

Séries thêta harmoniques

Olaf Kwiatkowski - Ferdinand Jacobé de Naurois

4 juin 2023

Table des matières

Introduction	2
1 Formes modulaires	6
1.1 Définition et premières propriétés	6
1.1.1 L'action de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré	6
1.1.2 Fonctions modulaires	7
1.1.3 Séries d'Eisenstein	7
1.2 Formule des zéros	10
1.3 Dimension des espaces de formes modulaires	13
2 Séries thêta	16
2.1 Réseaux et séries thêta	16
2.1.1 Généralités sur les réseaux	16
2.1.2 Réseau dual	17
2.1.3 Définition des séries thêta	17
2.2 La formule sommatoire de Poisson	17
2.2.1 Séries de Fourier	18
2.2.2 Preuve de la formule sommatoire de Poisson	19
2.3 Modularité de $\theta_L(z)$	20
2.3.1 L'équation fonctionnelle de θ_L	20
2.3.2 Contraintes sur la dimension et modularité de θ_L	22
3 La gaussienne harmonique	24
3.1 Introduction	24
3.2 Calcul par la moyenne harmonique	25
3.2.1 La propriété de la moyenne pour les fonctions harmoniques	25
3.2.2 Le calcul de la transformée de Fourier	26
3.3 Calcul par algèbre linéaire	28
3.3.1 Les opérateurs E, F, Δ	28
3.3.2 Le calcul de la transformée de Fourier, deuxième version	32
3.4 Modularité de $\theta_{L,P}$	34
4 Application à la théorie des réseaux	36
4.1 Propriétés des réseaux	36
4.2 Construction de réseaux unimodulaires pairs	37
4.3 Utilisation de séries thêta	38
4.4 Systèmes de racines	39
4.5 Classification des réseaux unimodulaires pairs de rang 8 et 16	49

5	Formes modulaires de niveaux supérieurs	53
5.1	Sous-groupes de congruences et formes modulaires	53
5.1.1	Définitions et premières propriétés	53
5.1.2	Dimension de l'espace $M_2(\Gamma_0(4))$	56
5.2	Les formes modulaires de poids 2 de niveaux supérieurs	58
5.2.1	La série d'Eisenstein de poids 2	58
5.2.2	Les formes modulaires $G_{1,N}$ de niveaux supérieurs	62
5.2.3	La fonction θ^4 est une forme modulaire de niveau 4	63
5.2.4	Application au théorème des quatre carrés de Lagrange	65
	Conclusion	66

Introduction

Les formes modulaires

La théorie des formes modulaires sur le demi-plan de Poincaré a reçu ces dernières années une attention considérable. Originellement découvertes par Gauss au XIX^{ème} siècle, elles furent presque 200 ans plus tard absolument déterminantes dans la preuve du grand théorème de Fermat par Andrew Wiles. Leur succès tient au fait que, bien que définies analytiquement comme des fonctions holomorphes vérifiant une certaine équation fonctionnelle que voici :

$$f(z+1) = f(z) \qquad f\left(\frac{-1}{z}\right) = z^{2k} f(z),$$

elles portent une quantité d'informations considérable sur l'arithmétique des entiers. Par exemple, les coefficients du développement en série entière de certaines formes modulaires, les séries d'Eisenstein, sont égaux aux nombres de la forme :

$$\sigma_k(n) = \sum_{d|n} d^k$$

où la somme porte sur les diviseurs de n . La connaissance de certaines relations de liaison entre les formes modulaires donne alors des identités non triviales entre les nombres $\sigma_k(n)$, qu'il semble parfois très difficile de prouver indépendamment des formes modulaires.

Une autre curiosité arithmétique similaire : on peut montrer que la fonction de la variable $q = e^{2\pi iz}$ définie par :

$$\theta(q) = \sum_{a,b,c,d \in \mathbb{Z}} q^{a^2+b^2+c^2+d^2}$$

est également (à peu de choses près) une forme modulaire, dont on peut dès lors calculer les coefficients du développement en série entière en utilisant la théorie générale des formes modulaires. Ceci donne alors le théorème de Jacobi, une expression exacte du nombre de manières d'écrire un entier n comme somme de 4 carrés d'entiers, qu'on note $r_4(n)$. Voici cette identité, qui semble être tout droit sortie d'un carnet de Ramanujan :

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d.$$

Objectifs

Les objectifs de ce mémoire sont multiples. Le développement de la théorie générale des formes modulaires nous occupera tout au long du premier chapitre. Il sera notamment

l'occasion de calculer la dimension des espaces de formes modulaires, un point crucial permettant d'exhiber des relations de dépendance linéaire entre certaines formes modulaires. Le reste du mémoire sera consacré à l'étude des séries thêta harmoniques, une classe particulière de formes modulaires définies à partir de la donnée d'un certain réseau de $\mathbb{R}^n$. En particulier, on s'attachera à prouver que les séries thêta harmoniques sont, sous certaines conditions, des formes modulaires.

Ce phénomène, permettant d'associer à une certaine classe de réseaux de $\mathbb{R}^n$ des formes modulaires, a de profondes implications en théorie des réseaux. En effet, ces formes modulaires attachées à un réseau contiennent de nombreuses informations sur ce réseau, et fournissent notamment un invariant utile : si deux réseaux sont isométriques, ils ont les mêmes formes modulaires. Ces applications à la théorie des réseaux seront l'objet du quatrième chapitre. Enfin, le dernier chapitre aura pour objet d'étude les formes modulaires de niveaux supérieurs, et se terminera par la démonstration de la formule de Jacobi pour $r_4(n)$ citée en introduction.

Remerciements

Nous tenons à remercier chaleureusement Yi Shan pour son soutien constant, ses explications passionnantes et sa bonne humeur quotidienne. Nos indécisions ponctuelles quant à la direction à prendre ont toujours été compensées par ses nombreuses bonnes idées.

Nous remercions également Gaëtan Chenevier pour les quelques discussions déterminantes sur les réseaux que nous avons eu la chance d'avoir avec lui.

Chapitre 1

Formes modulaires

“There are five fundamental operations of mathematics : addition, subtraction, multiplication, division, and modular forms.” - Martin Eicher.

1.1 Définition et premières propriétés

Dans cette section, on définit la notion de forme modulaire. On en démontre les premières propriétés, et on donne l'exemple des séries d'Eisenstein.

1.1.1 L'action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré

Le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit naturellement sur le demi-plan $\mathbb{H} = \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$ de la manière suivante :

$$\begin{aligned} \cdot : \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} &\rightarrow \mathbb{H} \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \right) &\mapsto \frac{az + b}{cz + d}. \end{aligned}$$

En effet, pour tout $z \in \mathbb{H}$, toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ on a :

$$\mathrm{Im} \left(\frac{az + b}{cz + d} \right) = \frac{1}{2i} \left(\frac{az + b}{cz + d} - \frac{a\bar{z} + b}{c\bar{z} + d} \right) = \frac{1}{2i} \frac{(ad - bc)(z + \bar{z})}{|cz + d|^2} = \frac{\mathrm{Im}(z)}{|cz + d|^2}.$$

Si bien que pour $z \in \mathbb{H}$, et $M \in \mathrm{SL}_2(\mathbb{Z})$, on a $M \cdot z \in \mathbb{H}$. On vérifie alors que l'application $\cdot : \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \rightarrow \mathbb{H}$ définit alors bien une action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan supérieur $\mathbb{H}$. Son noyau contient $\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pm I_2\}$, donc cette action se factorise en une action de $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) / \{\pm I_2\}$ sur $\mathbb{H}$.

La question naturelle est alors : quelles sont les orbites de cette action ? On définit à cet effet **le domaine fondamental de Poincaré** :

$$\mathcal{D} = \left\{ z \in \mathbb{H}, \mathrm{Re}(z) \in \left[-\frac{1}{2}, \frac{1}{2} \right], |z| \geq 1 \right\}.$$

Ce domaine est un « domaine fondamental » pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$, ce qui signifie que chaque point de $\mathbb{H}$ est congru à un unique point de $\mathcal{D}$ modulo l'action de $\mathrm{SL}_2(\mathbb{Z})$ (si on identifie les points de la frontière de $\mathcal{D}$ comme il se doit). Nous ne démontrerons pas ce point.

1.1.2 Fonctions modulaires

Les formes modulaires sont, en deux mots, les fonctions de $\mathbb{H}$ dans $\mathbb{C}$ invariantes sous l'action de $\mathrm{SL}_2(\mathbb{Z})$.

Définition 1.1.1. Soit $k \in \mathbb{Z}$. On dit qu'une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbb{C}$ est une **fonction modulaire** de poids $2k$ si et seulement si pour tout $z \in \mathbb{H}$ et toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on a :

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z). \quad (1.1)$$

Remarque 1.1.2. On pourrait également définir des fonctions modulaires de poids $2k+1$, $k \in \mathbb{Z}$, mais une telle fonction f serait nécessairement nulle.

En effet constatons que $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$; si bien que :

$$\forall z \in \mathbb{H}, \quad f(z) = f\left(\frac{-1z+0}{0z-1}\right) = (-1)^{2k+1} f(z) = -f(z),$$

d'où la nullité de f .

Remarque 1.1.3. En constatant que la forme différentielle $d\left(\frac{az+b}{cz+d}\right)$ est égale à :

$$d\left(\frac{az+b}{cz+d}\right) = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} dz = \frac{dz}{(cz+d)^2}$$

L'équation précédente se ré-écrit donc de manière beaucoup plus compacte, pour tout matrice $M \in \mathrm{SL}_2(\mathbb{Z})$:

$$f(M \cdot z) d(M \cdot z)^k = f(z) dz^k.$$

Remarquons que $\mathrm{SL}_2(\mathbb{Z})$ est engendré uniquement par les deux matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Ces deux éléments vérifient les relations suivantes dans $\mathrm{PSL}_2(\mathbb{Z})$, pour $z \in \mathbb{H}$:

$$\begin{aligned} S^2 &= I_2, & (ST)^3 &= I_2, \\ Sz &= -\frac{1}{z}, & Tz &= z + 1. \end{aligned}$$

On en déduit immédiatement le lemme suivant, qui sera très pratique pour montrer qu'une fonction f donnée est une forme modulaire :

Lemme 1.1.4. Une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbb{C}$ est une fonction modulaire de poids $2k$ si et seulement si elle est 1-périodique, et vérifie pour tout $z \in \mathbb{H}$:

$$f\left(\frac{-1}{z}\right) = z^{2k} f(z). \quad (1.2)$$

1.1.3 Séries d'Eisenstein

Définition

Une première manière d'obtenir des fonctions modulaires est les séries d'Eisenstein. Pour tout $k > 1$ entier, on définit une fonction holomorphe sur $\mathbb{H}$ en posant :

$$\forall z \in \mathbb{H}, \quad G_k(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz+n)^{2k}}$$

Sous réserve que $k > 1$, la série converge normalement sur tout compact de $\mathbb{H}$, et définit donc une fonction holomorphe de $\mathbb{H}$ dans $\mathbb{C}$. Reste à voir qu'il s'agit bien d'une fonction modulaire.

Soit donc $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. En remarquant que M induit une permutation du réseau $\mathbb{Z}^2$ donnée par $(x, y) \mapsto (ax + cy, bx + dy)$, il vient pour tout $z \in \mathbb{H}$:

$$\begin{aligned} G_k(M \cdot z) &= \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{\left(m \frac{az+b}{cz+d} + n\right)^{2k}} \\ &= (cz + d)^{2k} \cdot \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{((am + cn)z + (bm + dn))^{2k}} \\ &= (cz + d)^{2k} \cdot \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz + n)^{2k}} = (cz + d)^{2k} \cdot G_k(z), \end{aligned}$$

qui montre que G_k est une fonction modulaire de poids $2k$.

G_k étant une fonction 1-périodique, on peut tâcher de l'écrire comme une fonction de la variable $q = e^{2\pi iz}$, ce qui revient essentiellement à déterminer son développement en série de Fourier. Ce calcul sera l'objet de la section suivante.

Développement en la variable $q = e^{2\pi iz}$

On part de la célèbre identité, due à Euler :

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{+\infty} \frac{2z}{z^2 - n^2} = \frac{1}{z} + \sum_{n=1}^{+\infty} \left(\frac{1}{z - n} + \frac{1}{z + n} \right)$$

où la série converge normalement sur tout compact de $\mathbb{H}$.

Voici une manière particulièrement simple de démontrer cette identité : on remarque que $z \mapsto \pi \cot(\pi z)$ a des pôles simples de résidus 1 à tous les entiers relatifs, et n'a aucun autre pôle. Dès lors, si l'on forme la différence $f(z)$ des deux membres de l'égalité précédente, on obtient une fonction entière, qui est 1-périodique et est bornée dans l'espace $\{z \in \mathbb{C} \mid |\mathrm{Im}(z)| > 1\}$. C'est donc une fonction entière bornée, donc constante par le théorème de Liouville. En l'étudiant au voisinage de 0, on obtient aisément que cette constante est nulle, ce qui montre l'égalité ci-dessus.

On développe ensuite $\cot(\pi z)$ en série géométrique de la variable $q = e^{2\pi iz}$, pour $z \in \mathbb{H}$ (de sorte que $q \in \mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$). Il vient :

$$\pi \cot(\pi z) = \pi i \frac{e^{\pi iz} + e^{-\pi iz}}{e^{\pi iz} - e^{-\pi iz}} = \pi i \frac{q + 1}{q - 1} = \pi i - 2\pi i \frac{1}{1 - q} = \pi i - 2\pi i \sum_{n=0}^{+\infty} q^n.$$

Si bien que pour $z \in \mathbb{H}$, et $q = e^{2\pi iz} \in \mathbb{D}$, il vient :

$$\pi i - 2\pi i \sum_{n=0}^{+\infty} q^n = \frac{1}{z} + \sum_{n=1}^{+\infty} \frac{1}{z - n} + \frac{1}{z + n}.$$

On dérive $2k - 1$ fois cette formule par rapport à la variable z (où $k \in \mathbb{N}$ avec $k \geq 2$), en remarquant que la dérivée de q par rapport à z est $2\pi i q$. Il vient :

$$-2\pi i \sum_{n=0}^{+\infty} (2\pi i)^{2k-1} n^{2k-1} q^n = (-1)^{2k-1} (2k-1)! \sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^{2k}}.$$

D'où :

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{1}{(2k-1)!} \sum_{n=0}^{+\infty} (2\pi i)^{2k} n^{2k-1} q^n.$$

Ceci étant valable pour tout $z \in \mathbb{H}$, on peut également l'appliquer à mz où $m \in \mathbb{N}^*$. On obtient alors l'expression suivante de $G_k(z)$, en séparant la somme selon que $m = 0$, $m > 0$ ou $m < 0$:

$$\begin{aligned} G_k(z) &= \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz+n)^{2k}} = 2\zeta(2k) + 2 \sum_{m=1}^{+\infty} \sum_{n \in \mathbb{Z}} \frac{1}{(mz+n)^{2k}} \\ &= 2\zeta(2k) + 2 \sum_{m=1}^{+\infty} \frac{1}{(2k-1)!} \sum_{n=0}^{+\infty} (2\pi i)^{2k} n^{2k-1} (q^m)^n \\ &= 2\zeta(2k) + \frac{4k(2\pi i)^{2k}}{(2k)!} \sum_{m=1}^{+\infty} \sum_{n=1}^{+\infty} n^{2k-1} q^{mn}. \end{aligned}$$

En sommant d'abord sur la variable $N = mn$, on obtient alors la formule suivante :

$$G_k(z) = 2\zeta(2k) + \frac{4k(2\pi i)^{2k}}{(2k)!} \sum_{N=1}^{+\infty} \sigma_{2k-1}(N) q^N,$$

où $\sigma_{2k-1}(N) = \sum_{d|N} d^{2k-1}$, la somme portant sur les diviseurs strictement positifs de N .

On peut alors utiliser la célèbre formule :

$$\zeta(2k) = \frac{(-1)^{k-1} B_{2k} \pi^{2k} 4^k}{2(2k)!},$$

où B_{2k} désigne le $2k$ -ième nombre de Bernoulli, pour obtenir :

$$G_k(z) = 2\zeta(2k) \left(1 - \frac{4k}{B_{2k}} \sum_{n=1}^{+\infty} \sigma_{2k-1}(n) q^n \right).$$

On définit alors naturellement la fonction modulaire normalisée E_k par :

$$E_k(z) = \frac{1}{2\zeta(2k)} G_k(z) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{+\infty} \sigma_{2k-1}(n) q^n.$$

On notera que, comme fonction de q , E_k se prolonge naturellement en $q = 0$. C'est cette condition qui distinguera les formes modulaires des simples fonctions modulaires.

Définition 1.1.5. Toute fonction modulaire f étant 1-périodique, elle s'écrit sous la forme $f(z) = F(q)$ où $q = e^{2\pi iz}$ et F est une fonction holomorphe de $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$ dans $\mathbb{C}$. La fonction f est alors appelée une **forme modulaire** si la fonction F a une singularité effaçable en $q = 0$.

Remarque 1.1.6. La théorie des singularités des fonctions holomorphes permet de donner des caractérisations équivalentes nettement plus simples du fait qu'une fonction modulaire soit une forme modulaire. En effet, en notant f une fonction modulaire, et F la fonction de $q = e^{2\pi iz}$ associée comme dans la définition ci-dessus, on a équivalence entre les propositions suivantes :

- (i) f est une forme modulaire ;
- (ii) F est bornée au voisinage de 0 ;
- (iii) $f(z)$ reste bornée quand $\text{Im}(z) \rightarrow +\infty$;
- (iv) F se prolonge en une fonction holomorphe de $\mathbb{D}$ dans $\mathbb{C}$.

En effet, (i) $\iff$ (iv) n'est qu'une ré-écriture de la définition, (ii) $\iff$ (iii) s'obtient immédiatement avec le changement de variable $q = e^{2\pi iz}$, et (ii) $\iff$ (iv) découle de la théorie élémentaire des singularités isolées des fonctions holomorphes (qu'on ne détaille pas ici).

Par ailleurs, le développement en série de Fourier des fonctions d'Eisenstein donné ci-dessus assure que pour tout entier $k > 1$, la fonction G_k est non seulement une fonction modulaire, mais bien une forme modulaire.

1.2 Formule des zéros

Cette section est très largement inspirée de l'influent *Cours d'arithmétique* [1] de Jean-Pierre Serre. Son objectif est le démontrer un théorème donnant le nombre de zéros et de pôles, comptés avec multiplicité, d'une fonction modulaire. On fera référence à ce théorème sous le nom de « formule des zéros » ou « lemme des zéros ».

Avant de démontrer ladite formule, commençons par introduire quelques notations. On fixe une fonction f méromorphe sur $\mathbb{H}$. Pour tout $p \in \mathbb{H}$, on note $v_p(f)$ l'ordre du zéro de f en p , qui est l'unique entier $n \in \mathbb{Z}$ tel que $z \mapsto f(z)/(z-p)^n$ se prolonge en une fonction holomorphe au voisinage de p , non nulle en p . Si de plus, f est 1-périodique, on peut considérer la fonction $\tilde{f} : \mathbb{D} \rightarrow \mathbb{C}$ telle que pour tout $z \in \mathbb{H}$, $q = e^{2\pi iz}$, on a $\tilde{f}(q) = f(z)$. L'ordre de f en ∞ , noté $v_\infty(f)$, est alors naturellement défini comme l'ordre de $\tilde{f}$ en 0. Notons que dans le cas où f est une fonction modulaire, $v_p(f)$ ne dépend que de la classe de p modulo $\text{SL}_2(\mathbb{Z})$, en vertu de l'équation modulaire. On s'autorisera donc la notation $v_{\bar{p}}(f)$ où $\bar{p}$ désigne la classe de p modulo l'action de $\text{SL}_2(\mathbb{Z})$. On notera également $j = e^{\frac{2\pi i}{3}}$.

Soit maintenant f une fonction modulaire, de telle sorte que $\tilde{f}$ soit une fonction méromorphe sur $\mathbb{D}$, et qu'on suppose non identiquement nulle. Alors, par le principe des zéros isolés, $\tilde{f}$ n'a qu'un nombre fini de zéros et de pôles dans tout compact de $\mathbb{D}$. Par le changement de variable $q = e^{2\pi iz}$, on en déduit que f n'a qu'un nombre fini de zéros et de pôles dans le domaine fondamental :

$$\mathcal{D} = \left\{ z \in \mathbb{H}, \quad |\Re(z)| \leq \frac{1}{2}, \quad |z| \geq 1 \right\}.$$

Autrement dit, il n'existe qu'un nombre fini de points $p \in \mathcal{D}$ tels que $v_p(f) \neq 0$. La somme apparaissant dans le théorème suivant est donc bien définie.

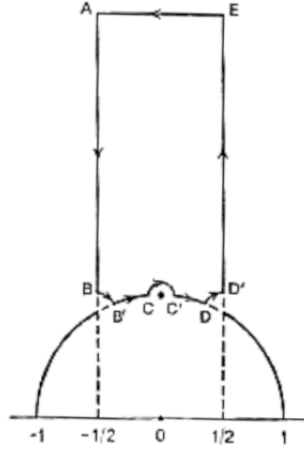
Théorème 1.2.1. (*La formule des zéros*) Soit $f : \mathbb{H} \rightarrow \mathbb{C}$ une fonction modulaire de

poids $2k$, $k \in \mathbb{N}$, de la variable z . On a alors l'égalité :

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_j(f) + \sum_{\substack{p \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \\ p \neq i, \bar{j}}} v_p(f) = \frac{k}{6}.$$

Démonstration. La preuve qui suit est empruntée au *Cours d'arithmétique* [1] de Jean-Pierre Serre.

Soit f une fonction modulaire. L'idée est d'intégrer la fonction $\frac{1}{2\pi i} \frac{f'}{f}$ sur la frontière du domaine fondamental $\mathcal{D}$. On suppose dans un premier temps que f n'a sur la frontière de $\mathcal{D}$ aucun autre zéro ou pôle que $j, i, -j^2$. Il existe alors un contour $\mathcal{C}$ tel que celui représenté ci-dessous, dont l'intérieur contient un représentant de chaque zéro ou pôle de f non congru à i ou j modulo $\mathrm{SL}_2(\mathbb{Z})$.



