré qu'il existe une forme propre normalisée qui satisfait une congruence diédrale en p si et seulement si $h(-p) > 1$. Afin d'y parvenir, nous avons étudié les représentations galoisiennes associées aux formes modulaires. Cette théorie nous a permis de démontrer l'existence d'une forme modulaire satisfaisant une congruence diédrale en p sous l'hypothèse que $h(-p) > 1$. Avec succès, nous avons montré que la propriété d'existence d'une congruence diédrale n'est pas uniquement vraie pour l'espace $\mathcal{S}_k(\Gamma(1))$, mais pour tous les espaces $\mathcal{S}_{k'}(\Gamma(1))$ avec $k' \equiv k \pmod{p-1}$. Cette généralisation a été obtenue de deux façons. La première utilisait une propriété de congruence des séries d'Eisenstein de poids $p-1$ alors que la deuxième utilisait la théorie des formes modulaire Λ-adiques.

Pour conclure, ce mémoire a permis de mieux comprendre le comportement du nombre de classes d'un corps quadratique à l'aide des formes modulaires. Toutefois, l'étude du nombre de classes ne s'arrête certainement pas là. Par exemple, les résultats mentionnés dans ce mémoire concernaient principalement le nombre de classe d'un corps quadratique *imaginaire*. En ce sens, on pourrait se demander : qu'en est-il du nombre de classes d'un corps quadratique *réel* ?

Bibliographie

[AAC52] N. C. Ankeny, E. Artin et S. Chowla : The class-number of real quadratic number fields. *Ann. of Math. (2)*, 56:479–493, 1952.

[AIK14] Tsuneo Arakawa, Tomoyoshi Ibukiyama et Masanobu Kaneko : *Bernoulli numbers and zeta functions*. Springer Monographs in Mathematics. Springer, Tokyo, 2014. With an appendix by Don Zagier.

[And09] Anatoli Andrianov : *Introduction to Siegel modular forms and Dirichlet series*. Universitext. Springer, New York, 2009.

[BG02] Alexander F. Brown et Eknath P. Ghate : Dihedral congruence primes and class fields of real quadratic fields. *J. Number Theory*, 95(1):14–37, 2002.

[Car59] L. Carlitz : Some arithmetic properties of generalized Bernoulli numbers. *Bull. Amer. Math. Soc.*, 65:68–69, 1959.

[Coh75] Henri Cohen : Sums involving the values at negative integers of L-functions of quadratic characters. *Math. Ann.*, 217(3):271–285, 1975.

[Coh13] Henri Cohen : Haberland's formula and numerical computation of Petersson scalar products. *In ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 de *Open Book Ser.*, pages 249–270. Math. Sci. Publ., Berkeley, CA, 2013.

[Del71] Pierre Deligne : Formes modulaires et représentations l-adiques. *In Séminaire Bourbaki. Vol. 1968/69 : Exposés 347–363*, volume 175 de *Lecture Notes in Math.*, pages Exp. No. 355, 139–172. Springer, Berlin, 1971.

[Del79] P. Deligne : Valeurs de fonctions L et périodes d'intégrales. *In Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 313–346. Amer. Math. Soc., Providence, R.I., 1979. With an appendix by N. Koblitz and A. Ogus.

[DH10] Neil Dummigan et Bernhard Heim : Symmetric square L-values and dihedral congruences for cusp forms. *J. Number Theory*, 130(9):2078–2091, 2010.

[DS05] Fred Diamond et Jerry Shurman : *A first course in modular forms*, volume 228 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Edi92] Bas Edixhoven : The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Gar84] Paul B. Garrett : Pullbacks of Eisenstein series ; applications. *In Automorphic forms of several variables (Katata, 1983)*, volume 46 de *Progr. Math.*, pages 114–137. Birkhäuser Boston, Boston, MA, 1984.

[Hid86a] Haruzo Hida : Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.*, 85(3):545–613, 1986.

[Hid86b] Haruzo Hida : Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup. (4)*, 19(2):231–273, 1986.

[Hid93] Haruzo Hida : *Elementary theory of L-functions and Eisenstein series*, volume 26 de *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1993.

[Hid98] Haruzo Hida : Global quadratic units and Hecke algebras. *Doc. Math.*, 3:273–284, 1998.

[Kha06] Chandrashekhar Khare : Serre's modularity conjecture : the level one case. *Duke Math. J.*, 134(3):557–589, 2006.

[KL64] Tomio Kubota et Heinrich-Wolfgang Leopoldt : Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.*, 214(215):328–339, 1964.

[Kli90] Helmut Klingen : *Introductory lectures on Siegel modular forms*, volume 20 de *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.

[KW09a] Chandrashekhar Khare et Jean-Pierre Wintenberger : Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare et Jean-Pierre Wintenberger : Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lou01] Stéphane Louboutin : Explicit upper bounds for residues of Dedekind zeta functions and values of L-functions at $s = 1$, and explicit lower bounds for relative class numbers of CM-fields. *Canad. J. Math.*, 53(6):1194–1222, 2001.

[Maa64] Hans Maass : Die Fourierkoeffizienten der Eisensteinreihen zweiten Grades. *Mat.-Fys. Medd. Danske Vid. Selsk.*, 34(7):25 pp. (1964), 1964.

[Maa72] Hans Maass : Über die Fourierkoeffizienten der Eisensteinreihen zweiten Grades. *Mat.-Fys. Medd. Danske Vid. Selsk.*, 38(14):13, 1972.

[Mil12] James S. Milne : *Modular Functions and Modular Forms* (v1.30), 2012. www.jmilne.org/math/.

[Miy89] Toshitsune Miyake : *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

[Neu99] Jürgen Neukirch : *Algebraic number theory*, volume 322 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[PAR18] PARI Group, Univ. Bordeaux. *PARI/GP version 2.11.0*, 2018. disponible à http://pari.math.u-bordeaux.fr/.

[Sag] Sage Developers : *SageMath, the Sage Mathematics Software System*. disponible à https://www.sagemath.org.

[Ser72] Jean-Pierre Serre : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser73a] Jean-Pierre Serre : Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]. pages 319–338. Lecture Notes in Math., Vol. 317, 1973.

[Ser73b] Jean-Pierre Serre : Formes modulaires et fonctions zêta p-adiques. pages 191–268. Lecture Notes in Math., Vol. 350, 1973.

[Ser77] Jean-Pierre Serre : *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Ser87] Jean-Pierre Serre : Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Shi94] Goro Shimura : *Introduction to the arithmetic theory of automorphic functions*, volume 11 de *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Sta67] H. M. Stark : A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[Ste07] William Stein : *Modular forms, a computational approach*, volume 79 de *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[vdG08] Gerard van der Geer : Siegel modular forms and their applications. *In The 1-2-3 of modular forms*, Universitext, pages 181–245. Springer, Berlin, 2008.

[Was97] Lawrence C. Washington : *Introduction to cyclotomic fields*, volume 83 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1997.

[Zag77] D. Zagier : Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields. pages 105–169. Lecture Notes in Math., Vol. 627, 1977.

[Zag81] D. Zagier : Sur la conjecture de Saito-Kurokawa (d'après H. Maass). *In Seminar on Number Theory, Paris 1979–80*, volume 12 de *Progr. Math.*, pages 371–394. Birkhäuser, Boston, Mass., 1981.