Stage de fin de Licence

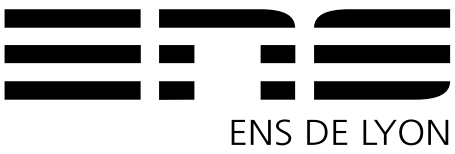
Théophile Cailliau

Théorème des quatre carrés et formes modulaires

Maître de Stage
Didier Lesesvre

Laboratoire
Paul Painlevé
Université de Lille

Laboratoire
Paul Painlevé



Année 2021 – 2022

Introduction

Ce rapport constitue une introduction à la détermination ou à l'étude des quantités du type

$$r_k(n) = \#\left\{(a_1, \cdots, a_k) \in \mathbf{Z}^k, \quad \sum_{i=1}^{k} a_i^2 = n\right\}, \qquad k \geqslant 0.$$

La première question qui se pose est celle du support de r_k, c'est à dire la détermination des entiers n décomposables en somme de k carrés. Un théorème de Lagrange (1770) affirme que lorsque $k = 4$, r_k a pour support $\mathbf{N}$. Plus tard, Jacobi montre une formule explicite pour r_4. Le travail de Jacobi est séminal dans le développement de la théorie des formes modulaires, qui constituent un outil puissant et un objet important de théorie analytique des nombres. Dans le paradigme actuel, les formes modulaires constituent le cadre naturel de l'analyse des quantités du type r_k.

Didier Lesesvre et moi avons fixé l'objectif de stage suivant : obtenir une démonstration auto-contenue du théorème des quatre carrés, en exploitant des outils qui s'avèrent généraux. Cela donnera lieu au théorème suivant.

Théorème de Jacobi.

$$r_4(n) = 8 \sum_{\substack{0<d|n \\ 4\nmid n}} d$$

Table des matières

1 Théorème des quatre carrés : existence des décompositions **3**
- 1.1 Sommes de quatre carrés . . . 3
- 1.2 Sommes de deux carrés . . . 4

2 Théorie des formes modulaires : résultats élémentaires **5**
- 2.1 Formes modulaires . . . 5
- 2.2 Sous-groupes de congruence . . . 6
- 2.3 Pointes sous l'action d'un sous-groupe . . . 9
- 2.4 Domaine fondamental . . . 11
- 2.5 Formules de valence . . . 13
- 2.6 Dimension des espaces de formes modulaires . . . 17

3 Application à la détermination de r_k : la fonction θ **18**
- 3.1 Fonction θ . . . 18
- 3.2 Séries d'Eisenstein . . . 19
- 3.3 Séries d'Eisenstein de poids 2 . . . 21
- 3.4 Détermination de r_4 . . . 23

A Éléments de géométrie hyperbolique **25**
- A.1 Distance hyperbolique . . . 25
- A.2 Isométries hyperboliques . . . 25
- A.3 Gauss-Bonnet et volume du domaine fondamental . . . 26

Références **26**

1 Théorème des quatre carrés : existence des décompositions

Les preuves classiques d'existence de décompositions en sommes de 2 et 4 carrés suivent le même schéma de preuve : on se place dans un $\mathbf{Z}$-module libre muni d'une multiplication, puis on exprime les sommes de 4 carrés comme une forme quadratique qui s'avèrera multiplicative. Il reste alors à déterminer quels sont les nombres premiers qui sont dans l'image de la forme quadratique que l'on a construite.

1.1 Sommes de quatre carrés

La preuve proposée ici est attribuée à B. Venkov [Ven22].

Théorème 1.1.1 (Lagrange).
| Le support de r_4 est $\mathbf{N}$.

Preuve. On se place dans l'algèbre à division des quaternions rationnels

$$B(\mathbf{Q}) = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$$

où

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Dans cette algèbre, on définit la conjugaison $\overline{a + ib + jc + kd} = a - ib - jc - kd$ (avec $a, b, c, d \in \mathbf{Q}$), et on introduit la norme réduite $\mathrm{Nr}(z) = z\overline{z} = a^2 + b^2 + c^2 + d^2$. Le calcul $\overline{zz'} = \overline{z'}\overline{z}$ permet d'obtenir la multiplicativité de cette norme réduite

$$\mathrm{Nr}(zz') = \mathrm{Nr}(z)\,\mathrm{Nr}(z').$$

On considère les deux sous-anneaux de $B(\mathbf{Q})$ suivants :

$$B(\mathbf{Z}) = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$$

$$\mathcal{O}_B = \mathbf{Z}\left[i, j, k, \frac{1 + i + j + k}{2}\right].$$

On désigne par *quaternions de Hurwitz* ce deuxième anneau. On a la chaine d'inclusions (strictes) suivante :

$$B(\mathbf{Z}) \subsetneq \mathcal{O}_B \subsetneq B(\mathbf{Q}).$$

Puis, un calcul rapide montre que $\mathrm{Nr}(\mathcal{O}_B) \subseteq \mathbf{N}$, $\mathrm{tr}(\mathcal{O}_B) \subseteq \mathbf{N}$. Les inversibles de ces deux anneaux sont

$$B(\mathbf{Z})^\times = \{\pm 1, \pm i, \pm j, \pm k\}$$

$$\mathcal{O}_B^\times = B(\mathbf{Z})^\times \cup \left\{\frac{\pm 1 \pm i \pm j \pm k}{2}\right\}$$