En appliquant le théorème des résidus, il vient donc :

$$\int_{\mathcal{C}} \frac{f'(z)}{f(z)} \frac{dz}{2\pi i} = \sum_{\substack{p \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \\ p \neq i, \bar{j}}} v_p(f). \quad (1.3)$$

Reste donc à évaluer l'intégrale de gauche. Pour chacun des arcs de l'intégrale, on fait les remarques suivantes :

a) Le changement de variable $q = e^{2\pi i z}$ transforme l'arc EA en un cercle ω centré en 0, parcouru dans le sens anti-trigonométrique, et ne refermant comme unique éventuel zéro ou pôle de $\tilde{f}$ seulement le point 0. On a donc, comme $dq = 2\pi i dz$ et $f'(z) = 2\pi i \tilde{f}'(q)$:

$$\frac{1}{2\pi i} \int_E^A \frac{f'(z)}{f(z)} dz = \frac{1}{2\pi i} \int_\omega \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq = -v_0(\tilde{f}) = -v_\infty(f).$$

b) L'intégrale de $\frac{1}{2\pi i} \frac{f'}{f}$ sur le cercle auquel appartient l'arc BB' , parcouru dans le sens anti-trigonométrique, vaut par le théorème des résidus $-v_j(f)$. Lorsque le rayon de ce

cercle tend vers 0, l'angle $B'jB$ tend vers $\frac{2\pi}{6}$, et donc on obtient, en intégrant le développement en série de Laurent de f en j sur l'arc $B'B$, quand le rayon du cercle auquel appartient l'arc $B'B$ tend vers 0 :

$$\frac{1}{2\pi i} \int_B^{B'} \frac{f'(z)}{f(z)} dz \rightarrow -\frac{1}{6} v_j(f).$$

Le même argument sur les arcs des cercles CC' et DD' fournit, quand les rayons des cercles tendent vers 0 :

$$\begin{aligned} \frac{1}{2\pi i} \int_D^{D'} \frac{f'(z)}{f(z)} dz &\rightarrow -\frac{1}{6} v_{-j^2}(f) = -\frac{1}{6} v_j(f), \\ \frac{1}{2\pi i} \int_C^{C'} \frac{f'(z)}{f(z)} dz &\rightarrow -\frac{1}{2} v_i(f). \end{aligned}$$

c) La translation $T : z \mapsto z + 1$ laissant f invariante et transformant l'arc AB en l'arc ED' , on a naturellement la compensation :

$$\frac{1}{2\pi i} \int_A^B \frac{f'(z)}{f(z)} dz + \frac{1}{2\pi i} \int_{D'}^E \frac{f'(z)}{f(z)} dz = 0.$$

d) L'application $S : z \mapsto \frac{-1}{z}$ transforme l'arc $B'C$ en l'arc DC' (attention aux orientations!). On peut donc espérer une forme de compensation entre les intégrales le long de ces deux arcs. Précisons cela. Il vient avec le changement de variable $z = \frac{-1}{u}$, $du = \frac{1}{z^2} dz$:

$$\frac{1}{2\pi i} \int_{B'C} \frac{f'(u)}{f(u)} du = \frac{1}{2\pi i} \int_D^{C'} \frac{f'(S(z))}{f(S(z))} \frac{dz}{z^2}. \quad (1.4)$$

Maintenant, f étant une fonction modulaire, on a $f(S(z)) = z^{2k} f(z)$, d'où, en dérivant les deux membres par rapport à z :

$$\frac{1}{z^2} f'(S(z)) = z^{2k-1} (2k f(z) + z f'(z)).$$

En injectant ce résultat dans eq. (1.4), il vient :

$$\frac{1}{2\pi i} \int_{B'C} \frac{f'(u)}{f(u)} du = \frac{1}{2\pi i} \int_D^{C'} \frac{z^{2k+1} (2k f(z) + z f'(z))}{z^{2k} f(z)} \frac{dz}{z^2} = \frac{1}{2\pi i} \int_D^{C'} \frac{f'(z)}{f(z)} dz + \frac{2k}{2\pi i} \int_D^{C'} \frac{dz}{z}.$$

Maintenant, comme la portion du cercle unité couverte par l'arc DC' tend vers $\frac{1}{12}$ quand les distances CC' et DD' tendent vers 0, il vient, quand le rayon des cercles contenant les arcs BB' , CC' , DD' tend vers 0 :

$$\frac{1}{2\pi i} \int_D^{C'} \frac{dz}{z} \rightarrow \frac{1}{12}.$$

Ce qui, avec le calcul précédent, donne la compensation attendue :

$$\frac{1}{2\pi i} \int_{B'C} \frac{f'(z)}{f(z)} dz + \frac{1}{2\pi i} \int_{C'D} \frac{f'(u)}{f(u)} dz \rightarrow \frac{k}{6}.$$

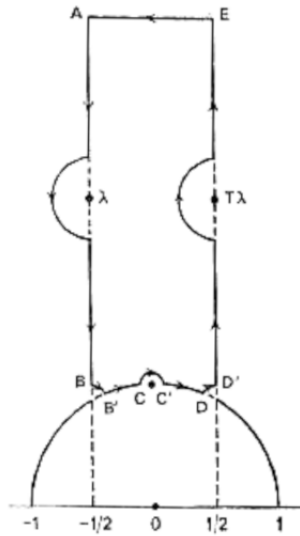
On obtient donc, en vertu des remarques a), b), c) et d), que quand le rayon des cercles qui contiennent les arcs BB' , CC' , DD' tend vers 0, on a :

$$\frac{1}{2\pi i} \int_C \frac{f'(z)}{f(z)} dz \rightarrow -v_\infty(f) - \frac{1}{6} v_j(f) - \frac{1}{3} v_i(f) - \frac{1}{6} v_j(f) + \frac{k}{6}.$$

En reprenant eq. (1.3), ceci fournit donc l'égalité attendue :

$$v_{\infty}(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_j(f) + \sum_{\substack{p \in \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \\ p \neq \bar{i}, \bar{j}}} v_p(f) = \frac{k}{6}.$$

Dans le cas où la frontière de $\mathcal{D}$ contient un zéro ou un pôle de f , on reprend la même démonstration, avec un contour modifié comme suit (le dessin représente le cas où f a un zéro sur le segment AB , et donc également sur le segment $D'E$; on procède évidemment de même si f a un zéro sur l'arc de cercle entre j et $-j^2$).



□

1.3 Dimension des espaces de formes modulaires

La formule précédente nous permettra de déterminer complètement la structure et la dimension des espaces de formes modulaires. En effet, elle nous permet de nous assurer que les formes modulaires n'ont en un certain sens « pas trop de zéros ». Autrement dit, une forme modulaire avec trop de zéros est la forme nulle : c'est ce genre de considérations qui nous permettront de borner la dimension des espaces de formes modulaires.

Pour la suite, on dira qu'une forme modulaire f est une **forme parabolique** si :

$$\lim_{\mathrm{Im}(z) \rightarrow +\infty} f(z) = 0.$$

Introduisons quelques notations :

$$\begin{aligned} M_{2k} &= \{\text{formes modulaires de poids } 2k\}, \\ M_{2k}^0 &= \{\text{formes paraboliques de poids } 2k\}. \end{aligned}$$

Remarquons déjà que M_{2k}^0 est le noyau vu dans M_{2k} de la forme linéaire $f \mapsto \lim_{\text{Im}(z) \rightarrow +\infty} f(z)$.

On en déduit que $\dim M_{2k}/M_{2k}^0 \leq 1$.

On pose :

$$\Delta = g_2^3 - 27g_3^2,$$

où :

$$g_2 = 60G_2, \quad g_3 = 140G_3.$$

C'est une forme parabolique de poids 12 (ce que l'on voit en utilisant les valeurs de $\zeta(4)$ et $\zeta(6)$).

On peut maintenant calculer explicitement les dimensions des espaces M_{2k} de formes modulaires.

Théorème 1.3.1. (*dimensions des espaces de formes modulaires*)

(i) Si $k < 0$ ou $k = 1$ $\dim M_{2k} = 0$.

(ii) Si $k = 0, 2, 3, 4$ ou 5 , M_{2k} est de dimension 1.

(iii) L'application $f \mapsto \Delta f$ est un isomorphisme entre M_{k-6} et M_{2k}^0 pour tout $k \in \mathbb{Z}$.

Démonstration. Pour le point (i), si $f \in M_{2k} \setminus \{0\}$ on doit écrire $\frac{k}{6} = n_1 + \frac{n_2}{2} + \frac{n_3}{3}$, avec $n_1, n_2, n_3 \in \mathbb{N}$.

On voit que cela est impossible si $k < 0$ ou $k = 1$. Pour $k = 2$, on voit que G_2 ne s'annule qu'en $j = e^{\frac{2\pi i}{3}}$ dans le domaine fondamental. De même pour $k = 3$, G_3 ne s'annule qu'en i .

On obtient donc que Δ ne s'annule pas en i . On en déduit que c'est une forme parabolique non nulle. On peut donc lui appliquer la formule des zéros. On sait déjà que Δ s'annule en ∞ , donc l'ordre de Δ en ∞ est ≥ 1 . Par la formule des zéros, ce zéro a pour multiplicité 1 exactement. On en déduit l'injectivité de $f \mapsto \Delta f$.

On en déduit que si $f \in M_{2k}^0 \setminus \{0\}$, on a :

$$v_p\left(\frac{f}{\Delta}\right) = \begin{cases} v_p(f) & \text{si } p \neq \infty \\ v_p(f) - 1 & \text{si } p = \infty \end{cases}$$

On en déduit que $\frac{f}{\Delta}$ est une forme modulaire de poids $2k-12$. Ceci démontre la surjectivité de l'application $f \mapsto \Delta f$, et donc (iii). On obtient (ii) en appliquant ce qui précède avec $k \in \{0, 2, 3, 4, 5\}$, puisque $k-6 < 0$, $M_{2k}^0 = \{0\}$. Mais par l'existence des séries d'Eisenstein si $k \geq 2$, et des fonctions constantes si $k = 0$ (qui sont modulaires), on obtient $\dim M_{2k} = 1$ dans ces cas. $\square$

Corollaire 1.3.2. Si $k \in \mathbb{N}$, $\dim M_{2k} = \begin{cases} \left\lfloor \frac{k}{6} \right\rfloor & \text{si } k \equiv 1 \pmod{6} \\ \left\lfloor \frac{k}{6} \right\rfloor + 1 & \text{si } k \not\equiv 1 \pmod{6} \end{cases}$

Démonstration. On utilise en itérant l'isomorphisme entre M_{2k}^0 et M_{k-6} , puis le fait que $\dim M_{2k} = \dim M_{2k}^0 + 1$ si $k \geq 2$, car on dispose des séries d'Eisenstein qui ne sont pas paraboliques. $\square$

Concluons cette section par un joli théorème sur la structure des formes modulaires.

Notons $M = \bigoplus_{k \in \mathbb{Z}} M_{2k}$

Corollaire 1.3.3. *On dispose d'un isomorphisme de $\mathbb{C}$ -algèbres :*

$$\begin{aligned}\Phi : \mathbb{C}[X, Y] &\rightarrow M \\ P(X, Y) &\mapsto P(G_2, G_3).\end{aligned}$$

Démonstration. On va montrer que $\{G_2^\alpha G_3^\beta, 2\alpha + 3\beta = k\}$ est une base de M_{2k} . On sait déjà que le résultat est vrai si $k \leq 3$. Pour $k \geq 4$, on peut raisonner par récurrence en choisissant un couple (α, β) tel que $2\alpha + 3\beta = k$, puis si $f \in M_{2k}$, alors on peut fixer $\lambda \in \mathbb{C}$ tel que $f - \lambda G_2^\alpha G_3^\beta$ est parabolique. On conclut en utilisant l'isomorphisme donné par Théorème 1.3.1.

Pour montrer que la famille est libre, remarquons que si l'on dispose d'une famille $(\lambda_{\alpha, \beta})$ non tous nuls tels que : $\sum_{\alpha, \beta} \lambda_{\alpha, \beta} G_2^\alpha G_3^\beta = 0$, alors $\frac{G_2^3}{G_3^2}$ annule un polynôme à coefficients complexes non nul. On peut l'obtenir en fixant un couple (γ, δ) tel que $2\gamma + 3\delta = k$, avec disons δ maximal. En divisant la relation précédente par $G_2^\gamma G_3^\delta$, et en utilisant la relation $2(\alpha - \gamma) + 3(\beta - \delta) = 0$ qui montre que $2|(\beta - \delta)$ et $3|(\alpha - \gamma)$, on obtient le polynôme voulu. On en déduit que $\frac{G_2^3}{G_3^2}$ est une fonction constante, ce qui est absurde car $G_2(j) = 0$, donc on obtiendrait $G_2 = 0$. $\square$

Chapitre 2

Séries thêta

2.1 Réseaux et séries thêta

2.1.1 Généralités sur les réseaux

Définition 2.1.1. On dit que $L \subset \mathbb{R}^d$ est un **réseau** de $\mathbb{R}^d$ si L vérifie l'une des conditions équivalentes suivantes :

- (i) L est un groupe abélien libre de rang d ;
- (ii) L est un sous-groupe discret de $\mathbb{R}^d$ qui l'engendre en tant que $\mathbb{R}$ -espace vectoriel.

Définition 2.1.2. Soit $\mathbf{e} = (e_1, \dots, e_d)$ une base de L . On note $\text{disc}(L)$ le déterminant de la matrice de Gram de $\mathbf{e}$: $\text{Gram}(\mathbf{e}) = (e_i \cdot e_j)_{1 \leq i, j \leq d}$.

Cette quantité est un invariant bien défini de L car si $\mathbf{e}'$ est une autre base de L , la matrice de passage de $\mathbf{e}$ à $\mathbf{e}'$ est un élément de $\text{GL}_d(\mathbb{Z})$ noté P . On a alors :

$$\text{Gram}(\mathbf{e}') = P^T \text{Gram}(\mathbf{e}) P.$$

D'où :

$$\det \text{Gram}(\mathbf{e}') = \det(P)^2 \det \text{Gram}(\mathbf{e}).$$

Mais puisque $P \in \text{GL}_d(\mathbb{Z})$, $\det(P) = \pm 1$, donc $\det \text{Gram}(\mathbf{e}') = \det \text{Gram}(\mathbf{e})$.

On peut par ailleurs interpréter $\sqrt{\text{disc}(L)}$ comme le volume d'un domaine fondamental de L , ou encore comme le volume de l'espace compact $\mathbb{R}^d/L$ (qui est homéomorphe à un d -tore).

Vocabulaire

Soit $L \subset \mathbb{R}^d$ un réseau. On dira que L est **entier** si le produit scalaire canonique $x \cdot y$ sur $\mathbb{R}^d$ prend des valeurs entières sur L . On suppose L entier dans la suite.

Si $\text{disc}(L) = 1$, on dira que le réseau L est **unimodulaire**.

Si la forme quadratique $x \cdot x$ prend des valeurs paires sur L , on dira que le réseau L est **pair**.

2.1.2 Réseau dual

Définition 2.1.3. On définit le **réseau dual** L' de L par :

$$L' = \{x \in \mathbb{R}^d \mid \forall y \in L, x \cdot y \in \mathbb{Z}\}.$$

Si $\mathbf{e}$ est une base de L , on vérifie aisément que la base duale $\mathbf{e}^*$ de $\mathbf{e}$, identifiée à une base de $\mathbb{R}^d$ via le théorème de représentation de Riesz, est une base de L' .

Notons A la matrice de $\mathbf{e}$ dans la base canonique de $\mathbb{R}^d$, et B celle de $\mathbf{e}^*$. Alors on a par définition de $\mathbf{e}^*$: $A^T B = I_d$. On en déduit que $B = (A^T)^{-1}$. Ceci permet de remarquer que si L est un réseau unimodulaire, alors L est auto-dual : $L' = L$. En effet, on a dans ce cas $A, B \in \text{GL}_d(\mathbb{Z})$, donc le changement de base $\mathbf{e} \rightarrow \mathbf{e}^*$ est un élément de $\text{GL}_d(\mathbb{Z})$. On en déduit que $\mathbf{e}$ et $\mathbf{e}^*$ engendrent le même réseau.

2.1.3 Définition des séries thêta

Définition 2.1.4. Soit $L \subset \mathbb{R}^d$ un réseau. La **fonction thêta** de L est définie par :

$$\begin{aligned} \theta_L : \mathbb{H} &\longrightarrow \mathbb{C} \\ z &\longmapsto \sum_{x \in L} e^{i\pi z(x \cdot x)}. \end{aligned}$$

On pose $N_L(k) = \#\{x \in L \mid x \cdot x = k\}$

On peut également exprimer θ_L en fonction de $q = e^{2i\pi z}$ (de façon un peu abusive si $x \cdot x$ prend des valeurs impaires) par :

$$\begin{aligned} \theta_L(q) &= \sum_{x \in L} q^{\frac{x \cdot x}{2}} \\ &= \sum_{k \in \mathbb{N}} N_L(k) q^{\frac{k}{2}}. \end{aligned}$$

La série définissant θ_L converge normalement sur tout compact de $\mathbb{H}$. En effet, on peut pour $k \in \mathbb{N}$ inclure $N_L(k)$ boules de rayon 1 dans la boule de rayon $k^{\frac{1}{2}} + 1$. On en déduit $N_L(k) = O_{k \rightarrow \infty}(k^{\frac{d}{2}})$.

2.2 La formule sommatoire de Poisson

Soit $f : \mathbb{R}^d \longrightarrow \mathbb{C}$ une fonction $\mathcal{C}^\infty$. On dira que f est à **décroissance rapide** si $\forall \alpha \in \mathbb{N}^d, \forall k \in \mathbb{N}, |\partial_\alpha f(x)| = o_{\|x\| \rightarrow +\infty}(\|x\|^{-k})$ (où α désigne un multi-indice).

L'objectif de cette partie est de démontrer la formule suivante :

Théorème 2.2.1. (*Formule sommatoire de Poisson*)

Soit $L \subset \mathbb{R}^d$ un réseau entier. Soit $f : \mathbb{R}^d \longrightarrow \mathbb{C}$ une fonction $\mathcal{C}^\infty$ à décroissance rapide. Alors :

$$\sum_{x \in L} f(x) = \frac{1}{\sqrt{\text{disc}(L)}} \sum_{y \in L'} \hat{f}(y),$$

où pour tout $y \in \mathbb{R}^d$:

$$\hat{f}(y) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i(y \cdot x)} dx.$$

2.2.1 Séries de Fourier

Soit $f : \mathbb{R} \rightarrow \mathbb{C}$ continue et 1-périodique. Il est connu que f est somme de sa série de Fourier. Ce résultat permet de démontrer la formule sommatoire de Poisson classique, qui correspond au cas $L = \mathbb{Z}$. Afin de démontrer la formule dans un cadre plus général, nous allons devoir généraliser ce résultat à des fonctions $\mathcal{C}^\infty$ invariantes par l'action par translation d'un réseau $L \subset \mathbb{R}^d$ que l'on fixe pour la suite.

Lemme 2.2.2. *Soit $\mathcal{P} = \text{Vect}\{e_y : x \mapsto e^{2\pi i(x \cdot y)} \mid y \in L'\} \subset \mathcal{C}(\mathbb{R}^d/L, \mathbb{C})$. Alors $\mathcal{P}$ est dense dans $\mathcal{C}(\mathbb{R}^d/L, \mathbb{C})$ (muni de la norme infinie).*

Démonstration. $\mathcal{P}$ est une sous-algèbre de $\mathcal{C}(\mathbb{R}^d/L, \mathbb{C})$ stable par conjugaison, qui contient les constantes et sépare les points. Comme $\mathbb{R}^d/L$ est compact, on peut conclure à l'aide du théorème de Stone-Weierstrass. $\square$

Fixons $\mathcal{D} \subset \mathbb{R}^d$ un domaine fondamental pour L . On définit un produit scalaire hermitien sur $\mathcal{C}(\mathbb{R}^d/L, \mathbb{C})$ par : $\langle f, g \rangle = \frac{1}{\sqrt{\text{disc}(L)}} \int_{\mathcal{D}} f(x) \bar{g}(x) dx$.

Lemme 2.2.3. *La famille $\mathcal{E} = \{e_y \mid y \in L'\}$ est orthonormée totale.*

Démonstration. Soit $\mathbf{e} = (e_1, \dots, e_d)$ une base de L définissant le domaine $\mathcal{D}$. Soit $y \neq y' \in L'$. En utilisant la formule de changement de variables pour les intégrales :

$$\begin{aligned} \langle e_y, e_{y'} \rangle &= \frac{1}{\sqrt{\text{disc}(L)}} \int_{\mathcal{D}} e^{-2\pi i((y-y') \cdot x)} dx \\ &= \int_{[0,1]^d} e^{-2\pi i((y-y') \cdot (x_1 e_1 + \dots + x_d e_d))} dx_1 \dots dx_d = \delta_{y, y'} \end{aligned}$$

en séparant la dernière intégrale en un produit de d intégrales.

Il reste à montrer que $\mathcal{P} = \text{Vect}(\mathcal{E})$ est dense dans $\mathcal{C}(\mathbb{R}^d/L, \mathbb{C})$ (pour la norme 2), mais c'est une conséquence immédiate du Lemme 2.2.2, car l'intégrale définissant le produit scalaire hermitien (f, g) est définie sur un compact, donc la convergence uniforme implique la convergence pour la norme hilbertienne. $\square$

Théorème 2.2.4. *Soit $f : \mathbb{R}^d \rightarrow \mathbb{C}$ une fonction $\mathcal{C}^\infty$ invariante par L . Alors f est somme de sa série de Fourier, et la convergence est normale :*

$$\forall x \in \mathbb{R}^d, f(x) = \sum_{y \in L'} \langle f, e_y \rangle e^{2\pi i(x \cdot y)}.$$

Démonstration. Posons pour tout $y \in L'$:

$$c_y(f) = \langle f, e_y \rangle.$$

Commençons par remarquer que si $y = n_1 e_1^* + \dots + n_d e_d^*$, alors une intégration par parties montre que :

$$c_y(\partial_j f) = 2\pi i n_j c_y(f)$$

où les dérivées partielles sont prises par rapport à la base $\mathbf{e}$. En itérant, on voit que pour tout $k \in \mathbb{N}$, $c_k(f) = o_{\|y\| \rightarrow +\infty}(\frac{1}{\|y\|^k})$. On en déduit que la fonction :

$$g(x) = \sum_{y \in L'} \langle f, e_y \rangle e^{2\pi i(x \cdot y)}$$

est somme d'une série normalement convergente sur $\mathbb{R}^d$, donc continue, et clairement invariante par L . On en déduit que g se factorise dans $\mathcal{C}(\mathbb{R}^d/L, \mathbb{C})$. Par Lemme 2.2.3, $\|g - f\|_2 = 0$, c'est à dire :

$$\int_{\mathcal{D}} |f(x) - g(x)|^2 dx = 0$$

comme $f - g$ est continue, on a bien $f = g$ sur $\mathcal{D}$, donc sur $\mathbb{R}^d$ car $f - g$ est invariante par L et que $\mathcal{D}$ est un domaine fondamental. $\square$

2.2.2 Preuve de la formule sommatoire de Poisson

Démonstration du Théorème 2.2.1. On se place dans le cadre du Théorème 2.2.1. On se donne donc $f : \mathbb{R}^d \rightarrow \mathbb{C}$ une fonction $\mathcal{C}^\infty$ à décroissance rapide. On note pour $y \in \mathbb{R}^d$:

$$\hat{f}(y) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i(x \cdot y)} dx$$

la transformée de Fourier de f .

On définit pour $t \in \mathbb{R}^d$:

$$F(t) = \sum_{x \in L} f(t + x).$$

Comme f est à décroissance rapide, la série précédente converge normalement sur $\mathbb{R}^d$, et définit donc une fonction $\mathcal{C}^\infty$ invariante par L sur $\mathbb{R}^d$. On en déduit que F est somme de sa série de Fourier :

$$\forall t \in \mathbb{R}^d, F(t) = \sum_{y \in L'} \langle F, e_y \rangle e^{2\pi i(y \cdot t)}.$$

Il reste donc à calculer les coefficients de cette série de Fourier. Or pour $y \in L'$:

$$\begin{aligned} \langle F, e_y \rangle &= \frac{1}{\sqrt{\text{disc}(L)}} \int_{\mathcal{D}} F(t) e^{-2\pi i(y \cdot t)} dt \\ &= \frac{1}{\sqrt{\text{disc}(L)}} \int_{\mathcal{D}} \left(\sum_{x \in L} f(t + x) \right) e^{-2\pi i(y \cdot t)} dt \\ &= \frac{1}{\sqrt{\text{disc}(L)}} \sum_{x \in L} \left(\int_{\mathcal{D}} f(x + t) e^{-2\pi i(y \cdot t)} dt \right) \\ &= \frac{1}{\sqrt{\text{disc}(L)}} \sum_{x \in L} \left(\int_{\mathcal{D}-x} f(t) e^{-2\pi i(y \cdot t)} dt \right) \\ &= \frac{1}{\sqrt{\text{disc}(L)}} \int_{\mathbb{R}^d} f(t) e^{-2\pi i(y \cdot t)} dt = \frac{1}{\sqrt{\text{disc}(L)}} \hat{f}(y). \end{aligned}$$

On justifie l'interversion entre intégrale et somme par le théorème de Fubini et le fait que f est intégrable car à décroissance rapide. L'avant dernière égalité provient du fait que $\mathcal{D}$ est un domaine fondamental, donc ses translatés recouvrent $\mathbb{R}^d$, et ne se chevauchent que sur un ensemble de mesure nulle.

On obtient la formule souhaitée en prenant $t = 0$. $\square$

2.3 Modularité de $\theta_L(z)$

On va montrer dans cette section, en utilisant la formule sommatoire de Poisson, que les séries thêta sont des formes modulaires. On fixe donc un réseau unimodulaire pair $L \subset \mathbb{R}^d$, où $d \in \mathbb{N}^*$ est un multiple de 8, et on considère la série thêta associée, en la variable $q = e^{2\pi iz}$:

$$\theta_L(z) = \sum_{x \in L} q^{\frac{x \cdot x}{2}} = \sum_{x \in L} e^{\pi i z (x \cdot x)}.$$

Le fait que le réseau L soit pair assure que pour tout $x \in L$, $\frac{x \cdot x}{2}$ est un entier, si bien que la formule ci-dessus définit bien une fonction holomorphe de q dans le disque ouvert $\mathbb{D}$, et donc une fonction holomorphe 1-périodique de la variable $z \in \mathbb{H}$.

On souhaite montrer que sous les hypothèses qui précèdent, la fonction θ_L est une forme modulaire de poids $2k = \frac{d}{2}$. Comme on sait déjà que $\theta_L(z+1) = \theta_L(z)$ pour tout $z \in \mathbb{H}$, et comme $\mathrm{SL}_2(\mathbb{Z})$ est engendré par $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, il suffit de montrer l'égalité suivante, où on a posé $2k = \frac{d}{2}$:

$$\theta_L\left(\frac{-1}{z}\right) = z^{2k} \theta_L(z). \quad (2.1)$$

Seulement, a priori, $2k = \frac{d}{2}$ n'est même pas entier. On va cependant voir que pour qu'il existe un réseau unimodulaire pair dans $\mathbb{R}^d$, il faut que d soit multiple de 8.

2.3.1 L'équation fonctionnelle de θ_L

Pour éviter les problèmes liés aux racines carrées multivaluées, on va commencer par se placer sur la demi-droite $i\mathbb{R}_+^*$. Soit donc $t \in \mathbb{R}_+^*$. On va démontrer l'égalité suivante :

Théorème 2.3.1. (*Équation fonctionnelle pour la fonction θ_L*)

Pour tout $t \in \mathbb{R}_+^*$, on a :

$$\theta_L\left(\frac{i}{t}\right) = t^{2k} \theta_L(it) \quad (2.2)$$

où on a posé $2k = \frac{d}{2}$, qui se ré-écrit (en utilisant au passage le fait que $k = \frac{d}{4}$ est un entier pair) :

$$\sum_{x \in L} e^{-\frac{\pi}{t} x \cdot x} = t^{2k} \sum_{x \in L} e^{-\pi t (x \cdot x)} \quad (2.3)$$

Démonstration. On fixe dans toute la suite un tel $t \in \mathbb{R}_+^*$, dans l'optique de démontrer la formule 2.2. On considère la fonction $f : x \mapsto e^{-t\pi(x \cdot x)}$. Cette fonction est de classe C^∞ à décroissance rapide à l'infini, et satisfait donc bien les hypothèses de la formule sommatoire de Poisson. Dans l'optique de lui appliquer la formule en question, calculons sa transformée de Fourier $\hat{f}$. On a, pour tout $y \in \mathbb{R}^d$:

$$\hat{f}(y) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i (y \cdot x)} dx = \int_{\mathbb{R}^d} \prod_{j=1}^d e^{-\pi t x_j^2 - 2\pi i x_j y_j} dx_1 dx_2 \dots dx_d.$$

D'où, en séparant l'intégrale du produit en produit des intégrales :

$$\hat{f}(y) = \prod_{j=1}^d \int_{-\infty}^{+\infty} e^{-\pi t x_j^2 - 2\pi i x_j y_j} dx_j = \prod_{j=1}^d \int_{-\infty}^{+\infty} e^{-\pi t x^2 - 2\pi i x y_j} dx. \quad (2.4)$$

Afin de calculer cette intégrale, on s'intéresse à la fonction :

$$g : z \mapsto \int_{-\infty}^{+\infty} e^{-\pi t x^2 - 2\pi x z} dx$$

Les théorèmes de dérivation sous le signe intégral assurent que la fonction g est holomorphe sur le plan $\mathbb{C}$. De plus, il est aisé de calculer g dans le cas où z est réel. En effet, on a alors par un changement de variable élémentaire :

$$g(z) = \int_{-\infty}^{+\infty} e^{-\pi t x^2 - 2\pi x z} dx = e^{\frac{\pi}{t} z^2} \int_{-\infty}^{+\infty} e^{-\pi t (x + \frac{z}{t})^2} dx = e^{\frac{\pi}{t} z^2} \sqrt{\frac{1}{t}}.$$

Cette expression reste naturellement valable dans le cas où z est un complexe quelconque, en vertu du théorème des zéros isolés (ou, selon les auteurs, le principe du prolongement analytique), les deux membres étant des fonctions holomorphes. En évaluant cette égalité en $z = iy_j$, il vient donc :

$$\int_{-\infty}^{+\infty} e^{-\pi t x^2 - 2\pi x i y_j} dx = e^{-\frac{\pi}{t} y_j^2} \sqrt{\frac{1}{t}}.$$

On en déduit alors le calcul de $\hat{f}$, en reportant cette intégrale dans 2.3 :

$$\hat{f}(y) = \prod_{j=1}^d \left(e^{-\frac{\pi}{t} y_j^2} \sqrt{\frac{1}{t}} \right) = \frac{1}{t^{d/2}} e^{-\frac{\pi}{t} y \cdot y}.$$

On est maintenant en mesure d'appliquer la formule sommatoire de Poisson à la fonction f . Il vient, en notant L' le réseau dual de L :

$$\sum_{x \in L} f(x) = \frac{1}{\mu(\mathbb{R}^d/L)} \sum_{y \in L'} \hat{f}(y).$$

On utilise alors l'unimodularité de L , qui assure non seulement que $L = L'$, mais également que $\mu(\mathbb{R}^d/L) = 1$. Il vient dès lors :

$$\sum_{x \in L} f(x) = \sum_{x \in L} \hat{f}(x).$$

Le calcul de f mené précédemment fournit donc l'égalité :

$$\sum_{x \in L} e^{-\pi t (x \cdot x)} = \frac{1}{t^{d/2}} \sum_{x \in L} e^{-\frac{\pi}{t} (x \cdot x)}.$$

qui se ré-écrit :

$$\sum_{x \in L} e^{-\frac{\pi}{t} (x \cdot x)} = t^{2k} \sum_{x \in L} e^{-\pi t (x \cdot x)},$$

qui est exactement la formule 2.3. Ceci conclut la preuve de l'équation fonctionnelle de la série θ_L . $\square$

Ainsi, on a obtenu que pour $z = it$ avec $t \in \mathbb{R}_+^*$, on a :

$$\theta_L \left(\frac{i}{t} \right) = t^{d/2} \theta_L(it).$$

Ce qui se ré-écrit :

$$\theta_L \left(\frac{-1}{z} \right) = \left(\frac{z}{i} \right)^{d/2} \theta_L(z)$$

où la racine carrée est l'unique racine carrée positive. Cependant, il reste un facteur i à faire disparaître, ainsi qu'un problème d'exposant non entier à régler. Ceci sera l'objet de la section suivante.

2.3.2 Contraintes sur la dimension et modularité de θ_L

Reprenons l'équation fonctionnelle précédente, valable pour tout $z \in i\mathbb{R}_+^*$:

$$\theta_L \left(\frac{-1}{z} \right) = \left(\frac{z}{i} \right)^{d/2} \theta_L(z). \quad (2.5)$$

On note que si l'on parvient à démontrer que d est en fait un multiple de 8, tous nos problèmes s'envelopent : le facteur $\left(\frac{z}{i}\right)^{d/2}$ devient alors z^{2k} avec $k = \frac{d}{4}$ entier, et on obtient bien une équation fonctionnelle de forme modulaire (valable a priori uniquement sur la demi-droite $i\mathbb{R}_+^*$, mais s'étendant à tout le demi-plan $\mathbb{H}$ par le principe des zéros isolés, les deux membres étant holomorphes sur $\mathbb{H}$).

On va donc dans cette section s'attacher à montrer le :

Théorème 2.3.2. *Si $L \subset \mathbb{R}^d$ est un réseau unimodulaire pair, alors d est un multiple de 8.*

Démonstration. On continue de noter θ_L la série thêta associée au réseau L . On commence par noter que l'équation 2.5 se prolonge naturellement par rigidité à tout le demi-plan $\mathbb{H}$. En effet, la fonction :

$$z \mapsto \theta_L \left(\frac{-1}{z} \right) - \left(\left(\frac{z}{i} \right)^{1/2} \right)^d \theta_L(z)$$

(où on a pris la détermination principale de la racine carrée, définie par $(re^{i\theta})^{1/2} = re^{i\frac{\theta}{2}}$ pour $r \in \mathbb{R}_+$, et $\theta \in]-\pi, \pi]$) est holomorphe sur $\mathbb{H}$, et nulle sur $i\mathbb{R}$. Elle est donc identiquement nulle, par le principe des zéros isolés. On en déduit la formule suivante, valable pour tout $z \in \mathbb{H}$:

$$\theta_L \left(\frac{-1}{z} \right) = \left(\left(\frac{z}{i} \right)^{1/2} \right)^d \theta_L(z) \quad (2.6)$$

où on note $w^{\frac{1}{2}}$ la racine carrée principale d'un complexe w .

Le membre de gauche est égal à $\theta_L(S \cdot z)$, avec les notations habituelles :

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

L'idée va alors être d'itérer l'équation 2.6, en remarquant que $(TS)^3 = I_2$. On note en effet que :

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

dont le polynôme caractéristique est $X^2 + X + 1$, diviseur de $X^3 - 1$. Le théorème de Cayley-Hamilton assure donc que $(TS)^3 = I_2$. Dès lors, il vient pour tout $z \in \mathbb{H}$:

$$\theta_L((TS)^3 z) = \theta_L(z).$$

En utilisant l'équation 2.6 et le fait que θ_L soit invariante par $z \mapsto Tz$, il vient alors :

$$\begin{aligned} \theta_L(z) &= \theta_L((TS)^3 z) = \left(\left(\frac{(TS)^2 z}{i} \right)^{1/2} \right)^d \theta_L((TS)^2 z) \\ &= \left(\left(\frac{(TS)^2 z}{i} \right)^{1/2} \right)^d \left(\left(\frac{(TS)z}{i} \right)^{1/2} \right)^d \theta_L((TS)z) \\ &= \left(\left(\frac{(TS)^2 z}{i} \right)^{1/2} \right)^d \left(\left(\frac{(TS)z}{i} \right)^{1/2} \right)^d \left(\left(\frac{z}{i} \right)^{1/2} \right)^d \theta_L(z). \end{aligned}$$

La fonction θ_L n'est pas identiquement nulle, et donc par intégrité de l'anneau des fonctions holomorphes sur $\mathbb{H}$, il vient pour tout $z \in \mathbb{H}$:

$$\left(\left(\frac{(TS)^2 z}{i} \right)^{1/2} \left(\frac{(TS)z}{i} \right)^{1/2} \left(\frac{z}{i} \right)^{1/2} \right)^d = 1. \quad (2.7)$$

Calculons le membre de gauche. On a :

$$\frac{(TS)^2 z}{i} \frac{(TS)z}{i} \frac{z}{i} = \frac{ST^{-1}z}{i} \frac{TSz}{i} \frac{z}{i} = \frac{1}{i^3} \frac{-1}{z-1} \left(\frac{-1}{z} + 1 \right) z = -i.$$

Le nombre :

$$\omega = \left(\frac{(TS)^2 z}{i} \right)^{1/2} \left(\frac{(TS)z}{i} \right)^{1/2} \left(\frac{z}{i} \right)^{1/2}$$

est donc une des deux racines carrées de $-i$, donc une racine primitive 8-ième de l'unité. L'équation $\omega^d = 1$ ci-dessus assure donc que 8 divise d , comme annoncé. $\square$

Comme annoncé au début de la section, la contrainte $8|d$ fait s'envoler tous nos problèmes. En effet, en posant $k = \frac{d}{4}$, on obtient :

Corollaire 2.3.3. *Si $L \subset \mathbb{R}^d$ est un réseau unimodulaire pair, alors la fonction θ_L est une forme modulaire de poids $2k = \frac{d}{2}$.*

Démonstration. On a montré dans la section précédente que pour tout $z \in i\mathbb{R}_+^*$, on a :

$$\theta_L \left(\frac{-1}{z} \right) = \left(\frac{z}{i} \right)^{d/2} \theta_L(z).$$

Maintenant, 8 divisant d , cette formule devient, pour tout $z \in i\mathbb{R}_+^*$:

$$\theta_L \left(\frac{-1}{z} \right) = z^{2k} \theta_L(z)$$

où k est l'entier $\frac{d}{4}$. Cette formule étant valable pour tout $z \in i\mathbb{R}_+^*$ et les deux membres de l'équation étant holomorphes sur $\mathbb{H}$, le principe du prolongement analytique permet alors de conclure que cette équation reste valable sur tout $\mathbb{H}$, ce qui prouve que θ_L est une forme modulaire de poids $2k$. $\square$

Chapitre 3

La gaussienne harmonique

3.1 Introduction

Dans ce chapitre, on va voir que la série thêta étudiée au chapitre précédent est un cas particulier d'un résultat beaucoup plus large. En effet, L étant un réseau unimodulaire pair, θ_L n'est pas la seule forme modulaire que l'on peut obtenir à partir du réseau L . Précisons cela.

Soit $L \subset \mathbb{R}^n$ un réseau unimodulaire pair. Par le chapitre précédent, ceci impose que n soit un multiple de 8. Soit P un polynôme harmonique (c'est à dire, tel que $\Delta P = 0$) homogène de degré d . On considère la fonction de la variable $q = e^{2\pi iz}$ (où $z \in \mathbb{H}$) suivante :

$$\theta_{L,P}(z) = \sum_{x \in L} P(x) q^{\frac{x \cdot x}{2}} = \sum_{x \in L} P(x) e^{\pi i z (x \cdot x)}. \quad (3.1)$$

Ceci définit bien une fonction holomorphe en la variable $q \in \mathbb{D}$ car le réseau L est pair (si bien que pour tout $x \in L$, $\frac{x \cdot x}{2}$ est un entier). C'est donc une fonction holomorphe 1-périodique en la variable $z \in \mathbb{H}$. Si d est impair, cette fonction dégénère en la fonction nulle. On supposera donc dans la suite que d est un entier pair.

On va montrer que sous les hypothèses qui précèdent, cette fonction $\theta_{L,P}$ est une forme modulaire de poids $2k = \frac{n}{2} + d$. On notera que si on prend $P = 1$, on retrouve le résultat de la partie précédente.

Pour cela, $SL_2(\mathbb{Z})$ étant engendré par les deux matrices S et T , il suffit de vérifier que l'équation suivante est vérifiée :

$$\forall z \in \mathbb{H}, \quad \theta_{L,P} \left(\frac{-1}{z} \right) = z^{\frac{n}{2} + d} \theta_{L,P}(z).$$

(ici, $z^{\frac{n}{2}}$ est bien défini car on a vu que 8 divise n).

Par le théorème des zéros isolés, il suffit en fait de vérifier cette égalité seulement sur $i\mathbb{R}_+^*$ (les deux membres étant des fonctions holomorphes sur $\mathbb{H}$). En posant $z = it$, $t \in \mathbb{R}_+^*$, on est donc ramené à montrer l'égalité suivante, pour tout $t \in \mathbb{R}_+^*$:

$$\theta_{L,P} \left(\frac{i}{t} \right) = (it)^{\frac{n}{2} + d} \theta_{L,P}(it).$$

Comme n est un multiple de 8 et d est un entier pair, cette équation se ré-écrit :

$$\forall t \in \mathbb{R}_+^*, \quad \theta_{L,P} \left(\frac{i}{t} \right) = (-1)^{\frac{d}{2}} t^{\frac{n}{2}+d} \theta_{L,P}(it).$$

Soit, pour tout $t \in \mathbb{R}_+^*$:

$$\sum_{x \in L} P(x) e^{-\frac{\pi}{t}(x \cdot x)} = (-1)^{\frac{d}{2}} t^{\frac{n}{2}+d} \sum_{x \in L} P(x) e^{-\pi t(x \cdot x)}. \quad (3.2)$$

C'est cette équation 3.2 que nous allons démontrer dans les sections précédentes, prouvant ainsi que $\theta_{L,P}$ est une forme modulaire de poids $\frac{n}{2} + d$.

Encore une fois, le résultat découlera de la formule sommatoire de Poisson, appliquée à la fonction lisse à décroissance rapide suivante (ici, $t \in \mathbb{R}_+^*$ est fixé) :

$$f : x \mapsto P(x) e^{-\pi t(x \cdot x)}.$$

Toute la difficulté résidant dans le calcul de la transformée de Fourier $\hat{f}$, naturellement définie par la formule suivante, valable pour tout $y \in \mathbb{R}^n$:

$$\hat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i(x \cdot y)} dx. \quad (3.3)$$

On va démontrer le résultat suivant, qui donne la valeur de la transformée de Fourier $\hat{f}$:

Théorème 3.1.1. (*Transformée de Fourier de la gaussienne-harmonique*)

Soit P un polynôme harmonique homogène à n variables, de degré $d \geq 0$, et t un réel strictement positif. On considère la fonction $f : x \mapsto P(x) e^{-\pi t(x \cdot x)}$ de la variable $x \in \mathbb{R}^n$, dont on note $\hat{f}$ la transformée de Fourier. On a alors, pour tout $y \in \mathbb{R}^n$:

$$\hat{f}(y) = \frac{1}{i^d t^{\frac{n}{2}+d}} e^{-\frac{\pi}{t}(y \cdot y)} P(y).$$

On propose deux preuves de ce résultat. La première est originale, et utilise la propriété de la moyenne pour les fonctions harmoniques, ainsi que la rigidité des fonctions holomorphes. La seconde est tirée du cours de Noam Elkies [2], et est fondée sur des relations algébriques entre certains opérateurs linéaires.

3.2 Calcul par la moyenne harmonique

On démontre dans cette section le Théorème 3.1.1 annoncé ci-dessus, en utilisant deux ingrédients : la rigidité des fonctions holomorphes, et la propriété de la moyenne pour les fonctions harmoniques. Pour cela, commençons par démontrer cette formule de la moyenne, en utilisant le théorème de Gauss sur la divergence (un avatar du théorème de Stokes).

3.2.1 La propriété de la moyenne pour les fonctions harmoniques

On démontre dans ce paragraphe le théorème suivant, conséquence du théorème de Gauss sur la divergence :

Théorème 3.2.1. Soit $f : \mathbb{R}^n \rightarrow \mathbb{C}$ une fonction harmonique (c'est à dire de classe $\mathcal{C}^2$, vérifiant $\Delta f = 0$). Soit $r > 0$.

On munit la sphère unité $\mathbb{S}^{n-1}$ de $\mathbb{R}^n$ de sa mesure de surface normalisée du (c'est à dire que $\int_{\mathbb{S}^{n-1}} du = 1$). Alors, on a pour tout $y \in \mathbb{S}^{n-1}$, tout $r > 0$:

$$f(y) = \int_{u \in \mathbb{S}^{n-1}} f(y + ru) du.$$

Autrement dit, $f(y)$ est égal à la moyenne de f sur la sphère de centre y et de rayon r .

Démonstration. Soient f et y fixés comme dans l'énoncé. On considère la fonction :

$$\begin{aligned} \psi : \mathbb{R}_+ &\rightarrow \mathbb{C} \\ r &\mapsto \int_{u \in \mathbb{S}^{n-1}} f(y + ru) du. \end{aligned}$$

Il est aisé de constater que la continuité de f en y assure que $\psi(r)$ tend vers $f(y)$ quand r tend vers 0. Pour conclure, il suffit donc de prouver que ψ est constante. Pour cela, on dérive ψ sous le signe intégral (le théorème de dérivation sous le signe intégral s'applique car on peut localement dominer les dérivées de f par des constantes, l'intégrale portant sur un compact). Il vient, pour tout $r > 0$:

$$\psi'(r) = \int_{u \in \mathbb{S}^{n-1}} (\nabla f(y + ru) \cdot u) du.$$

Par le théorème de Gauss sur la divergence, ceci vaut, à une constante multiplicative près :

$$\int_{x \in B(0,1)} \operatorname{div}(\nabla f(y + rx)) dx = \int_{x \in B(0,1)} \Delta f(y + rx) dx = 0.$$

Ainsi, ψ est constante, et tend vers $f(y)$ en 0. Donc, on a pour tout $r > 0$, $\psi(r) = f(y)$, ce qui conclut. $\square$

3.2.2 Le calcul de la transformée de Fourier

À l'aide de cette formule de la moyenne harmonique, on va pouvoir calculer la transformée de Fourier de la gaussienne harmonique.

Démonstration du Théorème 3.1.1. On conserve les notations et hypothèses du Théorème 3.1.1 : t est un réel strictement positif, P est un polynôme harmonique homogène de degré d , f est la fonction de $\mathbb{R}^n$ dans $\mathbb{C}$ définie par $f : x \mapsto P(x)e^{-\pi t(x \cdot x)}$. On note $\hat{f}$ sa transformée de Fourier, définie par :

$$\forall y \in \mathbb{R}^n, \quad \hat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i(x \cdot y)} dx.$$

Donnons nous dès maintenant un $y \in \mathbb{R}^n$. Il restera fixé tout au long de la preuve. On considère ensuite la fonction de la variable complexe z :

$$h(z) = \int_{\mathbb{R}^n} f(x) e^{-2\pi z(x \cdot y)} dx. \quad (3.4)$$

De sorte que le nombre qui nous intéresse est $\hat{f}(y) = h(i)$. L'intérêt de cette manoeuvre est le fait qu'il est nettement plus aisé de calculer $h(z)$ pour des valeurs réelles. Une formule

pour $h(z)$ valable pour z réel s'étendra alors à tout le plan complexe grâce au principe du prolongement analytique.

Soit donc $z \in \mathbb{R}$ réel. Calculons $h(z)$. Il vient :

$$\begin{aligned} h(z) &= \int_{\mathbb{R}^n} f(x) e^{-2\pi z(x \cdot y)} dx = \int_{\mathbb{R}^n} P(x) e^{-\pi t(x \cdot x) - 2\pi z(x \cdot y)} dx \\ &= e^{\frac{\pi}{t} z^2 (y \cdot y)} \int_{\mathbb{R}^n} P(x) e^{-\pi t((x \cdot x) + 2\frac{z}{t}(x \cdot y) + \frac{z^2}{t^2}(y \cdot y))} dx \\ &= e^{\frac{\pi}{t} z^2 (y \cdot y)} \int_{\mathbb{R}^n} P(x) e^{-\pi t(x + \frac{z}{t}y) \cdot (x + \frac{z}{t}y)} dx \\ &= e^{\frac{\pi}{t} z^2 (y \cdot y)} \int_{\mathbb{R}^n} P\left(u - \frac{z}{t}y\right) e^{-\pi t(u \cdot u)} du \quad \text{en posant : } u = x + \frac{z}{t}y. \end{aligned}$$

On utilise ensuite le fait que P est homogène de degré d pour obtenir, toujours pour $z \in \mathbb{R}$:

$$h(z) = \frac{(-z)^d e^{\frac{\pi}{t} z^2 (y \cdot y)}}{t^d} \int_{\mathbb{R}^n} P\left(y - \frac{t}{z}u\right) e^{-\pi t(u \cdot u)} du.$$

On se débarrasse du t dans l'exponentielle en posant $x = \sqrt{t}u$, de sorte que $dx = t^{\frac{n}{2}} du$:

$$h(z) = \frac{(-z)^d e^{\frac{\pi}{t} z^2 (y \cdot y)}}{t^{d+\frac{n}{2}}} \int_{\mathbb{R}^n} P\left(y - \frac{\sqrt{t}}{z}x\right) e^{-\pi(x \cdot x)} dx. \quad (3.5)$$

Reste à voir que l'intégrale du membre de droite de Equation (3.5) est indépendante de z . Pour simplifier les notations, posons pour tout $a > 0$:

$$g(a) = \int_{\mathbb{R}^n} P(y + ax) e^{-\pi(x \cdot x)} dx.$$

On va montrer que g est indépendante de a . En intégrant en coordonnées polaires (c'est à dire en posant $x = ru$ où $r \in \mathbb{R}_+$ et $u \in \mathbb{S}^{n-1}$), il vient, en notant $\mathbb{S}^{n-1}$ la sphère unité munie de sa mesure de surface du :

$$g(a) = \int_{r=0}^{+\infty} \int_{u \in \mathbb{S}^{n-1}} P(y + a(ru)) e^{-\pi(ru \cdot ru)} r^{n-1} du dr. \quad (3.6)$$

En ré-arrangeant cette intégrale, on obtient :

$$g(a) = \int_{r=0}^{+\infty} r^{n-1} e^{-\pi r^2} \left(\int_{u \in \mathbb{S}^{n-1}} P(y + (ar)u) du \right) dr.$$

Maintenant, pour tout $r \geq 0$, par la propriété de la moyenne pour les fonctions harmoniques, on a :

$$\frac{1}{\text{vol}(\mathbb{S}^{n-1})} \int_{u \in \mathbb{S}^{n-1}} P(y + (ar)u) du = P(y).$$

En reprenant la formule précédente, il vient donc pour tout $a > 0$:

$$g(a) = P(y) \text{vol}(\mathbb{S}^{n-1}) \int_0^{+\infty} r^{n-1} e^{-\pi r^2} dr,$$

g est donc constante sur $\mathbb{R}_+^*$. Comme g est clairement polynomiale (car c'est le cas de P) en la variable a , la fonction g est donc constante sur tout $\mathbb{R}$, égale à $g(0) = P(y)$.

En injectant l'égalité $g\left(-\frac{\sqrt{t}}{z}\right) = P(y)$ dans l'équation 3.5, on obtient donc que pour tout $z \in \mathbb{R}$, on a :

$$h(z) = \frac{(-z)^d e^{\frac{\pi}{t} z^2 (y \cdot y)}}{t^{d + \frac{n}{2}}} P(y).$$

Les deux membres sont des fonctions holomorphes de la variable $z \in \mathbb{C}$ (pour le membre de droite, c'est évident, et pour le membre de gauche, c'est une conséquence du théorème d'holomorphicité sous le signe intégral, au vu de la définition de h). Par le principe du prolongement analytique, comme ces deux membres coïncident sur $\mathbb{R}$, ils sont égaux sur tout $\mathbb{C}$. Reste à évaluer en i pour obtenir :

$$\hat{f}(y) = h(i) = \frac{(-i)^d e^{-\frac{\pi}{t} (y \cdot y)}}{t^{d + \frac{n}{2}}} P(y).$$

Ainsi, on a bien démontré, pour tout $y \in \mathbb{R}^n$, la formule :

$$\hat{f}(y) = \frac{1}{i^d t^{\frac{n}{2} + d}} e^{-\frac{\pi}{t} (y \cdot y)} P(y).$$

Ceci termine le calcul de la transformée de Fourier de la gaussienne harmonique. □

3.3 Calcul par algèbre linéaire

3.3.1 Les opérateurs E , F , Δ

Cette section, à saveur plus algébrique que les précédentes, portera sur certains opérateurs agissant sur l'espace des fonctions lisses de $\mathbb{R}^n$ dans $\mathbb{C}$.

On note, pour tout $d \in \mathbb{N}$, $\mathcal{P}_d$ l'espace des polynômes homogènes de degré d , en n variables et à coefficients complexes.

Définition 3.3.1 (Opérateurs). On introduit maintenant quelques opérateurs linéaires de l'espace $\mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$ dans lui-même.

· L'opérateur d'Euler E . Pour tout $f \in \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$, on note $E(f)$ la fonction :

$$E(f) : x \mapsto \sum_{j=1}^n x_j \partial_j f(x).$$

On remarque naturellement que pour tout $P \in \mathcal{P}_d$ (où $d \in \mathbb{N}$), on a $E(P) = dP$. La vérification, qui ne présente aucune difficulté particulière, est laissée au lecteur.

· L'opérateur norme F . C'est l'opérateur linéaire qui à une fonction $f \in \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$ associe la fonction $F(f)$ définie par :

$$F(f) : x \mapsto \|x\|^2 f(x)$$

où $\|\cdot\|$ désigne la norme euclidienne canonique sur $\mathbb{R}^n$.

· L'opérateur de Laplace Δ . Il associe à une fonction $f \in \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$ la fonction :

$$\Delta(f) = \sum_{j=1}^n \partial_j^2 f.$$

On rappelle que les fonctions de $\ker \Delta$ sont appelées fonctions "harmoniques".

· L'opérateur gaussien G_α . Pour tout $\alpha \in \mathbb{C}$, G_α est l'opérateur qui à une fonction $f \in \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$ associe la fonction $G_\alpha(f) : x \mapsto e^{-\alpha\pi(x \cdot x)} f(x)$.

· L'opérateur identité sur $\mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$ sera noté I .

Pour préparer le terrain, on commence par expliciter les relations de commutations entre certains de ces opérateurs.

Lemme 3.3.2. *Soit $\alpha \in \mathbb{C}$. L'opérateur G_α a pour inverse $G_{-\alpha}$ et commute avec F . De plus, on a les relations :*

$$G_\alpha E G_{-\alpha} = E + 2\pi\alpha F, \quad G_\alpha \Delta G_{-\alpha} = \Delta + \pi\alpha(4E + 2nI) + (2\pi\alpha)^2 F.$$

Démonstration. On fixe $\alpha \in \mathbb{C}$. Le fait que G_α soit inversible d'inverse $G_{-\alpha}$ est immédiat, de même que le fait que G_α commute avec F . Montrons les deux autres relations de commutations. Soit donc $f \in \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{C})$.

On a pour tout $x \in \mathbb{R}^n$:

$$\begin{aligned} G_\alpha E G_{-\alpha}(f)(x) &= e^{-\pi\alpha(x \cdot x)} \sum_{j=1}^n x_j \partial_j (f(x) e^{\alpha\pi(x \cdot x)}) \\ &= e^{-\pi\alpha(x \cdot x)} \sum_{j=1}^n x_j \left(\partial_j f(x) e^{\alpha\pi(x \cdot x)} + f(x) 2x_j \pi e^{\alpha\pi(x \cdot x)} \alpha \right) \\ &= \sum_{j=1}^n x_j \partial_j f(x) + 2\pi\alpha f(x) \sum_{j=1}^n x_j^2 = E(f)(x) + 2\pi\alpha F(f)(x). \end{aligned}$$

Ce qui fournit la première égalité : $G_\alpha E G_{-\alpha} = E + 2\pi\alpha F$.

Démontrons maintenant la seconde. Un calcul similaire donne, pour tout $x \in \mathbb{R}^n$:

$$\begin{aligned} G_\alpha \Delta G_{-\alpha}(f)(x) &= e^{-\pi\alpha(x \cdot x)} \sum_{j=1}^n \partial_j^2 (f(x) e^{\alpha\pi(x \cdot x)}) \\ &= e^{-\pi\alpha(x \cdot x)} \sum_{j=1}^n \left(\partial_j^2 f(x) e^{\alpha\pi(x \cdot x)} + 2\partial_j f(x) \partial_j (e^{\alpha\pi(x \cdot x)}) + f(x) \partial_j^2 (e^{\alpha\pi(x \cdot x)}) \right) \\ &= e^{-\pi\alpha(x \cdot x)} \sum_{j=1}^n \left(\partial_j^2 f(x) e^{\alpha\pi(x \cdot x)} + 4\pi\alpha x_j \partial_j f(x) e^{\alpha\pi(x \cdot x)} + f(x) \partial_j^2 e^{\alpha\pi(x \cdot x)} \right) \\ &= \sum_{j=1}^n (\partial_j^2 f(x) + 4\pi\alpha x_j \partial_j f(x)) + e^{-\alpha\pi(x \cdot x)} f(x) \sum_{j=1}^n \partial_j (2\pi\alpha x_j e^{\pi\alpha(x \cdot x)}) \\ &= \Delta(f)(x) + 4\pi\alpha E(f) + (2\pi\alpha) f(x) e^{-\alpha\pi(x \cdot x)} \sum_{j=1}^n \left(e^{\pi\alpha(x \cdot x)} + 2\pi\alpha x_j^2 e^{\alpha\pi(x \cdot x)} \right) \\ &= \Delta(f)(x) + 4\pi\alpha E(f) + 2\pi\alpha f(x) (n + 2\pi\alpha \|x\|^2) \\ &= \Delta(f)(x) + 4\pi\alpha E(f) + 2\pi\alpha f(x) + (2\pi\alpha)^2 F(f). \end{aligned}$$

On obtient donc bien la seconde égalité annoncée : $G_\alpha \Delta G_{-\alpha} = \Delta + \pi\alpha(4E + 2nI) + (2\pi\alpha)^2 F$. $\square$

Avant de passer au calcul de la transformée de Fourier de la gaussienne à proprement parler, on va également expliciter les relations entre ses opérateurs et la transformée de Fourier.

Pour cela, on va introduire l'espace fonctionnel de Schwartz, cadre naturel de ces calculs de transformée de Fourier.

Définition 3.3.3. Soit $n \in \mathbb{N}^*$. **L'espace de Schwartz $\mathcal{S}$** est défini comme l'espace des fonctions $\mathcal{C}^\infty$ de $\mathbb{R}^n$ dans $\mathbb{C}$ telles que pour tout $k \geq 0$, la différentielle k -ième de f , $D^k f$ est une fonction à décroissance rapide, c'est à dire vérifie pour tout $\beta > 0$:

$$D^k f(x) = o(\|x\|^{-\beta})$$

pour $x \in \mathbb{R}^n$ au voisinage de l'infini.

On peut alors définir la transformée de Fourier $\mathcal{F}$ dans un cadre légèrement plus formel.

Définition 3.3.4. L'opérateur $\mathcal{F} : \mathcal{S} \rightarrow \mathcal{S}$ est défini, pour tout $f \in \mathcal{S}$, par la formule :

$$\forall y \in \mathbb{R}^n, \quad \mathcal{F}f(y) = \hat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i(x \cdot y)} dx.$$

Les théorèmes de dérivation sous le signe intégral ainsi que des intégrations par parties permettent de vérifier que $\mathcal{F}$ est bien un opérateur de $\mathcal{S}$ dans $\mathcal{S}$.

On peut enfin expliciter le lien entre la transformée de Fourier et les opérateurs E , F et Δ .

Lemme 3.3.5. Soit $f : \mathbb{R}^n \rightarrow \mathbb{C}$ une fonction de l'espace de Schwartz, on note $\hat{f} = \mathcal{F}(f)$ sa transformée de Fourier. On a alors les résultats suivants sur les transformées de Fourier :

(i) Pour tout $j \in \llbracket 1, n \rrbracket$, on a :

$$\mathcal{F}(x_j f) = \frac{-1}{2\pi i} \partial_j \hat{f}, \quad \mathcal{F}(\partial_j f) = 2\pi i y_j \hat{f}$$

(où on note abusivement $x_j f$ la fonction $x \mapsto x_j f(x)$ et $y_j \hat{f}$ la fonction $y \mapsto y_j \hat{f}(y)$).

(ii) On a de plus les relations suivantes entre $\mathcal{F}$ et les opérateurs E, F, Δ :

$$\mathcal{F}(\Delta \hat{f}) = -4\pi^2 F(\hat{f}), \quad \mathcal{F}((2E + nI)f) = -(2E + nI)\hat{f}, \quad \mathcal{F}(Ff) = \frac{-1}{4\pi^2} \Delta(\hat{f}).$$

Démonstration. Seul le point (i) nécessite des arguments de nature analytique. En effet, le point (ii) découlera aisément du point (i) par linéarité et itération du point (i). Commençons donc par montrer le premier point.

(i) Soit donc $f \in \mathcal{S}$ et $j \in \llbracket 1, n \rrbracket$. En dérivant sous le signe intégral (ce qui est licite, car f est à décroissance rapide), il vient pour tout $y \in \mathbb{R}^n$:

$$\partial_j \hat{f}(y) = \int_{\mathbb{R}^n} f(x) \partial_j (e^{-2\pi i(x \cdot y)}) dx = \int_{\mathbb{R}^n} f(x) (-2\pi i x_j) e^{-2\pi i(x \cdot y)} dx = -2\pi i \mathcal{F}(x_j f)(y).$$

Ce qui prouve la première formule. Pour la seconde, on réalise une intégration par parties

par rapport à la variable x_j . Il vient, pour tout $y \in \mathbb{R}^n$:

$$\begin{aligned}
 \mathcal{F}(\partial_j f)(y) &= \int_{\mathbb{R}^n} \partial_j f(x) e^{-2\pi i(x \cdot y)} dx \\
 &= \int_{x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n \in \mathbb{R}} \left(\int_{x_j=-\infty}^{+\infty} \partial_j f(x) e^{-2\pi i(x \cdot y)} dx_j \right) dx_1 \dots dx_{j-1} dx_{j+1} dx_n \\
 &= \int_{x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n \in \mathbb{R}} \left(\left[f(x) e^{-2\pi i(x \cdot y)} \right]_{-\infty}^{+\infty} \right. \\
 &\quad \left. - \int_{x_j=-\infty}^{+\infty} f(x) (-2\pi i y_j) e^{-2\pi i(x \cdot y)} dx_j \right) dx_1 \dots dx_{j-1} dx_{j+1} dx_n \\
 &= 2\pi i y_j \int_{\mathbb{R}^n} f(x) e^{-2\pi i(x \cdot y)} dx = 2\pi i y_j \hat{f}(y).
 \end{aligned}$$

Ce qui démontre la seconde formule du point (i).

(ii) Le second point est une conséquence du premier, qu'on itère en utilisant la linéarité des équations. Fixons f une fonction de l'espace de Schwartz, dont on note $\hat{f} = \mathcal{F}(f)$ la transformée de Fourier. Il vient, par linéarité et en utilisant le (i) :

$$\mathcal{F}(\Delta f) = \mathcal{F} \left(\sum_{j=1}^n \partial_j^2 f \right) = \sum_{j=1}^n \mathcal{F}(\partial_j^2 f) = \sum_{j=1}^n (2\pi i y_j)^2 \mathcal{F}(f) = -4\pi^2 F(\hat{f}).$$

De même, pour la seconde et la troisième équations, on obtient (en utilisant la notation abusive $x_j f$ pour désigner la fonction $x \mapsto x_j f(x)$) :

$$\begin{aligned}
 \mathcal{F}((2E + nI))(f) &= \mathcal{F} \left(\sum_{j=1}^n (2x_j \partial_j f) + n f \right) = 2 \sum_{j=1}^n \mathcal{F}(x_j \partial_j f) + n \hat{f} \\
 &= n \hat{f} + 2 \sum_{j=1}^n \frac{-1}{2\pi i} \partial_j \mathcal{F}(\partial_j f) = -n \hat{f} - 2 \sum_{j=1}^n \partial_j (y_j \hat{f}) \\
 &= n \hat{f} - 2 \sum_{j=1}^n (y_j \partial_j \hat{f} + \hat{f}) = -2E(\hat{f}) - n \hat{f} = -(2E + nI) \hat{f} \\
 \text{et : } \quad \mathcal{F}(Ff) &= \mathcal{F} \left(\sum_{j=1}^n x_j^2 f \right) = \sum_{j=1}^n \mathcal{F}(x_j^2 f) = \sum_{j=1}^n \left(\frac{-1}{2\pi i} \right)^2 \partial_j^2 \hat{f} = \frac{-1}{4\pi^2} \Delta(\hat{f}).
 \end{aligned}$$

Ce qui démontre les deux dernières formules, et conclut donc la preuve du lemme. $\square$

Remarque 3.3.6. On constate aisément en utilisant la linéarité de $\mathcal{F}$ que la seconde formule du point (ii) est équivalente à la formule suivante, légèrement plus maniable dans certaines situations : $\mathcal{F}(E)(f) = -(E + nI)(f)$.

Ces quelques lemmes d'algèbre linéaire vont nous permettre de calculer la transformée de Fourier de la gaussienne harmonique, comme annoncé. Ce calcul sera l'objet de la section suivante.

3.3.2 Le calcul de la transformée de Fourier, deuxième version

On va commencer par donner la forme générale de la transformée de Fourier de f dans le cas où P est un polynôme homogène de degré d (pas forcément harmonique). Ceci résulte d'un calcul élémentaire.

Lemme 3.3.7. *Soit $P \in \mathcal{P}_d$ homogène de degré d en n variables, $t > 0$. On s'intéresse à la fonction :*

$$f : x \mapsto P(x)e^{-\pi t(x \cdot x)}$$

Il existe alors un polynôme Q de degré au plus $d - 1$ tel que pour tout $y \in \mathbb{R}$, on ait :

$$\hat{f}(y) = i^{-d} t^{-(\frac{n}{2}+d)} e^{-\frac{\pi}{t}(y \cdot y)} (P(y) + Q(y)).$$

Remarque 3.3.8. Ceci exprime le fait que la partie de plus haut degré du polynôme P est conservée par passage à la transformée de Fourier. Cependant, comme on le verra plus tard, dans le cas particulier où P est harmonique, le polynôme Q est nul, et donc P multiplié par la gaussienne est - à quelques constantes près - sa propre transformée de Fourier.

Démonstration. La preuve est une bête récurrence, associée à une petite intégration par parties. On raisonne par récurrence sur d . Le cas $d = 0$ a déjà été traité dans le chapitre précédent : il correspond au calcul de la transformée de Fourier de la gaussienne. On fixe donc un degré $d \geq 0$ tel que le résultat soit vérifié pour les polynômes de $\mathcal{P}_d$, et on le montre pour ceux de $\mathcal{P}_{d+1}$.

Soit donc un polynôme P homogène de degré $d + 1$. Par linéarité de la transformée de Fourier et de l'équation à démontrer, on peut sans perte de généralité supposer que P s'écrit sous la forme $P = X_j P_0$ où $P_0 \in \mathcal{P}_d$ et $j \in \llbracket 1, n \rrbracket$. Il vient alors, pour tout $y \in \mathbb{R}^n$:

$$\hat{f}(y) = \int_{\mathbb{R}^n} P(x) e^{-\pi t(x \cdot x) - 2\pi i(x \cdot y)} dx = \int_{\mathbb{R}^n} x_j P_0(x) e^{-\pi t(x \cdot x) - 2\pi i(x \cdot y)} dx.$$

Par le théorème de dérivation sous le signe intégral (qui s'applique car on peut dominer localement chacune des dérivées par des fonctions intégrables), cette dernière intégrale est égale à :

$$\hat{f}(y) = \frac{1}{-2\pi i} \partial_j \left(\int_{\mathbb{R}^n} P_0(x) e^{-\pi t(x \cdot x) - 2\pi i(x \cdot y)} dx \right) \quad (3.7)$$

(où la dérivée partielle porte sur la variable y_j).

On utilise alors l'hypothèse de récurrence au rang d , appliquée à P_0 . On obtient donc l'existence de Q_0 de degré au plus $d - 1$ tel que :

$$\int_{\mathbb{R}^n} P_0(x) e^{-\pi t(x \cdot x) - 2\pi i(x \cdot y)} dx = i^{-d} t^{-(\frac{n}{2}+d)} e^{-\frac{\pi}{t}(y \cdot y)} (P_0(y) + Q_0(y)).$$

On injecte ceci dans l'équation 3.7, et il vient, pour tout $y \in \mathbb{R}^n$:

$$\hat{f}(y) = \frac{-1}{2\pi i} i^{-d} t^{-(\frac{n}{2}+d)} e^{-\frac{\pi}{t}(y \cdot y)} \left(-\frac{\pi}{t} 2y_j (P_0(y) + Q_0(y)) + \partial_j (P_0(y) + Q_0(y)) \right).$$

On pose alors $Q(Y) = Y_j Q_0(Y) - \frac{t}{2\pi} \partial_j (P_0(Y) + Q_0(Y))$ qui est un polynôme de degré au plus d , de sorte que :

$$\begin{aligned} \hat{f}(y) &= i^{-(d+1)} t^{-(\frac{n}{2}+(d+1))} e^{-\frac{\pi}{t}(y \cdot y)} (y_j P_0(y) + Q(y)) \\ &= i^{-(d+1)} t^{-(\frac{n}{2}+(d+1))} e^{-\frac{\pi}{t}(y \cdot y)} (P(y) + Q(y)). \end{aligned}$$

Ceci termine la récurrence, et achève donc la preuve du lemme. $\square$

On va maintenant pouvoir s'intéresser au cas où P est un polynôme harmonique. On fixe donc un polynôme harmonique homogène de degré $d \geq 0$ quelconque, et on considère la fonction de $\mathbb{R}^n$ dans $\mathbb{C}$ définie par :

$$f : x \mapsto P(x)e^{-\pi t(x \cdot x)}.$$

Le lemme précédent assure qu'il existe, pour tout $j \in \llbracket 1, d \rrbracket$, un polynôme $Q_j \in \mathcal{P}_j$ (comme dans le paragraphe précédent, $\mathcal{P}_j$ désigne l'espace des polynômes homogènes de degré j à coefficients complexes), avec $Q_d = P$, tels que :

$$\forall y \in \mathbb{R}^n, \quad \hat{f}(y) = \frac{e^{-\frac{\pi}{t}(y \cdot y)}}{i^d t^{\frac{n}{2}+d}} \sum_{j=0}^d Q_j(y). \quad (3.8)$$

Afin de conclure cette seconde preuve du Théorème 3.1.1, il s'agit donc de prouver que sous l'hypothèse supplémentaire " P harmonique", on a $Q_0 = \dots = Q_{d-1} = 0$. C'est l'objet de ce second lemme :

Lemme 3.3.9. *Sous les notations et hypothèses de l'équation 3.8, on a :*

$$Q_0 = \dots = Q_{d-1} = 0.$$

Démonstration. On fixe P un polynôme harmonique homogène de degré $d \geq 0$, à n variables et à coefficients complexes, et on considère la fonction de $\mathbb{R}^n$ dans $\mathbb{C}$:

$$f : x \mapsto P(x)e^{-\pi t(x \cdot x)},$$

où t est un réel fixé, strictement positif. On considère la transformée de Fourier $\hat{f} = \mathcal{F}(f)$ de f . Le lemme qui précède assure l'existence de $Q_0, \dots, Q_d$ homogènes de degrés respectifs $0, \dots, d$, avec $Q_d = P$, tels que :

$$\hat{f} = \frac{1}{i^d t^{\frac{n}{2}+d}} \sum_{j=1}^n G_{\frac{1}{t}} Q_j \quad (3.9)$$

(on rappelle que les opérateurs G_α sont définis au début de Section 3.3.1).

Maintenant, comme on sait que $f = G_t P$ soit $P = G_{-t} f$, le caractère harmonique de P donne $0 = \Delta P = \Delta G_{-t} f$, si bien que $G_t \Delta G_{-t} f = 0$. De la même façon, comme P est homogène de degré d , on a $EP = dP$, si bien que $EG_{-t} f = dG_{-t} f$, soit $G_t EG_{-t} f = df$. On obtient donc les deux équations linéaires suivantes, vérifiées par f , découlant respectivement de l'harmonicité et de l'homogénéité de P :

$$G_t \Delta G_{-t} f = 0, \quad G_t EG_{-t} f = df.$$

On utilise alors Lemme 3.3.2, qui donne une expression explicite des opérateurs présents dans l'équation ci-dessus. On obtient alors, en injectant le résultat de ce lemme dans ladite équation :

$$E(f) + 2\pi t F(f) = df, \quad \Delta(f) + \pi t(4E + 2nI)(f) + (2\pi t)^2 F(f) = 0$$

On applique alors la transformée de Fourier $\mathcal{F}$ aux deux membres de cette équation. En utilisant Lemme 3.3.5, on obtient donc successivement :

$$\begin{aligned} -(E + nI)(\hat{f}) - \frac{t}{2\pi}\Delta\hat{f} &= d\hat{f}, & -4\pi^2 F(\hat{f}) - 2\pi t(2E + nI)(\hat{f}) - t^2\Delta\hat{f} &= 0, \\ \text{soit :} \quad -\Delta\hat{f} &= \frac{2\pi}{t}(E(\hat{f}) + (n + d)\hat{f}), & -\Delta\hat{f} &= \frac{4\pi^2}{t^2}F(\hat{f}) + \frac{2\pi}{t}(2E + nI)(\hat{f}). \end{aligned}$$

On identifie les deux équations précédentes, pour obtenir :

$$\frac{2\pi}{t}(E(\hat{f}) + (n + d)\hat{f}) = \frac{4\pi^2}{t^2}F(\hat{f}) + \frac{2\pi}{t}(2E + nI)(\hat{f}).$$

On divise les deux membres par $\frac{2\pi}{t}$, et on simplifie les quantités égales. On obtient finalement l'équation :

$$\left(E + \frac{2\pi}{t}F\right)\hat{f} = d\hat{f}. \quad (3.10)$$

En repassant aux polynômes, on va voir que cette dernière équation impose que le polynôme :

$$Q = \sum_{j=0}^d Q_j$$

est homogène de degré d . Vérifions cela. On a vu au début de la démonstration qu'on a l'égalité $\hat{f} = i^{-d}t^{-\frac{n}{2}-d}G_{\frac{1}{t}}Q$. Il en découle donc que $Q = i^d t^{\frac{n}{2}+d}G_{-\frac{1}{t}}\hat{f}$, si bien que, en utilisant Lemme 3.3.2 :

$$G_{\frac{1}{t}}E(Q) = i^d t^{\frac{n}{2}+d}(G_{\frac{1}{t}}EG_{-\frac{1}{t}})(\hat{f}) = i^d t^{\frac{n}{2}+d}\left(E + \frac{2\pi}{t}F\right)(\hat{f}).$$

On utilise alors l'équation 3.10, qui fournit donc :

$$G_{\frac{1}{t}}E(Q) = i^d t^{\frac{n}{2}+d}d\hat{f}.$$

Ce qui se réécrit :

$$E(Q) = d \cdot i^d t^{\frac{n}{2}+d}G_{-\frac{1}{t}}\hat{f} = dQ.$$

Maintenant, l'équation $E(Q) = dQ$ ainsi obtenue impose que Q est homogène de degré d . En effet, on a $Q = Q_0 + \dots + Q_d$ où pour tout $j \in \llbracket 1, d \rrbracket$, Q_j est dans l'espace propre de E associé à la valeur propre j . Comme Q est lui-même dans l'espace propre de E de valeur propre d , le fait que les espaces propres de E sont en somme directe impose que $Q = Q_d$ et $Q_0 = \dots = Q_{d-1} = 0$, ce qui achève la preuve du lemme. $\square$

Des deux derniers lemmes, on déduit Théorème 3.1.1, comme attendu.

3.4 Modularité de $\theta_{L,P}$

Rappelons Théorème 3.1.1, démontré de deux manières différentes dans les sections précédentes :

Théorème (*Transformée de Fourier de la gaussienne-harmonique*)

Soit P un polynôme harmonique homogène à n variables, de degré $d \geq 0$, et t un réel

strictement positif. On considère la fonction $f : x \mapsto P(x)e^{-\pi t(x \cdot x)}$ de la variable $x \in \mathbb{R}^n$, dont on note $\hat{f}$ la transformée de Fourier. On a alors, pour tout $y \in \mathbb{R}^n$:

$$\hat{f}(y) = \frac{1}{i^d t^{\frac{n}{2}+d}} e^{-\frac{\pi}{t}(y \cdot y)} P(y).$$

Ce théorème va nous permettre de conclure la preuve du résultat qui nous occupe, à savoir la modularité de la fonction $\theta_{L,P}$. Rappelons les hypothèses. $L \subset \mathbb{R}^n$ est un réseau unimodulaire pair. En vertu des résultats du chapitre 2, ceci impose que n est un multiple de 8. On fixe également un polynôme harmonique homogène de degré d pair, à coefficients complexes, qu'on note P . On considère alors la fonction holomorphe de la variable $z \in \mathbb{H}$, $\theta_{L,P}$ définie par la série :

$$\forall z \in \mathbb{H}, \quad \theta_{L,P}(z) = \sum_{x \in L} P(x) e^{i\pi z(x \cdot x)}.$$

Le fait que L est un réseau pair assure que $\theta_{L,P}$ est 1-périodique. Pour montrer le théorème qui nous occupe, à savoir que $\theta_{L,P}$ est une forme modulaire de poids $\frac{n}{2} + d$, il suffit donc de montrer l'égalité :

$$\forall z \in \mathbb{H}, \quad \theta_{L,P}\left(\frac{-1}{z}\right) = z^{\frac{n}{2}+d} \theta_{L,P}(z).$$

Or, les deux membres sont des fonctions holomorphes de la variable $z \in \mathbb{H}$. Par le principe du prolongement analytique, il suffit donc de vérifier cette égalité pour $z = it$, $t \in \mathbb{R}_+^*$. Après ce changement de variable, l'égalité à démontrer devient donc (en prenant en compte le fait que n est divisible par 8, ce qui assure $i^{\frac{n}{2}} = 1$) :

$$\forall t \in \mathbb{R}_+^*, \quad \sum_{x \in L} P(x) e^{-\frac{\pi}{t}(x \cdot x)} = i^d t^{\frac{n}{2}+d} \sum_{x \in L} P(x) e^{-\pi t(x \cdot x)}. \quad (3.11)$$

Soit $t > 0$. Considérons la fonction $f : x \mapsto P(x)e^{-\pi t(x \cdot x)}$. D'après Théorème 3.1.1, sa transformée de Fourier $\hat{f}$ est donnée par : $\hat{f} : y \mapsto i^{-d} t^{-\frac{n}{2}-d} P(y) e^{-\frac{\pi}{t}(y \cdot y)}$. Ainsi, le réseau L étant unimodulaire (si bien que $L' = L$ et $\text{disc}(L) = 1$), la formule sommatoire de Poisson donne :

$$\sum_{x \in L} \hat{f}(x) = \sum_{y \in L} \hat{f}(y)$$

d'où, en utilisant l'expression de $\hat{f}$ et de f :

$$\sum_{x \in L} P(x) e^{-\pi t(x \cdot x)} = \sum_{x \in L} i^{-d} t^{-\frac{n}{2}-d} P(x) e^{-\frac{\pi}{t}(x \cdot x)},$$

qui est exactement la formule 3.11. Ainsi, on a donc prouvé le théorème :

Théorème 3.4.1. *Soit $L \subset \mathbb{R}^n$ un réseau unimodulaire pair, et P un polynôme harmonique homogène de degré $d \geq 0$. Alors, la formule :*

$$\forall z \in \mathbb{H}, \quad \theta_{L,P}(z) = \sum_{x \in L} e^{\pi i z(x \cdot x)}$$

définit une fonction holomorphe $\theta_{L,P}$ sur le demi-plan $\mathbb{H}$, qui est une forme modulaire de poids $\frac{n}{2} + d$.

Chapitre 4

Application à la théorie des réseaux

L'objectif de ce chapitre sera d'utiliser les séries thêta afin d'étudier les réseaux unimodulaires pairs. Nous allons principalement classifier les réseaux unimodulaires pairs en dimension 8 et 16. Pour y arriver, nous développeront aussi quelques outils pour étudier et construire ces réseaux.

4.1 Propriétés des réseaux

Nous allons tout d'abord présenter certaines propriétés qui simplifient l'étude et la construction des réseaux.

Proposition 4.1.1. *Soit $L \subset L^* \subset \mathbb{R}^n$ deux réseaux. Alors :*

$$\text{disc}(L) = [L^* : L]^2 \text{disc}(L^*)$$

Démonstration. D'après le théorème de la base adaptée, il existe une base $\mathbf{e} = (e_1, \dots, e_n)$ de L^* et des entiers (strictement positifs ici) $a_1, \dots, a_n$ tels que $(a_1 e_1, \dots, a_n e_n)$ est une base de L .

Alors d'un côté $[L^* : L] = a_1 \dots a_n$, et d'un autre : $\text{disc}(L) = a_1^2 \dots a_n^2 \text{disc}(L^*)$, d'où le résultat. $\square$

Ce résultat permet en particulier de relier l'indice d'un réseau entier dans son dual à son discriminant.

En effet remarquons d'abord que la condition L entier équivaut à $L \subset L'$. De plus les formules données précédemment sur le réseau dual montrent que $\text{disc}(L') = \frac{1}{\text{disc}(L)}$. La proposition 4.1.1 permet d'affirmer :

Proposition 4.1.2. *Soit $L \in \mathbb{R}^n$ un réseau entier. Alors :*

$$\text{disc}(L) = [L' : L]$$

Définition 4.1.3. Soit $L \in \mathbb{R}^n$ un réseau entier. On appelle résidu de L le groupe abélien fini de cardinal $\text{disc}(L) : L'/L$. On le note $\text{Res}(L)$

De façon générale, même si L est entier, il n'y a aucune raison a priori pour que L' le soit aussi. On peut alors considérer la forme $\mathbb{Z}$ -bilinéaire suivante :

$$\begin{aligned} (\cdot, \cdot) : \text{Res}(L) \times \text{Res}(L) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (x, y) &\longmapsto x \cdot y + \mathbb{Z}. \end{aligned}$$

Celle-ci est bien défini, car pour deux classes $x + L$, $y + L$, $x, y \in L'$, on a :

$$(x + L) \cdot (y + L) = x \cdot y + L \cdot y + L \cdot x + L \cdot L.$$

Les trois derniers termes étant à valeurs dans $\mathbb{Z}$, ceci assure que $(\cdot, \cdot)$ est bien définie. Alors les réseaux entiers Γ tels que $L \subset \Gamma \subset L'$ correspondent aux sous-modules totalement isotropes de $\text{Res}(L)$.

A présent supposons que l'on dispose d'un réseau entier L de discriminant $d^2 > 1$. On souhaite trouver un sur-réseau entier unimodulaire. d'après la proposition 4.1.1 et ci-dessus, on cherche donc les sous-modules totalement isotropes de $\text{Res}(L)$ d'indice d .

4.2 Construction de réseaux unimodulaires pairs

Commençons par construire les réseaux unimodulaires pairs de dimension 8 et 16. Partons d'un réseau unimodulaire présent en toute dimension : $\mathbb{Z}^n \subset \mathbb{R}^n$, noté aussi I_n . Il ne s'agit pas d'un réseau pair, mais on dispose d'un morphisme de groupe surjectif :

$$\begin{aligned} I_n &\longrightarrow \mathbb{Z}/2\mathbb{Z}, \\ x &\longmapsto x \cdot x. \end{aligned}$$

Son noyau est donc un sous-module de I_n d'indice 2, c'est à dire un réseau pair de discriminant 4. On le note D_n . Puisque dans $\mathbb{Z}/2\mathbb{Z}$, $x^2 = x$, on dispose de la caractérisation :

$$D_n = \{(x_1, \dots, x_n) \in I_n \mid \sum_{k=1}^n x_k = 0 \pmod{2}\}.$$

Puisque $\text{disc}(D_n) = 4$, $\text{Res}(D_n)$ est un groupe abélien fini d'ordre 4, il s'agit donc soit de $\mathbb{Z}/4\mathbb{Z}$, soit de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Par définition de D_n , on sait que $\varepsilon = \frac{1}{2}(1, \dots, 1) \in D'_n$. On a ensuite $2\varepsilon = (1, \dots, 1)$. On doit donc distinguer selon la parité de n .

-Si $n \equiv 0 \pmod{2}$, $2\varepsilon = 0 \pmod{D_n}$, donc $\text{Res}(D_n) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et on doit trouver un autre générateur. Or on dispose aussi de $e_1 = (1, 0, \dots, 0) \in D'_n \setminus D_n$. Puisque $D_n + e_1 \cup D_n = I_n$, $\varepsilon \notin D_n + e_1$, ce qui fournit un deuxième générateur de $\text{Res}(D_n)$. Le troisième est $\varepsilon - e_1 = \frac{1}{2}(-1, 1, \dots, 1)$. On notera D_n^+ le réseau correspondant au sous-groupe engendré par ε . C'est un réseau unimodulaire (pas forcément entier à ce stade). le réseau D_n^- obtenu à partir du sous-groupe engendré par $\varepsilon - e_1$ est isométrique à D_n^+ (par une réflexion).

-Si $n \equiv 1 \pmod{2}$, $2\varepsilon = e_1 \pmod{D_n}$, ce qui montre que $\text{Res}(D_n) = \mathbb{Z}/4\mathbb{Z}$, et que le seul réseau unimodulaire compris entre D_n et D'_n est I_n .

On ne peut donc obtenir un réseau unimodulaire pair de cette façon que si n est pair. Plaçons-nous dans ce cas, et calculons la forme bilinéaire $(\cdot, \cdot)$ définie précédemment. On utilise les générateurs e_1 et ε (dans cet ordre). Alors la matrice de cette forme dans cette base vaut :

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{n}{4} \end{pmatrix}.$$

Ainsi le réseau D_n^+ n'est entier que si n est un multiple de 4. Le morphisme :

$$\begin{aligned} D_n^+ &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\ x &\longmapsto x \cdot x \end{aligned}$$

se factorise en un morphisme $D_n^+/D_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$. Celui-ci est nul uniquement lorsque $\varepsilon \cdot \varepsilon = \frac{n}{4}$ est pair, c'est à dire lorsque n est multiple de 8.

Ceci fournit déjà une première famille infinie de réseaux unimodulaires pairs : D_{8k}^+ , $k \in \mathbb{N}^*$. On note en particulier $E_8 = D_8^+$, qui est donc le plus petit de ces réseaux. On verra qu'il s'agit à isométrie près de l'unique réseau unimodulaire pair en dimension 8.

On peut bien sûr également construire de nouveaux réseaux unimodulaires pairs comme sommes directes orthogonales de réseaux plus petits. Par exemple en dimension 16, on dispose à l'aide de la construction précédente de deux réseaux unimodulaires pairs :

- D_{16}^+ ,
- $E_8 \oplus E_8$.

Question : ces deux réseaux sont-ils isométriques ?

4.3 Utilisation de séries thêta

Soit $L \subset \mathbb{R}^n$ un réseau unimodulaire pair.

Une première idée pour classifier les réseaux est de déterminer la structure d'une ligne de niveau de la forme quadratique $x \cdot x$ à l'intérieur du réseau. Notons à cet effet $\mathcal{R}(2k) = \{x \in L \mid x \cdot x = 2k\}$ et $N_L(2k)$ son cardinal. On a vu que la série thêta associée à L peut être développée en puissances de $q = e^{2\pi iz}$ par :

$$\theta_L(q) = \sum_{k=0}^{\infty} N_L(2k)q^k = 1 + N_L(2)q + N_L(4)q^2 + \dots$$

et nous avons montré dans les chapitres 2 et 3 que θ_L est une forme modulaire de poids $\frac{n}{2}$. En particulier, les séries thêta θ_{E_8} , $\theta_{E_8 \oplus E_8}$, et $\theta_{D_{16}^+}$ sont modulaires de poids respectifs 4, 8, et 8.

Or nous avons vu dans le premier chapitre que les espaces de formes modulaires associées à ces poids sont de dimension 1. Le coefficient en q^0 étant fixé à 1, cela détermine entièrement

la fonction thêta.

On obtient donc les relations :

$$\begin{aligned}\theta_{E_8}(q) &= E_4(q) = 1 + 240q + 2160q^2 + \dots \\ \theta_{E_8 \oplus E_8}(q) &= \theta_{D_{16}^+}(q) = E_8(q) = E_4(q)^2 = 1 + 480q + 61920q^2 + \dots\end{aligned}$$

Mieux, la série thêta d'un réseau unimodulaire pair de rang 8 est toujours égale à celle de E_8 , et celle d'un réseau unimodulaire de rang 16 est toujours égale à celle de $E_8 \oplus E_8$.

À présent, nous savons que si L est un réseau unimodulaire pair de rang 8, $N_L(2k) = N_{E_8}(2k)$ pour tout $k \in \mathbb{N}$, et si L est de rang 16, $N_L(2k) = N_{E_8 \oplus E_8}(2k) = N_{D_{16}^+}(2k)$ pour tout $k \in \mathbb{N}$. Cependant on ne peut pas conclure a priori que les réseaux sont égaux pour autant. Pour cela il va falloir s'intéresser à la structure géométrique des ensembles $\mathcal{R}_L(2k)$. Notons particulièrement $\mathcal{R}_L = \mathcal{R}_L(2)$. Cet ensemble possède une structure géométrique particulièrement symétrique que l'on appelle un **système de racines**.

4.4 Systèmes de racines

On verra dans la suite que les réflexions jouent un rôle important dans l'étude des systèmes de racines. Ainsi si E est un espace euclidien, on notera σ_α la réflexion par rapport à $\alpha \in E \setminus \{0\}$.

Pour rappel, on a la formule explicite :

$$\forall \beta \in E, \sigma_\alpha(\beta) = \beta - 2 \frac{\beta \cdot \alpha}{\alpha \cdot \alpha} \alpha. \quad (4.1)$$

Définition 4.4.1. Soit E un espace euclidien de dimension ℓ . Un **système de racines** $\Phi \subset E$ de rang ℓ est un ensemble de vecteurs de E tel que :

- (i) $0 \notin \Phi$, Φ est fini et engendre E en tant qu'espace vectoriel.
- (ii) Si $\alpha \in \Phi$, les seuls multiples de α présents dans Φ sont $\pm\alpha$.
- (iii) Si $\alpha, \beta \in \Phi$, on a $\langle \alpha, \beta \rangle = 2 \frac{\alpha \cdot \beta}{\beta \cdot \beta} \in \mathbb{Z}$.
- (iv) Si $\alpha \in \Phi$, la réflexion par rapport à α préserve Φ : $\forall \beta \in \Phi, \sigma_\alpha(\beta) \in \Phi$.

Les éléments de Φ sont appelés **racines**.

Définition 4.4.2. On appelle groupe de Weyl de Φ et on note $\mathcal{W}$ le sous-groupe de $O(E)$ engendré par les réflexions $\sigma_\alpha, \alpha \in \Phi$.

On peut bien sûr pour cette nouvelle structure définir une notion de morphismes et d'isomorphismes. $u : \Phi \subset E \longrightarrow \Phi' \subset E'$ est un morphisme de systèmes de racines si u se prolonge en une application linéaire $E \longrightarrow E'$, et si u préserve l'application $\langle \cdot, \cdot \rangle$, soit $\langle u(\alpha), u(\beta) \rangle = \langle \alpha, \beta \rangle$ pour tous $\alpha, \beta \in \Phi$. u est un isomorphisme si son prolongement à E l'est. Par ailleurs un isomorphisme entre systèmes de racines induit un isomorphisme entre les groupes de Weyl $\sigma \in \mathcal{W} \longmapsto u \circ \sigma \circ u^{-1}$.

Remarquons qu'avec cette définition, les longueurs des racines n'importent pas dans l'absolu. En effet si Φ est un système de racines, le dilaté de Φ par un facteur non nul quelconque est un autre système de racines isomorphe. Cela signifie que les informations importantes dans un système de racines sont les angles entre les racines ainsi que les longueurs relatives entre elles.

De plus, la troisième condition de la définition impose que les angles entre deux racines sont des angles exceptionnels : ils ne peuvent valoir que l’une des valeurs $0, \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}, \pi$.

Les informations concernant ces angles et les longueurs pour deux racines α et β , avec $\|\beta\| \geq \|\alpha\|$ en fonction des valeurs de $\langle \alpha, \beta \rangle$ et $\langle \beta, \alpha \rangle$ sont résumées dans le tableau suivant :

$\langle \alpha, \beta \rangle$	$\langle \beta, \alpha \rangle$	θ	$\ \beta\ ^2 / \ \alpha\ ^2$
0	0	$\frac{\pi}{2}$	indéterminé
1	1	$\frac{\pi}{3}$	1
-1	-1	$\frac{2\pi}{3}$	1
1	2	$\frac{\pi}{4}$	2
-1	-2	$\frac{3\pi}{4}$	2
1	3	$\frac{\pi}{6}$	3
-1	-3	$\frac{5\pi}{6}$	3

Exemples

1/En dimension 1, il y a évidemment un unique système de racines, donné par $\Phi = \{\pm\alpha\}$ avec $\alpha \neq 0$ quelconque. On le note A_1 .

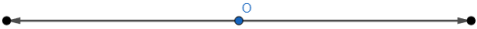


FIGURE 4.1 – Système de racines A_1

2/En dimension 2, on peut montrer en utilisant uniquement quelques outils donnés ci-dessous qu’il existe 4 systèmes de racines. On les représente ci-dessous :

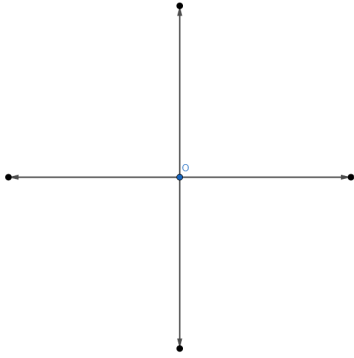
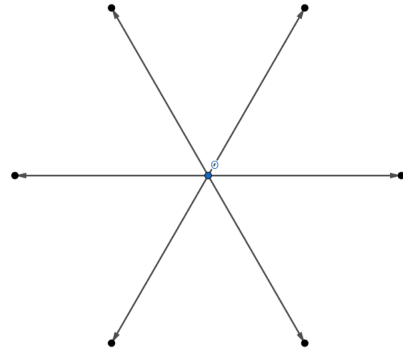
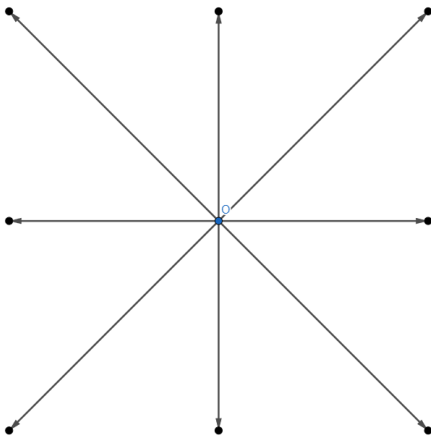
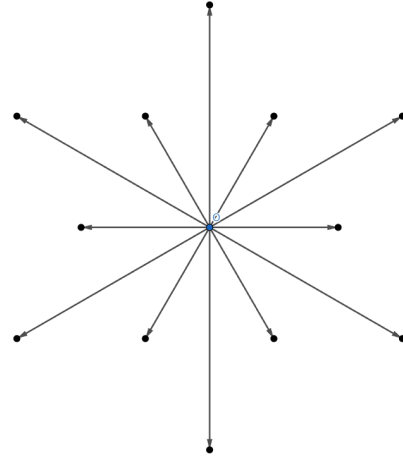
(a) Système de racines $A_1 \oplus A_1$ (b) Système de racines A_2 (c) Système de racines B_2 (d) Système de racines G_2

FIGURE 4.2 – Systèmes de racines en dimension 2

Revenons au cas des réseaux pairs. Fixons L un réseau pair. Alors pour $\alpha, \beta \in \mathcal{R}_L$ on a $\langle \alpha, \beta \rangle = \alpha \cdot \beta \in \mathbb{Z}$. On peut utiliser l'inégalité de Cauchy-Schwartz pour montrer de plus que $\langle \alpha, \beta \rangle$ ne peut valoir que $-2, -1, 0, 1, 2$, et les valeurs ± 2 ne sont prises que si $\beta = \pm \alpha$. Les stabilités par réflexions s'ensuivent par le fait que L est un réseau, la formule 4.1, et un calcul de norme :

$$\begin{aligned} \text{Si } \alpha \cdot \beta = 1 \quad \|\alpha - \beta\|^2 &= \|\alpha\|^2 + \|\beta\|^2 - 2\alpha \cdot \beta = 2 + 2 - 2 = 2 \\ \text{Si } \alpha \cdot \beta = -1 \quad \|\alpha + \beta\|^2 &= \|\alpha\|^2 + \|\beta\|^2 + 2\alpha \cdot \beta = 2 + 2 - 2 = 2. \end{aligned}$$

On en déduit que $\mathcal{R}_L$ est bien un système de racines, mais on remarque immédiatement que tous les systèmes de racines ne sont pas les systèmes de racines d'un réseau. En effet un réseau de rang 2 ne peut avoir B_2 ou G_2 comme système de racine, car toutes les racines du système de racines d'un réseau sont de même longueur. On dit que $\mathcal{R}_L$ est

de type ADE (terminologie inspirée de la classification des systèmes de racines, que l'on donne plus loin).

L'objectif principal de la théorie est de classifier les systèmes de racines. Pour cela on fait lien entre les systèmes de racines de rang ℓ et un type particulier de diagrammes à ℓ sommets, appelé diagrammes de Dynkin. Ces objets sont plus simples à étudier, mais le lien entre système de racine et diagramme de Dynkin n'est pas évident et demande un certain développement.

Un traitement complet de ces objets nous emmènerait cependant trop loin par rapport à notre sujet initial, à savoir la classification des réseaux de dimension 8 et 16. On se contentera donc d'annoncer les résultats principaux, et pour un traitement plus complet de ce sujet nous renvoyons à *Introduction to Lie Algebras and Representations* par James E. Humphreys.

Définition 4.4.3. Soit $\Delta \subset \Phi$. On dit que Δ est **une base de Φ** si :

- (i) Δ est une base de E en tant que $\mathbb{R}$ -espace vectoriel.
- (ii) Toute racine β s'écrit comme une combinaison linéaire à coefficients entiers de racines de Δ , et dont les coefficients sont soit tous positifs, soit tous négatifs.

Les racines de Δ sont dites **simples**. Similairement les réflexions par rapport à une racine simple sont aussi appelée **simples**.

Lorsque l'on dispose d'une base Δ de Φ , toute racine β s'écrit comme une combinaison linéaire à coefficients entiers tous positifs (ou tous négatifs) des racines simples, on peut donc parler de racines **positives** (resp. **négatives**), et on note $\beta \succ 0$ (resp. $\beta \prec 0$). On note Φ^+ (resp. Φ^-) l'ensemble des racines positives (resp. négatives) de Φ .

Remarque 4.4.4. Si α, β sont deux racines simples, on vérifie que $\alpha \cdot \beta \leq 0$ (sinon $\alpha - \beta$ serait une racine, ni positive ni négative donc). L'angle entre α et β est donc obtu.

Théorème 4.4.5. *Tout système de racine possède une base*

Théorème 4.4.6. *Soit Φ un système de racine dont on fixe une base Δ . On note $\mathcal{W}$ son groupe de Weyl.*

- (i) $\mathcal{W}$ agit simplement transitivement sur l'ensemble des bases de Φ .
- (ii) $\mathcal{W}$ est engendré par les réflexions simples.
- (iii) Pour toute racine β , il existe $\sigma \in \mathcal{W}$ tel que $\sigma(\beta) \in \Delta$.

Le fait que $\mathcal{W}$ agit transitivement sur les bases par isométries permet de définir sans ambiguïté la notion de matrice de Cartan et de faire le lien annoncé entre systèmes de racines et diagrammes de Dynkin.

Définition 4.4.7. On appelle **matrice de Cartan** de Φ la matrice formée des coefficients $\langle \alpha_i, \alpha_j \rangle$, où $\alpha_1 \dots \alpha_\ell$ est une base quelconque de Φ . Ces coefficients sont appelés **entiers de Cartan**.

Bien sûr l'expression de la matrice de Cartan de Φ dépend de l'ordre que l'on choisit pour les racines simples, cependant le fait que le groupe de Weyl de Φ agit transitivement sur les bases de Φ assure que cette expression ne dépend pas de la base choisie, si l'on choisit le bon ordre.

On a même mieux : un système de racine est entièrement caractérisé par sa base et sa matrice de Cartan, ce qu'exprime la proposition suivante :

Proposition 4.4.8. *Soit $\Phi \subset E$, $\Phi' \subset E'$ deux systèmes de racines. On fixe $\Delta = (\alpha_1, \dots, \alpha_\ell)$ une base de Φ et $\Delta' = (\alpha'_1, \dots, \alpha'_\ell)$ une base de Φ' . On suppose que $\langle \alpha_i, \alpha_j \rangle = \langle \alpha'_i, \alpha'_j \rangle$ pour tous $1 \leq i, j \leq \ell$. Alors la bijection ϕ envoyant α_i sur α'_i se prolonge en un isomorphisme entre Φ et Φ' .*

Démonstration. Comme Δ et Δ' sont des bases des espaces euclidiens E et E' , ϕ se prolonge naturellement en un isomorphisme d'espaces vectoriels.

Fixons $\alpha, \beta \in \Delta$ des racines simples. Alors :

$$\sigma_{\phi(\alpha)}(\phi(\beta)) = \sigma_{\alpha'}(\beta') = \beta' - \langle \beta', \alpha' \rangle \alpha' = \phi(\beta) - \langle \beta, \alpha \rangle \phi(\alpha) = \phi(\beta - \langle \beta, \alpha \rangle \alpha) = \phi(\sigma_\alpha(\beta)).$$

On en déduit que l'on a $\phi \circ \sigma_\alpha \circ \phi^{-1} = \sigma_{\phi(\alpha)} = \sigma_{\alpha'}$. Comme les réflexions simples engendrent les groupes de Weyl respectifs $\mathcal{W}$ et $\mathcal{W}'$, on dispose d'un isomorphisme de groupe $\sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$.

A présent soit $\beta \in \Phi$. On peut fixer $\sigma \in \mathcal{W}$ tel que $\alpha = \sigma^{-1}(\beta) \in \Delta$. Alors $\phi(\beta) = (\phi \circ \sigma \circ \phi^{-1})(\phi(\alpha)) \in \Phi'$. On en déduit que l'on a bien $\phi(\Phi) \subset \Phi'$, et que ϕ est surjective (même raisonnement avec ϕ^{-1} . Enfin, si β, α sont des racines quelconques de Φ , on fixe $\sigma \in \mathcal{W}'$ tel que $\sigma(\phi(\beta)) \in \Delta$, puis on calcule :

$$\begin{aligned} \langle \phi(\alpha), \phi(\beta) \rangle &= \langle (\sigma \circ \phi)(\alpha), (\sigma \circ \phi)(\beta) \rangle \\ ((\sigma \circ \phi)(\beta) \text{ est simple}) &= \langle (\phi^{-1} \circ \sigma \circ \phi)(\alpha), (\phi^{-1} \circ \sigma \circ \phi)(\beta) \rangle \\ &= \langle \alpha, \beta \rangle. \end{aligned}$$

□

La proposition ci-dessus montre donc que la matrice de Cartan d'un système de racine le détermine à isomorphisme près. On peut par ailleurs résumer les informations de cette matrice à l'aide d'un graphe, appelé **diagramme de Dynkin**. Pour comprendre ces objets, nous commencerons par définir les diagrammes de Coxeter, qui sont très proches des diagrammes de Dynkin.

On construit le diagramme de Coxeter de Φ , dont les sommets sont les racines d'une base de Φ . On relie ensuite deux racines simples distinctes par un nombre d'arrêtes dépendant de l'angle obtus (θ) formé par les deux racines. Ce nombre d'arrête et la façon de les représenter sont résumés dans le tableau suivant :

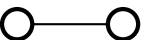
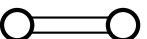
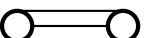
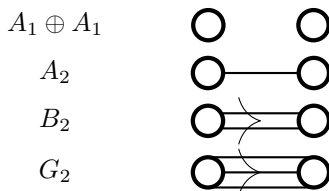
θ	arrête
$\frac{\pi}{2}$	
$\frac{2\pi}{3}$	
$\frac{3\pi}{4}$	
$\frac{5\pi}{6}$	

TABLE 4.1 – Règles de construction des diagrammes de Coxeter

On forme le diagramme de Dynkin en ajoutant simplement une flèche sur les arrêtes doubles ou triples, où la flèche pointe vers la racine la plus courte.

Exemple

Voici les diagrammes de Dynkin des systèmes de racines de dimension 2 :



Avant de commencer la classification de ces diagrammes, nous allons simplifier le problème pour se limiter à l'étude des diagrammes connexes

Définition 4.4.9. Un système de racines Φ est **réductible** s'il existe deux sous-systèmes de racines Φ_1 et Φ_2 orthogonaux tels que $\Phi = \Phi_1 \cup \Phi_2$. Dans le cas contraire, Φ est **irréductible**.

On en déduit par récurrence sur le rang du système de racines :

Proposition 4.4.10. Soit Φ un système de racines. Alors il existe des systèmes de racines irréductibles $\Phi_1, \dots, \Phi_k$ orthogonaux deux à deux tels que $\Phi = \bigcup_{i=1}^k \Phi_i$.

On a de plus la caractérisation suivante :

Proposition 4.4.11. Soit $\Phi \subset E$ un système de racines et Δ une base de Φ . Alors Φ est irréductible si et seulement si Δ ne peut être partitionné en deux ensembles de racines orthogonaux.

Démonstration. Si $\Phi = \Phi_1 \cup \Phi_2$, on obtient aussi une partition de Δ en deux ensembles orthogonaux. Ainsi si $\Delta \subset \Phi_1$, Δ est orthogonal à Φ_2 , mais comme Δ est une base de E , et que $0 \notin \Phi_2$, Φ_2 est vide. Ceci prouve une implication.

Dans l'autre sens, si $\Delta = \Delta_1 \cup \Delta_2$ orthogonaux, comme toute racine de Φ est conjugué à une racine simple par le groupe de Weyl, on considère Φ_i l'ensemble des racines conjuguées à un élément de Δ_i . Comme Δ_1 et Δ_2 sont orthogonaux et que le groupe de Weyl agit par isométries, Φ_1 et Φ_2 sont orthogonaux. Ainsi $\Phi = \Phi_1 \cup \Phi_2$ est une partition en ensembles orthogonaux. De plus Δ_i est une base de Φ_i , car le groupe de Weyl est engendré par les réflexions simples, puis on utilise la formule d'une réflexion. Si maintenant l'un des Φ_i est vide, alors l'un des Δ_i aussi. □

A partir de cette caractérisation, il est clair qu'un système de racines est irréductible si son diagramme de Coxeter est connexe.

On dira qu'un diagramme de Coxeter est **admissible** s'il existe un espace euclidien E et une base formée de vecteurs unitaires $(e_1, \dots, e_\ell)$ et tels que les angles entre ces vecteurs sont donnés par le diagramme. Nous allons à présent classier tous les diagrammes de Coxeter connexes admissibles.

Bien sûr tous les diagrammes de Coxeter associés à un système de racines sont admissibles.

On notera Γ un diagramme de Coxeter connexe. La preuve se déroule en plusieurs étapes :

(1) Si un diagramme de Coxeter est admissible, tous les sous-graphes obtenus en enlevant un certain nombre de sommets et uniquement les arêtes partant de ces sommets le sont

aussi. Il suffit pour cela d'enlever les vecteurs correspondants de la base donnée par le diagramme.

(2) Le nombre de paires de sommets reliés par au moins une arête est strictement inférieur à n . En effet posons : $\varepsilon = \sum_{i=1}^{\ell} e_i$, vecteur non nul car les e_i forment une base de E . Alors $\varepsilon \cdot \varepsilon > 0$.

Or $\varepsilon \cdot \varepsilon = n + 2 \sum_{i < j} e_i \cdot e_j$, avec $e_i \cdot e_j \leq -1$ pour tous $1 \leq i, j \leq \ell$. D'où le résultat.

(3) Γ ne contient pas de cycle. Sinon on pourrait considérer le sous-graphe constitué de ce cycle par l'étape (1), qui est donc admissible, mais ceci contredirait l'étape (2).

(4) Si ε est un sommet de Γ , pas plus de 3 arêtes (comptées avec les multiplicités) ne peuvent être reliées à ε . En effet notons $e_1, \dots, e_k$ les sommets reliés à ε . Puisque Γ ne contient pas de cycle, $e_i \cdot e_j = 0$ si $i \neq j$. La projection orthogonale de ε sur l'espace engendré par $e_1, \dots, e_k$ est de norme plus petite que celle de ε . D'où :

$$\begin{aligned} 1 = \varepsilon \cdot \varepsilon &> \sum_{i=1}^k (e_i \cdot \varepsilon)^2 \\ 4 &> \sum_{i=1}^k 4(e_i \cdot \varepsilon)^2 \end{aligned}$$

Or le nombre d'arêtes entre e_i et ε est donné par $4(e_i \cdot \varepsilon)^2$, ce qui prouve le résultat énoncé.

(5) Le seul diagramme de Coxeter ayant une arête triple est celui de G_2 : $\bigcirc \equiv \bigcirc$. C'est une conséquence immédiate de (4).

(6) Supposons que l'on dispose d'un sous-graphe $\bigcirc \text{---} \bigcirc \text{---} \dots \text{---} \bigcirc \text{---} \bigcirc$ de Γ . Alors le graphe obtenu en remplaçant cette chaîne par un unique point est encore admissible. En effet si $e_1, \dots, e_k$ sont les vecteurs associés aux sommets de cette chaîne, on pose $\varepsilon = \sum_{i=1}^k e_i$.

Alors :

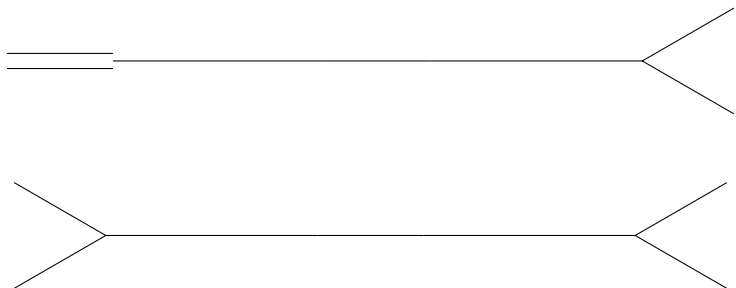
$$\begin{aligned} (\varepsilon \cdot \varepsilon)^2 &= n + 2 \sum_{i < j} e_i \cdot e_j \\ &= n - (n - 1) = 1 \end{aligned}$$

$$\text{Car } e_i \cdot e_j = \begin{cases} -\frac{1}{2} & \text{Si } i \text{ et } j \text{ sont consécutifs} \\ 0 & \text{Sinon} \end{cases}$$

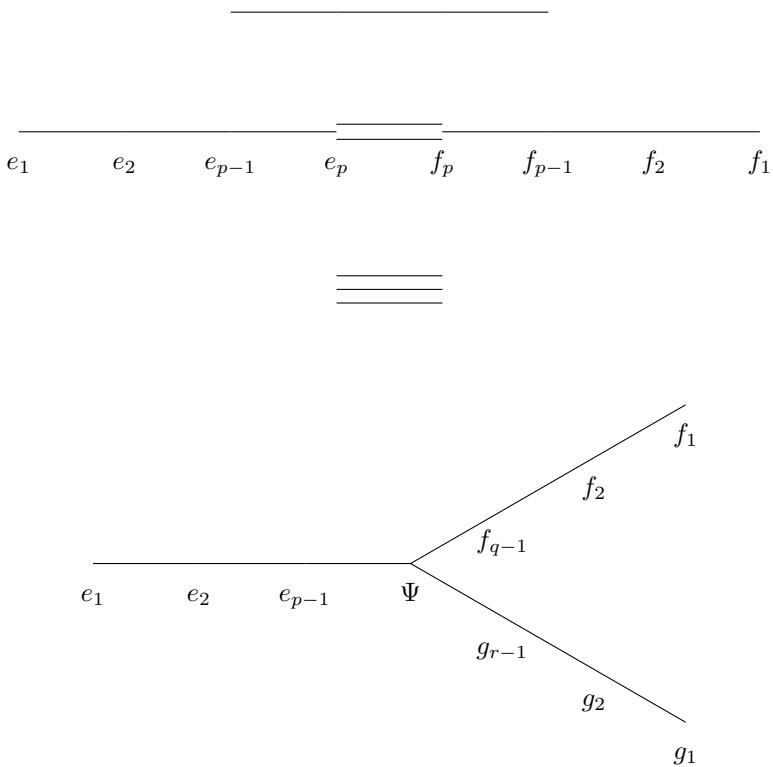
On vérifie aussi aisément que les produits scalaires avec les autres sommets sont conservés, car il n'y a pas de cycles donc les autres sommets du graphe Γ ne sont reliés qu'à au plus un sommet de la chaîne.

(7) Les diagrammes suivant ne sont pas admissibles :





En effet on pourrait sinon réduire la chaîne centrale à un point et obtenir un nouveau diagramme admissible, ce qui contredirait (4).
On en déduit que Γ contient au plus une double arrête ou embranchement par (1).
(8) les cas connexes restant sont les suivants :



Cela suit de (5), (3), et (7).
(9) On se place dans le cas 2. On pose :

$$e = \sum_{i=1}^p i e_i \quad , \quad f = \sum_{i=1}^q i f_i$$

Comme $e_i \cdot e_j = 0$ sauf $e_i \cdot e_{i+1} = -\frac{1}{2}$, on obtient :

$$\begin{aligned} e \cdot e &= \sum_{i=1}^p i^2 - \sum_{i=1}^p i(i+1) \\ &= \frac{p(p+1)}{2} \\ f \cdot f &= \frac{q(q+1)}{2} \end{aligned}$$

De plus $(e \cdot f)^2 = \frac{p^2 q^2}{2}$. En appliquant l'inégalité de Cauchy-Schwartz, sachant que e et f ne sont pas proportionnels, on obtient :

$$\frac{p^2 q^2}{2} = (e \cdot f)^2 < (e \cdot e)(f \cdot f) = \frac{p(p+1)q(q+1)}{4}$$

Soit en réarrangeant :

$$(p-1)(q-1) < 2$$

On en déduit que soit $p = q = 2$, soit p ou $q = 1$, et l'autre est quelconque.

(10) Dans le cas 4 de (8), On pose :

$$e = \sum_{i=1}^{p-1} i e_i, \quad f = \sum_{i=1}^{q-1} i f_i, \quad g = \sum_{i=1}^{r-1} i g_i.$$

Par le même calcul que ci-dessus, $e \cdot e = \frac{p(p-1)}{2}$, $f \cdot f = \frac{q(q-1)}{2}$, $g \cdot g = \frac{r(r-1)}{2}$. Notons $\theta_1, \theta_2, \theta_3$ les angles respectifs entre Φ et e, f, g . Comme e, f, g sont orthogonaux deux à deux, on obtient en considérant la norme de la projection de Φ sur l'espace engendré par e, f, g : $\cos^2(\theta_1) + \cos^2(\theta_2) + \cos^2(\theta_3) < 1$. Or on a :

$$\begin{aligned} \cos^2(\theta_1) &= \frac{(e \cdot \Phi)^2}{(e \cdot e)(\Phi \cdot \Phi)} \\ &= \frac{1}{4} \frac{2(p-1)^2}{p(p-1)} \\ &= \frac{1}{2} \left(1 - \frac{1}{p}\right). \end{aligned}$$

En additionnant les inégalités, il vient : $1 > \frac{1}{2} \left(3 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r}\right)$. Ce qui se réécrit :

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1 \tag{4.2}$$

On peut alors traiter les différents cas en supposant, sans perte de généralité, que $p \geq q \geq r$ ($\geq \frac{1}{2}$). Avec cette inégalité et la précédente, on a déjà $\frac{3}{r} > 1$, donc $r = 2$. On discute ensuite suivant la valeur de q :

-Si $q = 2$, tout p convient.

-Si $q = 3$, on obtient $\frac{1}{p} > \frac{1}{6}$, donc $3 \leq p \leq 5$.

-Si $q \geq 4$, comme on a aussi $p \geq q \geq 4$, l'inégalité 4.2 ne peut être satisfaite.

Ceci conclut la réduction des cas. Il resterait encore à montrer que les diagrammes que nous n'avons pas éliminés sont en effet admissibles. Mais avant, observons la classification des diagrammes de Dynkin admissibles que nous avons obtenue. On rappelle que pour passer d'un diagramme de Coxeter à un diagramme de Dynkin, on ajoute des flèches aux arrêtes multiples. A cause de la symétrie de la plupart des diagrammes, cela ne rajoute en fait qu'une famille infinie de diagrammes de Dynkin par rapport aux diagrammes de Coxeter. Voici la classification obtenue :

type	diagramme de Dynkin
$A_\ell (\ell \geq 1)$	
$B_\ell (\ell \geq 2)$	
$C_\ell (\ell \geq 3)$	
$D_\ell (\ell \geq 4)$	
E_6	
E_7	
E_8	
F_4	
G_2	

TABLE 4.2 – Classification des diagrammes de Dynkin admissibles

Afin de revenir aux systèmes de racines, il reste donc à montrer que tous les diagrammes précédents sont bien les diagrammes de Dynkin d'un système de racine, et en effet, on a le :

Théorème 4.4.12. *La classification obtenue est complète. C'est à dire que tous les diagrammes de Dynkin restants sont admissibles, et tout diagramme de Dynkin est le diagramme d'un système de racine irréductible.*

Démonstration. Nous allons nous contenter de démontrer le théorème pour les diagrammes de type A, D, E , car ce sont les seuls que l'on rencontre dans l'étude des réseaux.

- A_ℓ : On considère $\mathbb{Z}^{\ell+1} \subset \mathbb{R}^{\ell+1}$, munis de la base canonique notée $(e_1, \dots, e_\ell)$. on pose $e = (1, 1, \dots, 1)$, et on considère le réseau $A_\ell = \mathbb{Z}^{\ell+1} \cap e^\perp$. Ce réseau est engendré par les ℓ vecteurs linéairement indépendants : $e_1 - e_2, e_2 - e_3, \dots, e_\ell - e_{\ell+1}$. Son système de racines est onstitué des vecteurs $\pm(e_i - e_j)$, pour $i \neq j$. Comme $e_i - e_j = (e_i - e_{i+1}) + \dots + (e_{j-1} - e_j)$ pour $i < j$, la base précédente est aussi une base du système de racines de A_ℓ , et on voit immédiatement que son diagramme de Dynkin est celui voulu. Ce système de racines

possède donc au total $\ell(\ell + 1)$ racines.

- D_ℓ Le réseau D_ℓ déjà construit a comme racines les $\pm e_i \pm e_j$, $1 \leq i < j \leq \ell$, ce qui constitue au total $2\ell(\ell - 1)$ racines. Une base est donnée par $e_1 - e_2, \dots, e_{\ell-1} - e_\ell, e_{\ell-1} + e_\ell$. Le diagramme de Dynkin est celui voulu.

- E_6, E_7, E_8 : on utilise le fait que l'inclusion d'un diagramme dans un autre induit l'inclusion des systèmes de racines correspondants. On construit donc uniquement E_8 , qui est bien sûr le système de racines du réseau de même nom. Les racines sont soit de la forme $\pm e_i \pm e_j$, $i \neq j$, soit de la forme $\frac{1}{2}(\pm 1, \dots, \pm 1)$, où le nombre de signes $-$ est pair. on dénombre au total 112 racines de premier type, et $2^7 = 128$ du deuxième type. Une base est donnée par les vecteurs : $\frac{1}{2}(e_1 + e_8 - (e_2 + \dots + e_7))$, $e_1 + e_2, e_2 - e_1, e_3 - e_2, e_4 - e_3, e_5 - e_4, e_6 - e_5, e_7 - e_6$. $\square$

On définit par ailleurs pour tout système de racines Φ de rang ℓ le **nombre de Coxeter** par :

$$h = \frac{|\Phi|}{\ell}$$

On résume les informations obtenues dans le tableau suivant (on ajoute aussi la structure des groupes L'/L pour les réseaux correspondants) :

type	nombre de racines	nombre de Coxeter	L'/L
A_ℓ	$\ell(\ell + 1)$	$\ell + 1$	$\mathbb{Z}/(\ell + 1)\mathbb{Z}$
$D_\ell, \ell \geq 4$	$2\ell(\ell - 1)$	$2(\ell - 1)$	$\mathbb{Z}/4\mathbb{Z}$ ℓ impair $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ℓ pair
E_6	72	12	$\mathbb{Z}/3\mathbb{Z}$
E_7	126	18	$\mathbb{Z}/2\mathbb{Z}$
E_8	240	30	0

4.5 Classification des réseaux unimodulaires pairs de rang 8 et 16

Nous sommes prêts à obtenir la classification des réseaux unimodulaires pairs en dimension 8 et 16, et même d'obtenir quelques résultats en dimension 24 !

En effet nous savons que tout système de racine provenant d'un réseau unimodulaire pair en dimension 8 (resp. 16) admet 240 (resp. 480) racines. Ceci n'est cependant pas suffisant à moins d'utiliser des arguments combinatoires fastidieux. Afin de compléter la classification nous allons également avoir besoin du nombre de Coxeter. Pour cela nous allons utiliser une série thêta harmonique :

On pose pour $y \in \mathbb{R}^n$:

$$P(x) = (x \cdot y)^2 - \frac{(x \cdot x)(y \cdot y)}{n}$$

Proposition 4.5.1. *P est un polynôme harmonique homogène de degré 2.*

Démonstration. Il est clair que P est homogène de degré 2. Puis :

$$\begin{aligned}\Delta P(x) &= \sum_i \frac{\partial^2}{\partial x_i^2} \left((x \cdot y)^2 - \frac{(x \cdot x)(y \cdot y)}{n} \right) \\ &= \sum_i 2y_i^2 - \sum_i 2 \frac{y \cdot y}{n} \\ &= 2y \cdot y - 2y \cdot y \\ &= 0\end{aligned}$$

□

On se place dans les cas $n = 8, 16, 24$. Alors si L est un réseau unimodulaire pair de rang n , la série thêta $\theta_{L,P}$ est une forme parabolique de poids 6, 10 ou 14. Les espaces de formes paraboliques associés à ces poids sont tous nuls, on obtient donc :

Proposition 4.5.2. *Soit $n = 8, 16, 24$, et $L \subset \mathbb{R}^n$ un réseau unimodulaire pair. Alors pour tout $y \in \mathbb{R}^n$:*

$$\sum_{x \in \mathcal{R}_L} (x \cdot y)^2 = \frac{2|\mathcal{R}_L|(y \cdot y)}{n} \quad (4.3)$$

Corollaire 4.5.3. *Soit $\mathcal{R}_L = \emptyset$, soit $\mathcal{R}_L$ engendre $\mathbb{R}^n$*

Démonstration. Si $\mathcal{R}_L$ n'engendre pas $\mathbb{R}^n$, alors son orthogonal contient un vecteur non nul y . En appliquant la proposition à y , il vient $|\mathcal{R}_L| = 0$. □

L'objectif à présent sera de déterminer le nombre de Coxeter des composantes irréductibles du système de racines de L . On obtiendra pour cela la proposition remarquable suivante :

Proposition 4.5.4. *Toutes les composantes irréductibles du système de racines de $\mathcal{R}_L$ ont même nombre de Coxeter h , et ce nombre vaut : $h = \frac{|\mathcal{R}_L|}{n}$.*

Pour cela on commence par appliquer 4.3 à une racine y quelconque d'une composante irréductible Φ de $\mathcal{R}_L$. On obtient :

$$\sum_{x \in \Phi} (x \cdot y)^2 = \frac{4|\mathcal{R}_L|}{n} \quad (4.4)$$

On doit maintenant faire le lien entre le membre de gauche et le nombre de Coxeter de Φ . Nous avons d'abord besoin de quelques lemmes.

Lemme 4.5.5. *Soit $\Phi \subset E$ un système de racines irréductible de type ADE de groupe de Weyl $\mathcal{W}$. Alors $\mathcal{W}$ agit de façon irréductible sur E .*

Démonstration. Soit U un sous-espace de E stable par $\mathcal{W}$. Comme $\mathcal{W}$ agit par isométries, son orthogonal $U^\perp$ est aussi stable par $\mathcal{W}$. Supposons que U ne contient pas une racine $\alpha \in \Phi$. Alors pour $u \in U$, comme $\sigma_\alpha(u) \in U$, on obtient $u - \langle u, \alpha \rangle \alpha \in U$. Comme $\alpha \notin U$, ceci impose $u \cdot \alpha = 0$. Ainsi $\alpha \in U^\perp$. On en déduit que toute racine est soit dans U soit dans $U^\perp$. Ainsi on obtient une décomposition de Φ en deux systèmes de racines orthogonaux, donc l'un des deux est vide. Comme Φ engendre E , soit U , soit $U^\perp$ est égal à E . □

Lemme 4.5.6. *Soit Φ un système de racine et $\mathcal{W}$ son groupe de Weyl. On suppose que $\mathcal{W}$ agit de façon irréductible sur E . Alors :*

- (i) *Tout endomorphisme qui commute avec $\mathcal{W}$ est une homothétie.*
- (ii) *Toute forme bilinéaire sur E invariante par $\mathcal{W}$ est un multiple du produit scalaire canonique.*

Démonstration. (i) Soit u un tel endomorphisme. Alors u laisse invariant la droite $\mathbb{R}\alpha$, $\alpha \in \Phi$ quelconque, car il s'agit du noyau de $\sigma_\alpha + 1$. Ainsi u agit sur cette droite par une homothétie de rapport λ . Alors le noyau de $u - \lambda 1$ est un sous-espace invariant par $\mathcal{W}$ non nul, il est donc égal à E .

(ii) Fixons d'abord un endomorphisme u tel que $b(x, y) = u(x) \cdot y$ pour $x, y \in E$. Alors pour $\alpha \in \Phi$, $x, y \in E$:

$$\begin{aligned} \sigma_\alpha(u(x)) \cdot y &= u(x) \cdot \sigma_\alpha(y) \\ &= b(x, \sigma_\alpha(y)) \\ &= b(\sigma_\alpha(x), y) \\ &= u(\sigma_\alpha(x)) \cdot y \end{aligned}$$

On en déduit que u commute avec $\mathcal{W}$, donc par le point (i), u est une homothétie, ce qui démontre le résultat. $\square$

Proposition 4.5.7. *Soit $\Phi \subset E$ un système de racines irréductible, de groupe de Weyl $\mathcal{W}$. Alors pour tout $y \in E$:*

$$\sum_{x \in \Phi} (x \cdot y)^2 = 2h(y \cdot y) \quad (4.5)$$

Démonstration. On considère le polynôme harmonique homogène de degré 2 suivant :

$$P(y) = \sum_{x \in \Phi} \left((x \cdot y)^2 - \frac{(x \cdot x)(y \cdot y)}{n} \right)$$

Grâce à la sommation, P est même invariant par $\mathcal{W}$. P définit donc une forme quadratique invariante par $\mathcal{W}$, donc P est un multiple de la forme quadratique $(y \cdot y)$ par le lemme. En comparant les laplaciens, on en déduit que P est nul. La proposition en suit immédiatement. $\square$

On obtient la proposition 4.5.4 en égalisant 4.5 et 4.4.

Proposition 4.5.8. *Les composantes irréductibles du système de racines d'un réseau unimodulaire pair de rang 8 (ou 16) ont pour nombre de Coxeter 30.*

Démonstration. Le système de racines correspondant a 240 (resp. 480) racines, puis on utilise la proposition 4.5.4. $\square$

Nous sommes enfin prêts à classifier les réseaux unimodulaires pairs en dimension 8 et 16 :

Théorème 4.5.9. (i) *Il existe à isométrie près un unique réseau unimodulaire pair de rang 8 : E_8 .*

(ii) *Il existe à isométrie près deux réseaux unimodulaires pairs de rang 16 distincts : $E_8 \oplus E_8$ et D_{16}^+*

Démonstration. Soit L un réseau unimodulaire pair de rang 8 (resp. 16). (i) Le seul système de racines de rang ≤ 8 ayant un nombre de Coxeter égal à 30 est E_8 , donc L a pour système de racines E_8 , et donc contient le réseau E_8 . Comme E_8 est unimodulaire, $L = E_8$. (ii) Cette fois il y a deux systèmes de racines de rang au plus 16 : E_8 et D_{16} . Ainsi le système de racine de L vaut soit $E_8 \oplus E_8$, soit D_{16} . L contient donc les réseaux correspondant. On distingue les cas :

-Si $\mathcal{R}_L = E_8 \oplus E_8$, alors L contient le réseau correspondant qui est unimodulaire, donc $L = E_8 \oplus E_8$.

-Si $\mathcal{R}_L = D_{16}$, alors $D_{16} \subset L \subset D'_{16}$. Or on a déjà analysé ce cas : il y a exactement 3 réseaux unimodulaires satisfaisant cette condition : I_n , D_{16}^+ et D_{16}^- . Seul les deux derniers sont pairs, et isométriques par une réflexion, ce qui conclut.

Bien sûr $E_8 \oplus E_8$ et D_{16}^+ ne sont pas isométriques car leurs systèmes de racines diffèrent. $\square$

Chapitre 5

Formes modulaires de niveaux supérieurs

Dans cette section, on va s'intéresser à des fonctions holomorphes de $\mathbb{H}$ dans $\mathbb{C}$ qui sont "proches" d'être des formes modulaires pour $SL_2(\mathbb{Z})$: les formes modulaires de niveaux supérieurs. En fait, l'équation fonctionnelle définissant les formes modulaires sera pour ces fonctions vérifiée seulement pour des matrices appartenant à un certain sous-groupe d'indice fini de $SL_2(\mathbb{Z})$. Les sous-groupes de $SL_2(\mathbb{Z})$ qui apparaîtront à cette occasion seront appelés "sous-groupes de congruences".

5.1 Sous-groupes de congruences et formes modulaires

On introduit dans cette section les fameux sous-groupes de congruences de $SL_2(\mathbb{Z})$.

5.1.1 Définitions et premières propriétés

Commençons par la définition des sous-groupes de congruences de $SL_2(\mathbb{Z})$.

Définition 5.1.1. Pour tout entier $N \geq 1$, on définit le **sous-groupe de congruence d'ordre N de $SL_2(\mathbb{Z})$** par :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) , \ c \equiv 0 \pmod{N} \right\}$$

Il est aisé de vérifier que ceci définit un sous-groupe de $SL_2(\mathbb{Z})$, qui est d'indice fini dans $SL_2(\mathbb{Z})$.

Afin de mieux comprendre la dynamique de ces sous-groupes, on va s'intéresser de plus près à l'exemple de $N = 4$. Ce choix de 4 n'est évidemment pas anodin, puisque les remarques que nous ferons ici sur $\Gamma_0(4)$ nous permettront ultimement de démontrer le célèbre théorème des quatre carrés de Lagrange à l'aide de la théorie des formes modulaires de niveau supérieur (plus précisément, de niveau 4).

Explicitons sans plus tarder des générateurs de $\Gamma_0(4)$:

Proposition 5.1.2. *Le groupe $\Gamma_0(4)$ est engendré par les trois matrices $T, -T, R$ où on a posé :*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Démonstration. Soit $A \in \Gamma_0(4)$ qu'on note sous la forme :

$$A = \begin{pmatrix} a & b \\ 4c & d \end{pmatrix}$$

avec $a, b, c, d \in \mathbb{Z}$. On veut montrer que A appartient au sous-groupe de $\Gamma_0(4)$ engendré par R et T .

Dans un premier temps, supposons que $c = 0$. Alors, $1 = \det(A) = ab$ donc $a = b = 1$ ou $a = b = -1$. Dans le premier cas, A est une puissance entière de T , et dans le second cas, $-TA$ est de la forme du premier cas, donc est une puissance entière de T .

On passe au cas général où $c \neq 0$. Soit donc :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4).$$

Par récurrence, on peut supposer que toute matrice

$$A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(4)$$

vérifiant $|c'| < |c|$ est dans le sous groupe engendré par $T, -T, R$.

Alors, comme c est non nul, l'algorithme de division euclidienne fournit $k \in \mathbb{Z}$ tel que $|d + kc| \leq \frac{|c|}{2}$ (il suffit de prendre pour k l'entier le plus proche de $\frac{d}{c}$). En fait, comme d est impair (car c est pair et $ad - bc = 1$) et c multiple de 4, l'égalité $d + kc = \pm \frac{c}{2}$ ne peut avoir lieu, et on a donc même $|d + kc| < \frac{|c|}{2}$.

On considère alors

$$A' = AT^k = \begin{pmatrix} a & ak + b \\ c & ck + d \end{pmatrix} = \begin{pmatrix} a & e \\ c & f \end{pmatrix}$$

avec $|f| < \frac{|c|}{2}$. Maintenant, on peut trouver $k' \in \mathbb{Z}$ tel que $|c + k'(4f)| \leq 2|f| < |c|$ (prendre pour k' l'entier le plus proche de $\frac{c}{4f}$, f étant non nul car impair car d est impair et c pair). On calcule alors :

$$A'' = A'R^{k'} = \begin{pmatrix} a + 4k'c & e \\ c + 4k'f & f \end{pmatrix}.$$

Comme $|c + 4k'f| < |c|$, l'hypothèse de récurrence assure que A'' est dans le groupe engendré par $T, -T, R$, et donc il en va de même de A' puis de A , ce qui termine la preuve. $\square$

Un autre calcul qui nous sera utile dans la suite est celui de l'indice de $\Gamma_0(4)$ dans le groupe $SL_2(\mathbb{Z})$, que voici :

Proposition 5.1.3. *L'indice du groupe $\Gamma_0(4)$ dans $SL_2(\mathbb{Z})$ est :*

$$[SL_2(\mathbb{Z}) : \Gamma_0(4)] = 6.$$

Démonstration. On considère le morphisme :

$$\Phi : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}).$$

L'image de Φ contenant les transvections et $-I$, elle contient tout $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ (car il est facile de vérifier qu'il est engendré par $-I$ et ses transvections). Ainsi, Φ est surjectif. On note $K \subset \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ l'ensemble des matrices triangulaires supérieures de $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$. C'est l'image de $\Gamma_0(4)$ par Φ , car Φ est surjective. Alors, l'application ensembliste suivante :

$$\begin{aligned} \overline{\Phi} : \mathrm{SL}_2(\mathbb{Z})/\Gamma_0(4) &\rightarrow \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})/K, \\ \overline{M} &\mapsto \overline{\Phi(M)} \end{aligned}$$

(le quotient G/H désignant l'ensemble des classes à gauche modulo H) est bien définie, car si $\overline{M} = \overline{N}$ pour $M, N \in \mathrm{SL}_2(\mathbb{Z})$, alors $M^{-1}N \in \Gamma_0(4)$ et donc $\Phi(M)^{-1}\Phi(N) \in K$ soit $\overline{\Phi(M)} = \overline{\Phi(N)}$. Il est de plus immédiat que $\overline{\Phi}$ est surjective, car Φ l'est. Enfin, vérifions que $\overline{\Phi}$ est injective. Soient donc $M, N \in \mathrm{SL}_2(\mathbb{Z})$ tels que $\overline{\Phi(M)} = \overline{\Phi(N)}$. On a alors $\overline{\Phi(M)} = \overline{\Phi(N)}$ d'où $\Phi(M)^{-1}\Phi(N) \in K$, et donc $M^{-1}N \in \Phi^{-1}(K) \subset \Gamma_0(4)$, soit $\overline{M} = \overline{N}$. Ainsi, on a finalement montré que $\overline{\Phi}$ est une bijection, d'où :

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = [\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) : K].$$

Un palpitant dénombrement que nous n'explicitons pas montre ensuite que :

$$|\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})| = 48, \quad |K| = 8.$$

En faisant le quotient de ces deux quantités, on arrive donc bien à :

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = [\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) : K] = \frac{|\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})|}{|K|} = \frac{48}{8} = 6$$

comme attendu. □

On arrive enfin à la définition de forme modulaire de niveau N .

Définition 5.1.4. Soit $N \geq 1$ un entier, et $k \geq 0$. Une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbb{C}$ est une **fonction modulaire de niveau N et de poids $2k$** si, et seulement si, pour tout $z \in \mathbb{H}$, toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, on a :

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z).$$

On remarque qu'une fonction modulaire f de niveau N et de poids $2k$ est toujours 1-périodique, et donc admet un développement en série de Fourier en la variable $q = e^{2\pi iz}$. Si ce développement de Fourier ne fait intervenir que des puissances positives de q , alors il définit une fonction holomorphe sur le disque unité $\mathbb{D}$. En particulier, on en déduit que $f(z)$ reste bornée quand $\mathrm{Im}(z) \rightarrow +\infty$. La condition de modularité implique dès lors que pour tout $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, la fonction $z \mapsto \frac{1}{(cz+d)^{2k}} f(M \cdot z)$ reste bornée quand $\mathrm{Im}(z) \rightarrow +\infty$.

Cependant, une telle remarque n'est plus nécessairement vraie si M est prise dans $\mathrm{SL}_2(\mathbb{Z})$, et pas seulement dans $\Gamma_0(N)$. Ceci motive la définition suivante de forme modulaire de niveau N :

Définition 5.1.5. Soit $N \geq 1$ un entier. Une fonction modulaire $f : \mathbb{H} \rightarrow \mathbb{C}$ de niveau N et de poids $2k$ est dite une **forme modulaire** de niveau N et de poids $2k$ si et seulement si, pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, la fonction $z \mapsto \frac{1}{(cz+d)^{2k}} f(M \cdot z)$ reste bornée quand $\mathrm{Im}(z) \rightarrow +\infty$.

Remarque 5.1.6. Soit f une fonction modulaire de niveau N . On fixe $M_1, \dots, M_k$ un système de représentants de $\mathrm{SL}_2(\mathbb{Z})$ modulo $\Gamma_0(N)$. Pour vérifier que f est une forme modulaire de niveau N , grâce à la condition de modularité, il suffit de vérifier que pour tout $i \in \llbracket 1, k \rrbracket$, la fonction $z \mapsto f(M_i \cdot z)$ reste bornée quand $\mathrm{Im}(z) \rightarrow +\infty$.

Remarque 5.1.7. On peut également remarquer dès maintenant qu'une forme modulaire au sens classique (c'est à dire une forme modulaire de niveau 1) est toujours une forme modulaire de niveau N , ce pour tout $N \geq 1$.

On conviendra également dès maintenant de la notation suivante. Pour tout entier $k > 0$, tout $N > 1$, on notera $M_{2k}(\Gamma_0(N))$ l'espace des formes modulaires de poids $2k$ et de niveau N .

5.1.2 Dimension de l'espace $M_2(\Gamma_0(4))$

Cette section donne un exemple de la méthode générale permettant de borner les dimensions d'espaces de formes modulaires de niveaux supérieurs. Le principe général est le suivant : étant donné une fonction modulaire de niveau N ayant un grand ordre d'annulation en ∞ , on peut produire des formes modulaires pour tout $\mathrm{SL}_2(\mathbb{Z})$ (i.e. de niveau 1) ayant de grands ordres d'annulation en ∞ , en faisant le produit de f par ses translatés selon le quotient $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(4)$. Connaissant les espaces de formes modulaires de niveau 1, on en déduit des bornes sur les espaces de formes modulaires de niveau N , pour tout $N > 1$.

Théorème 5.1.8. *L'espace $M_2(\Gamma_0(4))$ des formes modulaires de poids 2 et de niveau 4 est un $\mathbb{C}$ -espace vectoriel de dimension au plus 2.*

Démonstration. On suppose par l'absurde que la dimension de $M_2(\Gamma_0(4))$ est supérieure ou égale à 3. En faisant d'habiles combinaisons linéaires de fonctions de $M_2(\Gamma_0(4))$, on peut alors trouver une fonction $f \in M_2(\Gamma_0(4))$ non nulle dont l'ordre d'annulation en ∞ est supérieur ou égal à 2.

On considère alors $M_1, \dots, M_k$ un système complet de représentants de $\mathrm{SL}_2(\mathbb{Z})$ modulo $\Gamma_0(4)$. (ici, $k = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = 6$) On note pour tout $i \in \llbracket 1, k \rrbracket$:

$$M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

On considère ensuite la fonction :

$$F : z \mapsto \prod_{i=1}^k \frac{1}{(c_i z + d_i)^2} f(M_i \cdot z)$$

On va démontrer que la fonction F est une forme modulaire de poids $2[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = 12$ pour le groupe $\mathrm{SL}_2(\mathbb{Z})$.

Soit donc $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. On a naturellement :

$$\begin{aligned} F(P \cdot z) &= \prod_{i=1}^k \left(c_i \frac{az + b}{cz + d} + d_i \right)^{-2} f(M_i P \cdot z) \\ &= \prod_{i=1}^k \frac{(cz + d)^2}{((c_i a + cd_i)z + (bc_i + dd_i))^2} f(M_i P \cdot z). \end{aligned}$$

Maintenant, la multiplication par P induisant une permutation des classes modulo $\Gamma_0(4)$, il existe une permutation $\sigma : \llbracket 1, k \rrbracket \rightarrow \llbracket 1, k \rrbracket$ et des matrices $N_1, \dots, N_k \in \Gamma_0(4)$ telles que pour tout $i \in \llbracket 1, k \rrbracket$, $M_i P = N_i M_{\sigma(i)}$. On note leur coefficients sous la forme :

$$N_i = \begin{pmatrix} a'_i & b'_i \\ c'_i & d'_i \end{pmatrix}.$$

Il vient alors, en utilisant le fait que les N_i sont dans $\Gamma_0(4)$ et que f est modulaire de poids 2 et de niveau 4 :

$$\begin{aligned} F(P \cdot z) &= \prod_{i=1}^k \frac{(cz + d)^2}{((c_i a + cd_i)z + (bc_i + dd_i))^2} f(N_i M_{\sigma(i)} \cdot z) \\ &= \prod_{i=1}^k \frac{(cz + d)^2}{((c_i a + cd_i)z + (bc_i + dd_i))^2} \left(c'_i \frac{a_{\sigma(i)}z + b_{\sigma(i)}}{c_{\sigma(i)}z + d_{\sigma(i)}} + d'_i \right)^2 f(M_{\sigma(i)} \cdot z) \\ &= (cz + d)^{2k} \left(\prod_{i=1}^k \frac{(c'_i a_{\sigma(i)} + c_{\sigma(i)} d'_i)z + (c'_i b_{\sigma(i)} + d'_i d_{\sigma(i)})}{((c_i a + cd_i)z + (bc_i + dd_i))} \right)^2 \\ &\quad \cdot \prod_{i=1}^k \frac{1}{(c_{\sigma(i)}z + d_{\sigma(i)})^2} f(M_{\sigma(i)} \cdot z) \\ &= (cz + d)^{2k} F(z) \left(\prod_{i=1}^k \frac{(c'_i a_{\sigma(i)} + c_{\sigma(i)} d'_i)z + (c'_i b_{\sigma(i)} + d'_i d_{\sigma(i)})}{((c_i a + cd_i)z + (bc_i + dd_i))} \right)^2. \end{aligned} \tag{5.1}$$

Maintenant, pour tout $i \in \llbracket 1, k \rrbracket$, l'égalité $M_i P = N_i M_{\sigma(i)}$ se ré-écrit :

$$\begin{pmatrix} a_i a + b_i c & a_i c + b_i d \\ c_i a + cd_i & c_i b + d_i d \end{pmatrix} = \begin{pmatrix} a'_i a_{\sigma(i)} + b'_i c_{\sigma(i)} & a'_i c_{\sigma(i)} + b'_i d_{\sigma(i)} \\ c'_i a_{\sigma(i)} + c_{\sigma(i)} d'_i & c'_i b_{\sigma(i)} + d'_i d_{\sigma(i)} \end{pmatrix}.$$

Ce qui, en identifiant les coefficients aux positions de c et d , fournit immédiatement que le produit du membre de droite de Equation (5.1) ci-dessus vaut 1. Ainsi, on obtient :

$$F(P \cdot z) = (cz + d)^{2k} F(z)$$

Ceci pour tout $z \in H$ et tout $P \in \mathrm{SL}_2(\mathbb{Z})$. Ceci montre donc que la fonction F est une fonction modulaire pour le groupe $\mathrm{SL}_2(\mathbb{Z})$ (c'est à dire de niveau 1) de poids $2k = 2[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = 2 \cdot 6 = 12$. Comme elle est bornée pour $\mathrm{Im}(z) \rightarrow +\infty$ (car c'est le cas de chacun des termes du produit), c'est donc bien une forme modulaire de niveau 1 et de poids 2.

De plus, le fait que f s'annule à l'ordre au moins 2 en ∞ assure que c'est également le cas de F (car f est un facteur de F , et tous les autres facteurs sont bornés au voisinage de ∞). Dès lors, l'espace des formes modulaires paraboliques de poids 12 étant de dimension 1 engendré par Δ (voir chapitre 1), on a $F = \lambda\Delta$ pour un certain $\lambda \in \mathbb{C}$. Comme le zéro de Δ en ∞ est simple, et celui de F est au moins double, ceci impose $\lambda = 0$, et donc $F = 0$ puis $f = 0$ par intégrité de l'anneau des fonctions holomorphes sur $\mathbb{H}$. Ceci est absurde, car on a supposé f non identiquement nulle. Ceci conclut donc la preuve.

Ainsi, on a démontré que l'espace $M_2(\Gamma_0(4))$ des formes modulaires de poids 2 et de niveau 4 est de dimension au plus 2. $\square$

5.2 Les formes modulaires de poids 2 de niveaux supérieurs

5.2.1 La série d'Eisenstein de poids 2

Dans le premier chapitre, on a introduit les séries d'Eisenstein G_k pour tout $k > 1$, qui sont respectivement des formes modulaires de poids $2k$. Cependant, il n'a pas été question du cas $k = 1$. C'est de cette série d'Eisenstein qu'on va traiter ici.

On pourrait être tentés d'écrire naïvement la définition suivante, pour tout $z \in \mathbb{H}$:

$$G_1(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz + n)^2}.$$

Cette approche est cependant vouée à l'échec, puisque la somme considérée n'est pas absolument convergente. L'ordre de sommation a donc une importance capitale. On préférera donc la définition univoque suivante.

Définition 5.2.1. Pour tout $z \in \mathbb{H}$, on pose :

$$G_1(z) = \sum_{m \in \mathbb{Z}} \sum_{n \in \mathbb{Z}'_m} \frac{1}{(mz + n)^2}$$

où on a posé $\mathbb{Z}'_m = \mathbb{Z}$ si $m \neq 0$, et $\mathbb{Z}^*$ si $m = 0$.

On peut ré-écrire cette définition sous la forme :

$$G_1(z) = 2\zeta(2) + \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz + n)^2}.$$

On repart alors du développement bien connu de la cotangente, démontré en Section 1.1.3 :

$$\pi i - 2\pi i \sum_{n=0}^{+\infty} q^n = \frac{1}{z} + \sum_{n=1}^{+\infty} \frac{1}{z-n} + \frac{1}{z+n},$$

où $q = e^{2\pi iz}$. Cette série de fonctions holomorphes convergeant localement uniformément, on peut dériver par rapport à la variable z , et il vient pour tout $z \in \mathbb{H}$:

$$(2\pi i)^2 \sum_{n=0}^{+\infty} n q^n = \sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^2}.$$

En injectant ceci dans l'expression de G_1 ci-dessus, on obtient pour tout $z \in \mathbb{H}$:

$$G_1(z) = 2\zeta(2) - 4\pi^2 \sum_{m \in \mathbb{Z}^*} \sum_{n=0}^{+\infty} nq^{mn}.$$

En ré-arrangeant les sommes, ce qui est légitime par sommabilité de la famille considérée (car $|q| < 1$), on arrive donc à la proposition suivante :

Proposition 5.2.2. *Pour tout $z \in \mathbb{H}$, on a, en notant $q = e^{2\pi iz}$:*

$$G_1(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma(n)q^n$$

où pour tout $n \in \mathbb{N}^*$, $\sigma(n) = \sum_{d|n} d$.

Par analogie avec le cas $k > 1$, on pourrait naturellement s'attendre à ce que G_1 soit une forme modulaire de poids 2. Cependant, la preuve de la modularité des fonctions G_k pour $k > 1$ reposait de manière cruciale sur la sommabilité de la famille $\left(\frac{1}{(mz+n)^{2k}}\right)_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}}$, et ne semble donc pas pouvoir s'adapter telle quelle à la fonction G_1 . Et, effectivement, la fonction G_1 n'est **pas** une forme modulaire.

Elle vérifie cependant une équation fonctionnelle proche de celle des formes modulaires, que nous allons ici expliciter. La fonction G_1 étant clairement 1-périodique, son défaut de modularité ne peut provenir que de la transformation $z \mapsto \frac{-1}{z}$ associée au générateur S de $\mathrm{SL}_2(\mathbb{Z})$. Voici donc la manière dont G_1 est affectée par la transformation $z \mapsto \frac{-1}{z}$:

Proposition 5.2.3. *Pour tout $z \in \mathbb{H}$, on a :*

$$G_1\left(\frac{-1}{z}\right) = z^2 G_1(z) - 2\pi iz.$$

Démonstration. Soit $z \in \mathbb{H}$. Il vient les calculs suivants (ici, on fait attention à ne pas interchanger deux sommes car la famille considérée n'est pas sommable!) :

$$\begin{aligned} \frac{1}{z^2} G_1\left(\frac{-1}{z}\right) &= \sum_{m \in \mathbb{Z}} \sum_{n \in \mathbb{Z}'_m} \frac{1}{z^2(m\frac{-1}{z} + n)^2} = \sum_{m \in \mathbb{Z}} \sum_{n \in \mathbb{Z}'_m} \frac{1}{(m + nz)^2} \\ &= \sum_{n \in \mathbb{Z}^*} \frac{1}{(nz)^2} + \sum_{m \in \mathbb{Z}^*} \left(\frac{1}{m^2} + \sum_{n \in \mathbb{Z}^*} \frac{1}{(m + nz)^2} \right) \\ &= 2\zeta(2) + \sum_{n \in \mathbb{Z}^*} \frac{1}{(nz)^2} + \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}^*} \frac{1}{(m + nz)^2} \\ &= 2\zeta(2) + \sum_{m \in \mathbb{Z}} \sum_{n \in \mathbb{Z}^*} \frac{1}{(m + nz)^2} \\ \text{et : } G_1(z) &= \sum_{m \in \mathbb{Z}} \sum_{n \in \mathbb{Z}'_m} \frac{1}{(mz + n)^2} = 2\zeta(2) + \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz + n)^2}. \end{aligned}$$

Il vient donc le résultat :

$$\frac{1}{z^2} G_1\left(\frac{-1}{z}\right) - G_1(z) = \sum_{n \in \mathbb{Z}} \sum_{m \in \mathbb{Z}^*} \frac{1}{(mz + n)^2} - \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz + n)^2}. \quad (5.2)$$

Si la famille considérée était sommable, on pourrait immédiatement échanger les deux sommes, et obtenir l'égalité entre $\frac{1}{z^2} G_1\left(\frac{-1}{z}\right)$ et $G_1(z)$. Ce n'est cependant pas le cas ici. Il faut donc évaluer l'erreur commise en échangeant les deux sommes dans les égalités ci-dessus. Pour cela, on introduit le terme suivant, forçant la sommabilité : $\frac{1}{(mz+n)(mz+n+1)}$. Plus précisément, la famille de terme général :

$$u_{m,n} = \frac{1}{(mz+n)^2} - \frac{1}{(mz+n)(mz+n+1)} = \frac{1}{(mz+n)^2(mz+n+1)}$$

est sommable (il y a en gros $O(R)$ termes qui sont de l'ordre de $\frac{1}{R^3}$) et donc on a :

$$\sum_{n \in \mathbb{Z}} \sum_{m \in \mathbb{Z}^*} u_{m,n} = \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} u_{m,n}.$$

Par linéarité de la double somme, on en déduit :

$$\begin{aligned} & \sum_{n \in \mathbb{Z}} \sum_{m \in \mathbb{Z}^*} \frac{1}{(mz+n)^2} - \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz+n)^2} \\ &= \sum_{n \in \mathbb{Z}} \sum_{m \in \mathbb{Z}^*} \frac{1}{(mz+n)(mz+n+1)} - \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz+n)(mz+n+1)}. \end{aligned} \quad (5.3)$$

L'intérêt de cette manœuvre étant que le membre de droite se calcule explicitement. En effet, il vient d'une part par télescopage :

$$\sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz+n)(mz+n+1)} = \sum_{m \in \mathbb{Z}^*} \sum_{n \in \mathbb{Z}} \frac{1}{(mz+n)} - \frac{1}{(mz+n+1)} = 0.$$

Et d'autre part, en utilisant le développement de la cotangente :

$$\begin{aligned} \sum_{n \in \mathbb{Z}} \sum_{m \in \mathbb{Z}^*} \frac{1}{(mz+n)(mz+n+1)} &= \lim_{N \rightarrow +\infty} \sum_{n=-N}^{N-1} \sum_{m \in \mathbb{Z}^*} \frac{1}{(mz+n)} - \frac{1}{(mz+n+1)} \\ &= \lim_{N \rightarrow +\infty} \sum_{m \in \mathbb{Z}} \sum_{n=-N}^{N-1} \frac{1}{(mz+n)} - \frac{1}{(mz+n+1)} \\ &= \lim_{N \rightarrow +\infty} \sum_{m \in \mathbb{Z}^*} \frac{1}{mz-N} - \frac{1}{mz+N} \\ &= \lim_{N \rightarrow +\infty} \frac{-1}{z} \sum_{m \in \mathbb{Z}^*} \frac{1}{\frac{N}{z} - m} + \frac{1}{\frac{N}{z} + m} \\ &= \lim_{N \rightarrow +\infty} \frac{-1}{z} \left(2\pi \cot\left(\pi \frac{N}{z}\right) - 2 \frac{z}{N} \right) \\ &= \lim_{N \rightarrow +\infty} \frac{-1}{z} 2\pi i \frac{1 + e^{\frac{-2\pi i}{z} N}}{1 - e^{\frac{-2\pi i}{z} N}} \\ &= -\frac{2\pi i}{z} \quad \text{car } \frac{-1}{z} \in \mathbb{H}. \end{aligned}$$

En réunissant les deux calculs précédents avec les équations 5.2 et 5.3, on obtient donc le résultat :

$$\frac{1}{z^2} G_1\left(\frac{-1}{z}\right) = G_1(z) - \frac{2\pi i}{z},$$

qui est exactement ce qu'il fallait démontrer. $\square$

Proposition 5.2.4. *Pour tout $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, tout $z \in \mathbb{H}$, on a :*

$$G_1\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 G_1(z) - 2\pi i(cz+d)c.$$

Maintenant qu'on connaît l'action de S et T sur la fonction G_1 , comme les matrices S et T engendrent $\mathrm{SL}_2(\mathbb{Z})$, on peut en déduire explicitement l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur G_1 . C'est exactement ce que l'on fait dans cette proposition.

Démonstration. Commençons par remarquer que si :

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

sont deux matrices de $\mathrm{SL}_2(\mathbb{Z})$ pour lesquelles l'équation ci-dessus est vérifiée, alors il en va de même de MM' et de M^{-1} . Pour le voir, notons :

$$M'' = MM' = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bc' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Et supposons l'équation vérifiée pour M et M' , et montrons la pour M'' . On a :

$$\begin{aligned} G_1(MM' \cdot z) &= G_1(M \cdot (M' \cdot z)) = (c(M' \cdot z) + d)^2 G_1(M' \cdot z) - 2\pi i(c(M' \cdot z) + d)c \\ &= \left(c \frac{a'z + b'}{c'z + d'} + d\right)^2 ((c'z + d')^2 G_1(z) - 2\pi i(c'z + d')c') - 2\pi i \left(c \frac{a'z + b'}{c'z + d'} + d\right) c \\ &= (ca'z + cb' + dc'z + dd')^2 G_1(z) \\ &\quad - 2\pi i \left(c'(c'z + d') \left(c \frac{a'z + b'}{c'z + d'} + d\right) + c\right) \left(c \frac{a'z + b'}{c'z + d'} + d\right) \\ &= (c''z + d'')^2 G_1(z) \\ &\quad - 2\pi i(c'((ca' + c'd)z + (cb' + dd')) + c) \left(c \frac{a'z + b'}{c'z + d'} + d\right) \\ &= (c''z + d'')^2 G_1(z) - 2\pi i(c'(ca' + dc')z + c'(cb' + dd') + c) \frac{c''z + d''}{c'z + d'} \\ &= (c''z + d'')^2 G_1(z) - 2\pi i(c'(ca' + dc')z + c'(cb' + dd') + c(a'd' - b'c')) \frac{c''z + d''}{c'z + d'} \\ &= (c''z + d'')^2 G_1(z) - 2\pi i(c'(ca' + dc')z + c'dd' + ca'd') \frac{c''z + d''}{c'z + d'} \\ &= (c''z + d'')^2 G(z) - 2\pi i(c'z + d')(ca' + dc') \frac{c''z + d''}{c'z + d'} \\ &= (c''z + d'')^2 G(z) - 2\pi i c''(c''z + d'') \end{aligned}$$

Qui est bien le résultat souhaité. Montrons le également pour $M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. On a :

$$\begin{aligned} G_1(z) &= G_1(MM^{-1} \cdot z) = G_1(M \cdot (M^{-1} \cdot z)) \\ &= (c(M^{-1} \cdot z) + d)^2 G_1(M^{-1} \cdot z) - 2\pi i c(c(M^{-1} \cdot z) + d) \\ &= \left(c \frac{dz - b}{-cz + a} + d\right)^2 G_1(z) - 2\pi i c \left(c \frac{dz - b}{-cz + a} + d\right) \end{aligned}$$

Ce qui se ré-arrange en :

$$(-cz + a)^2 G_1(z) = (cdz - bc - cdz + ad)G_1(M^{-1} \cdot z) - 2\pi i c(-cz + a)(cdz - bd - cdz + ad)$$

Avec $ad - bc = 1$, ceci se ré-écrit :

$$G_1(M^{-1} \cdot z) = (-cz + a)^2 G_1(z) - 2\pi i(-c)(-cz + a)$$

Qui est bien l'équation qu'il fallait démontrer. Finalement, on a montré que si M et M' vérifient l'équation de l'énoncé, alors il en va de même de MM' et de M^{-1} . Autrement dit, l'ensemble des matrices $M \in \mathrm{SL}_2(\mathbb{Z})$ vérifiant l'équation de l'énoncé est un sous-groupe

de $\mathrm{SL}_2(\mathbb{Z})$. Maintenant, ce sous-groupe contient $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (car G_1 est clairement

1-périodique) et contient également $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (c'est exactement le résultat de la proposition 3), et donc comme $\mathrm{SL}_2(\mathbb{Z})$ est engendré par S et T , il contient tout $\mathrm{SL}_2(\mathbb{Z})$. Ceci termine la preuve de la proposition 4. $\square$

5.2.2 Les formes modulaires $G_{1,N}$ de niveaux supérieurs

Comme on l'a vu dans le paragraphe précédent, la fonction G_1 n'est pas une forme modulaire. Cependant, on peut l'utiliser pour produire des formes modulaires ! Voici un exemple de telle construction.

Théorème 5.2.5. *Soit $N > 1$ un entier. Pour tout $z \in \mathbb{H}$, on pose :*

$$G_{1,N}(z) = G_1(z) - NG_1(Nz).$$

La fonction $G_{1,N}$ est alors une forme modulaire de poids 2 et de niveau N .

Démonstration. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. On considère la matrice :

$$B = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{1}{N} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & Nb \\ \frac{c}{N} & d \end{pmatrix}.$$

On remarque alors que $B \in \mathrm{SL}_2(\mathbb{Z})$, si bien que par l'équation fonctionnelle de G_1 (dernière proposition du paragraphe précédent), appliquée en Nz à la matrice B , on a :

$$G_1\left(\frac{aNz + Nb}{cz + d}\right) = (cz + d)^2 G_1(Nz) - 2\pi i \frac{c}{N} (cz + d).$$

Ceci se ré-écrit :

$$G_1(N(A \cdot z)) = (cz + d)^2 G_1(Nz) - 2\pi i (cz + d).$$

Et il vient donc, en appliquant également l'équation fonctionnelle de G_1 directement à A en z :

$$\begin{aligned} G_{1,N}(A \cdot z) &= G_1(A \cdot z) - NG_1(N(A \cdot z)) \\ &= (cz + d)^2 G_1(z) - 2\pi i c(cz + d) - N \left((cz + d)^2 G_1(Nz) - 2\pi i \frac{c}{N} (cz + d) \right) \\ &= (cz + d)^2 (G_1(z) - NG_1(Nz)) \\ &= (cz + d)^2 G_{1,N}(z). \end{aligned}$$

Ce qui termine la preuve. $\square$

On peut également établir un développement en série de Fourier de la variable $q = e^{2\pi iz}$ des formes modulaires de niveau N nouvellement construites.

Proposition 5.2.6. *Pour tout $z \in \mathbb{H}$, tout $N \geq 1$, on a l'égalité :*

$$G_{1,N}(z) = -(N-1)\frac{\pi^2}{3} - 8\pi^2 \sum_{n=0}^{+\infty} q^n \left(\sum_{\substack{d|n \\ N \nmid d}} d \right)$$

où on a posé $q = e^{2\pi iz}$.

Démonstration. On repart de la définition de $G_{1,N}$. En utilisant le développement de Fourier de G_1 , il vient :

$$\begin{aligned} G_{1,N}(z) &= G_1(z) - NG_1(Nz) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma(n)q^n - N\frac{\pi^2}{3} + 8N\pi^2 \sum_{n=1}^{+\infty} \sigma(n)q^{Nn} \\ &= -(N-1)\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma(n)q^n + 8\pi^2 \sum_{n=1}^{+\infty} \left(\sum_{d|n} dN \right) q^{Nn} \\ &= -(N-1)\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma(n)q^n + 8\pi^2 \sum_{\substack{n \geq 1 \\ N|n}} \left(\sum_{\substack{d|n \\ N \nmid d}} d \right) q^n \\ &= -(N-1)\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma(n)q^n + 8\pi^2 \sum_{n=1}^{+\infty} \left(\sum_{\substack{d|n \\ N \nmid d}} d \right) q^n \\ &= -(N-1)\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \left(\sum_{\substack{d|n \\ N \nmid d}} d \right) q^n. \end{aligned}$$

Ce qui conclut la preuve. $\square$

Ainsi, pour tout $N \geq 2$, on a construit une forme modulaire de poids 2 et de niveau N . En fait, on peut remarquer que pour certains entiers N , on a construit beaucoup plus qu'une forme modulaire de niveau N . En effet, si d est un diviseur de N , alors on a $\Gamma_0(N) \subset \Gamma_0(d)$, et donc les formes modulaires de niveau d sont en particulier des formes modulaires de niveau N , de même poids.

Comme on sait que $G_{1,d}$ est une forme modulaire de poids 2 et de niveau d , c'est en particulier également une forme modulaire de poids 2 et de niveau N si d divise N . Ainsi, par exemple, pour $N = 4$, on a construit deux formes modulaires de poids 2 et de niveau 4, à savoir $G_{1,2}$ et $G_{1,4}$.

5.2.3 La fonction θ^4 est une forme modulaire de niveau 4

Commençons par la définition de la fonction θ de Jacobi.

Définition 5.2.7. On définit la fonction $\theta : \mathbb{H} \rightarrow \mathbb{C}$, par la formule suivante, valable pour tout $z \in \mathbb{H}$:

$$\theta(z) = \sum_{n \in \mathbb{Z}} q^n = \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z}$$

où on a posé $q = e^{2\pi iz}$.

Une application standard de la formule sommatoire de Poisson fournit une équation fonctionnelle pour la fonction θ .

Lemme 5.2.8. *Pour tout réel $t > 0$, on a :*

$$\theta\left(\frac{i}{4t}\right) = \sqrt{2t}\theta(t).$$

Démonstration. Soit $t > 0$. On considère la fonction à décroissance rapide :

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R}, \\ x &\mapsto e^{-2\pi t x^2}. \end{aligned}$$

Le cas particulier de la dimension 1 des calculs de transformées de Fourier de gaussiennes assure que la transformée de Fourier de f est donnée par :

$$\hat{f} : t \mapsto \frac{1}{\sqrt{2t}} e^{-\frac{\pi}{2t} x^2}.$$

On considère le réseau $L = \mathbb{Z}$ de $\mathbb{R}$. C'est naturellement un réseau entier unimodulaire, et on peut donc lui appliquer la formule sommatoire de Poisson. On obtient donc :

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n).$$

Soit :

$$\sum_{n \in \mathbb{Z}} e^{-2\pi t n^2} = \frac{1}{\sqrt{2t}} \sum_{n \in \mathbb{Z}} e^{-\frac{\pi}{2t} n^2}.$$

Ce qui est exactement la formule :

$$\theta(it) = \frac{1}{\sqrt{2t}} \theta\left(\frac{i}{4t}\right).$$

□

On considère alors la fonction $\Theta = \theta^4$. L'équation fonctionnelle de θ implique que Θ est une fonction modulaire de poids 2 et de niveau 4.

Proposition 5.2.9. *La fonction $\Theta = \theta^4$ est une fonction modulaire de poids 2 et de niveau $N = 4$.*

Démonstration. On veut montrer que pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$, on a $\Theta(M \cdot z) = (cz + d)^2 \Theta(z)$. Exactement comme pour le cas des formes modulaires sur $\mathrm{SL}_2(\mathbb{Z})$, il suffit de vérifier le résultat sur un ensemble de générateurs de $\Gamma_0(4)$. Or, on a vu à l'occasion du paragraphe sur les sous-groupes de congruences que $\Gamma_0(4)$ est engendré par les trois matrices :

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad -T = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Il suffit donc de vérifier les équations suivantes, pour tout $z \in \mathbb{H}$:

$$\Theta\left(\frac{z+1}{1}\right) = 1^2 \Theta(z), \quad \Theta\left(\frac{-z-1}{-1}\right) = (-1)^2 \Theta(z), \quad \Theta\left(\frac{z}{4z+1}\right) = (4z+1)^2 \Theta(z).$$

Les deux premières équations sont claires, θ (et donc $\Theta = \theta^4$) étant 1-périodique. Montrons la troisième.

Pour cela, commençons par constater que l'équation fonctionnelle de la fonction θ implique que pour tout $t > 0$, on a :

$$\Theta\left(\frac{i}{4t}\right) = 4t^2\theta(it).$$

En posant $z = it$, ceci assure que pour tout $z \in i\mathbb{R}_+^*$, on a l'égalité :

$$\Theta\left(\frac{-1}{4z}\right) = -4z^2\Theta(z). \quad (5.4)$$

Les deux membres de cette équation sont des fonctions holomorphes sur $\mathbb{H}$, donc par le principe des zéros isolés, on obtient que l'égalité 5.4 reste vraie pour tout $z \in \mathbb{H}$. Dès lors, pour tout $z \in \mathbb{H}$, il vient (en utilisant l'égalité 5.4 ainsi que la 1-périodicité de Θ) :

$$\begin{aligned} \Theta\left(\frac{z}{4z+1}\right) &= \Theta\left(\frac{-1}{4(-1-\frac{1}{4z})}\right) = -4\left(-1-\frac{1}{4z}\right)^2 \Theta\left(-1-\frac{1}{4z}\right) \\ &= -4\left(1+\frac{1}{4z}\right)^2 \Theta\left(\frac{-1}{4z}\right) = -4\left(1+\frac{1}{4z}\right)^2 (-4z^2)\Theta(z) \\ &= (4z+1)^2\Theta(z), \end{aligned}$$

qui est bien l'égalité qu'il fallait démontrer. Ainsi, on a démontré que Θ est une forme modulaire de poids 2 et de niveau 4. $\square$

Pour voir que Θ est en fait une forme modulaire de niveau 4 (et pas seulement une fonction modulaire), il s'agit donc de vérifier la condition de bornitude qui distingue les formes modulaires des simples fonctions modulaires.

Proposition 5.2.10. *La fonction $\Theta = \theta^4$ est une forme modulaire de poids 2 et de niveau 4.*

Démonstration. Comme on sait déjà que Θ est une fonction modulaire de poids 2 et de niveau 4, il suffit de vérifier que pour tout $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, la fonction $z \mapsto \frac{1}{(cz+d)^2} \Theta\left(\frac{az+b}{cz+d}\right)$ est bornée pour $\mathrm{Im}(z) \rightarrow +\infty$.

On note pour cela H l'ensemble des $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ telles que la fonction $z \mapsto \frac{1}{(cz+d)^2} \Theta\left(\frac{az+b}{cz+d}\right)$ est bornée pour $\mathrm{Im}(z) \rightarrow +\infty$. On peut montrer que H contient les matrices élémentaires S et T , et que H est stable par multiplication et passage à l'inverse. Les détails de cette vérification sont laissés aux lecteurs et lectrices. $\square$

5.2.4 Application au théorème des quatre carrés de Lagrange

Le fait que la fonction Θ soit une forme modulaire est susceptible de nous donner de nombreuses informations sur les coefficients de son développement de Fourier. On peut donc commencer par expliciter son développement en série de Fourier. En développant le produit :

$$\Theta(z) = \theta(z)^4 = \left(\sum_{n \in \mathbb{Z}} q^{n^2}\right)^4 = \sum_{a,b,c,d \in \mathbb{Z}} q^{a^2+b^2+c^2+d^2}$$

(où, comme d'habitude, on a posé $q = e^{2\pi iz}$), on obtient immédiatement l'égalité suivante :

Proposition 5.2.11. *Pour tout $z \in \mathbb{H}$, en posant $q = e^{2\pi iz}$, on a :*

$$\Theta(z) = \sum_{n \in \mathbb{N}} r_4(n) q^n$$

où, pour tout $n \in \mathbb{N}$, on a posé :

$$r_4(n) = |\{(a, b, c, d) \in \mathbb{Z}, a^2 + b^2 + c^2 + d^2 = n\}|$$

Les premiers termes de ce développement sont donnés par :

$$\Theta(z) = 1 + 8q + 24q^2 + \dots$$

Par ailleurs, on sait que Θ est une forme modulaire de poids 2 et de niveau N . Connaissant une borne sur la dimension de l'espace $M_2(\Gamma_0(4))$ des formes modulaires de poids 2 et de niveau 4, on peut en déduire une autre expression de Θ faisant intervenir les fonctions $G_{1,N}$. Plus précisément, on a le résultat suivant :

Théorème 5.2.12. *On a l'égalité :*

$$\Theta = -\frac{1}{\pi^2} G_{1,4}$$

Démonstration. On a vu en 4.1.2 que l'espace $M_2(\Gamma_0(4))$ des formes modulaires de poids 2 et de niveau 4 est un $\mathbb{C}$ -espace vectoriel de dimension au plus 2. Par ailleurs, les remarques de la fin de la section 4.2.2 assurent que $G_{1,2}$ et $G_{1,4}$ sont des éléments de $M_2(\Gamma_0(4))$. Leurs développement de Fourier en la variable $q = e^{2\pi iz}$ commençant par :

$$G_{1,2}(z) = -\frac{\pi^2}{3} - 8\pi^2 q - 16\pi^2 q^2 + \dots \quad G_{1,4}(z) = -\pi^2 - 8\pi^2 q - 16\pi^2 q^2 + \dots$$

Il apparaît donc que $G_{1,2}$ et $G_{1,4}$ ne sont pas proportionnelles. Comme ces fonctions appartiennent à l'espace $M_2(\Gamma_0(4))$ qui est de dimension au plus 2, elles forment donc une base de l'espace $M_2(\Gamma_0(4))$. Comme $\Theta \in M_2(\Gamma_0(4))$, il existe donc $\lambda, \mu \in \mathbb{C}$ tels que :

$$\Theta = \lambda G_{1,2} + \mu G_{1,4}$$

En identifiant les deux premiers coefficients, on obtient le système :

$$\begin{aligned} 1 &= \lambda \frac{-\pi^2}{3} + \mu(-\pi^2) \\ 8 &= \lambda(-8\pi^2) + \mu(-8\pi^2) \end{aligned}$$

Qui se résout en $\lambda = 0$, $\mu = \frac{-1}{\pi^2}$, et donne donc l'égalité attendue :

$$\Theta = \frac{-1}{\pi^2 G_{1,4}}$$

□

En identifiant les coefficients du développement en la variable $q = e^{2\pi iz}$ de Θ et $\frac{-1}{\pi^2} G_{1,4}$, on obtient le corollaire suivant :

Corollaire 5.2.13. *Pour tout entier $n \geq 1$, on a :*

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d$$

Conclusion

Nous avons démontré la modularité des fonctions $\theta_{L,P}$, $L \subset \mathbb{R}^n$, P harmoniques de degré d , associées aux réseaux unimodulaires pairs. Pour cela on a démontré et utilise la formule sommatoire de Poisson afin de prouver une identité reliant une série définie par une fonction à sa transformée de Fourier. En utilisant cette formule, et la relation classique entre une fonction gaussienne et sa transformée de Fourier (qui est encore une gaussienne!), on a obtenu des identités vérifiées par les séries θ_L . En utilisant la théorie des fonctions de la variable complexe on en a déduit la modularité de θ_L .

Afin de démontrer la modularité de $\theta_{L,P}$, nous avons utilisé deux méthodes différentes. La première utilisait la propriété de la moyenne pour les fonctions harmoniques afin de démontrer l'identité du théorème 3.2 par un calcul direct. La deuxième utilisait 3 opérateurs agissant sur l'espace des polynômes à n variables, ainsi que la façon dont ces opérateurs se transforment après une transformée de Fourier, pour démontrer la même identité. De nouveau la théorie des fonctions de la variable complexe nous a permis de conclure que la série $\theta_{L,P}$ est bien modulaire de poids $d + \frac{n}{2}$.

La modularité de ces fonctions a de nombreuses conséquences, et possède des applications dans différents domaines des mathématiques. En théorie des réseaux, on peut utiliser la nullité des espaces de formes paraboliques en basse dimension (6, 10 et 14) afin d'obtenir des identités telles que :

$$\sum_{x \in \mathcal{R}_L} (x \cdot y)^2 = \frac{2|\mathcal{R}_L|(y \cdot y)}{n} \quad , \quad \mathcal{R}_L = \{x \in L | x \cdot x = 2\},$$

en utilisant le polynôme harmonique $P(x) = (x \cdot y)^2 - \frac{(x \cdot x)(y \cdot y)}{n}$, $n = 8, 16, 24$. Ce genre d'identité est le début de la classification des réseaux unimodulaires pairs en dimensions 8, 16 et 24. Remarquablement, il existe un unique réseau unimodulaire pair à isométrie près en dimension 8 : E_8 , et deux en dimension 16 : $E_8 \oplus E_8$ et D_{16}^+ . On trouve une preuve de ce résultat dans [5], qui utilise des résultats présents dans [6] sur les systèmes de racines. En revanche, dès la dimension 24, la classification se complique : il existe, à isométrie près, 24 réseaux unimodulaires pairs en dimension 24, dont le célèbre réseau de Leech. Pour plus de détails concernant cette classification, consulter [4].

En théorie des nombres, ces séries peuvent être utilisées afin de démontrer de très nombreux théorèmes, parmi lesquels on peut citer le très célèbre théorème des quatre carrés de Jacobi, qui donne la formule citée en introduction :

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d.$$

Cette formule peut être obtenue en utilisant une classe un peu plus large de fonctions modulaires, possédant une symétrie restreinte à des sous groupes d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$.

Bibliographie

- [1] Jean-Pierre Serre, *Cours d'Arithmétique*
- [2] Noam Elkies, Math 272y : *Rational Lattices and their Theta Functions (Fall 2019)*
- [3] Gaëtan Chenevier, Jean Lannes, *Automorphic Forms and Even Unimodular Lattices*
- [4] Hans-Volker Niemeier, *Definite quadratische Formen der Dimension 24 und Diskriminante 1*
- [5] Ebelin Wolfgang, *Lattices and Codes*
- [6] James E. Humphreys, *Introduction to Lie Algebras and Representation Theory*