L'anneau des quaternions de Hurwitz a la propriété suivante : pour tout $z \in \mathcal{O}_B$, il existe $u \in \mathcal{O}_B^\times$ tel que $uz \in B(\mathbf{Z})$ (calcul). Avec les propriétés que l'on a établies (la multiplicativité de la norme réduite et le lien entre $\mathcal{O}_B$ et $B(\mathbf{Z})$), il est désormais suffisant de montrer que $p \in \mathrm{Nr}(\mathcal{O}_B)$ pour tout p premier. La propriété essentielle des quaternions de Hurwitz est la suivante : tous les idéaux (à gauche, à droite) sont principaux. On le montre dans la proposition suivante. On a $\mathrm{Nr}(1) = 1$ et $\mathrm{Nr}(1 + i) = 2$. Soit $p > 2$ premier. Alors,

$$a^2 + b^2 + c^2 \equiv 0 \pmod{p}$$

admet une solution non nulle car $\{1 + b^2, b \in \mathbf{F}_p\}$ et $\{-c^2, c \in \mathbf{F}_p\}$ ont tous les deux le cardinal $\frac{p+1}{2}$ donc s'intersectent. Pour une telle solution, notée $\omega = ai + bj + ck$, $I = \mathcal{O}_B\omega + \mathcal{O}_B p$ est un idéal strictement inclus dans $\mathcal{O}_B$ (car I ne contient pas d'inversibles), et $\mathcal{O}_B p \subseteq I$. Comme $\mathcal{O}_B$ est principal, I est principal et il existe z tel que $I = \mathcal{O}_B z$. Il existe donc z' tel que $p = zz'$, et ni z ni z' n'est inversible. Donc, $\mathrm{Nr}(zz') = \mathrm{Nr}(p) = p^2 = \mathrm{Nr}(z)\,\mathrm{Nr}(z')$ donc $\mathrm{Nr}(z) = \mathrm{Nr}(z') = p$. Puis, quitte à multiplier par un inversible de $\mathcal{O}_B$, on peut supposer $z \in B(\mathbf{Z})$, ce qui conclut. □

Proposition 1.1.1.
| L'anneau $\mathcal{O}_B$ des quaternions de Hurwitz est principal.

Preuve. On va montrer que l'anneau est euclidien pour le stathme Nr. Soient z, q dans $\mathcal{O}_B$. Alors, $zq^{-1} \in \mathcal{O}_B$ et il existe $\ell \in B(\mathbf{Z})$ tel que $zq^{-1} - \ell$ a ses coordonnées comprises dans $[-1/2, 1/2]$. Dans ce cas, $\mathrm{Nr}(zq^{-1} - \ell) \leqslant 1$ avec égalité ssi toutes les coordonées valent $\pm 1/2$, mais dans ce cas un changement de ℓ en $\ell + \frac{\pm 1 \pm i \pm j \pm k}{2}$ permet de s'assurer que $\mathrm{Nr}(zq^{-1} - \ell) < 1$. On en déduit $\mathrm{Nr}(z - \ell q) < \mathrm{Nr}(q)$, ce qui conclut. □

1.2 Sommes de deux carrés

Dans le cas de deux carrés, il y a d'autres détails techniques mais le schéma de preuve reste identique. La preuve présentée ici est adaptée de [Per96].

Théorème 1.2.1.
Soit $n \in \mathbf{N}^\star$. Alors,

$$r_2(n) > 0 \iff 2 \mid v_p(n), \quad \forall p \in \mathcal{P}, p \equiv 3 \pmod 4$$

Preuve. On se place cette fois ci dans les entiers de Gauss : $\mathbf{Z}[i]$. On définit comme précédemment $\mathrm{Nr}(z) = z\overline{z}$ qui est multiplicative, et on note $\Sigma = \mathrm{Nr}(\mathbf{Z}[i])$. L'anneau $\mathbf{Z}[i]$ est euclidien pour le stathme $\mathbf{Z}[i]$ (preuve classique sur le même principe que pour $\mathcal{O}_B$), donc principal.

Si p est premier et $p \in \Sigma$, alors $p = \mathrm{Nr}(z) = z\overline{z}$ pour un z donc c'est un élément réductible de $\mathbf{Z}[i]$. Réciproquement, si p est un premier réductible en $p = zz'$, avec $z, z' \neq \pm 1, \pm i$, alors $\mathrm{Nr}(p) = \mathrm{Nr}(z)\,\mathrm{Nr}(z') = p^2$ donc $\mathrm{Nr}(z) = \mathrm{Nr}(z') = p$ et $p \in \Sigma$.

Trouver les premiers qui sont dans Σ revient donc à trouver les premiers qui sont réductibles dans $\mathbf{Z}[i]$. On écrit pour cela

$$\begin{aligned} p \text{ réductible} &\iff (p) \text{ n'est pas premier} \\ &\iff \mathbf{Z}[i]/(p) \text{ n'est pas intègre.} \end{aligned}$$

Or, on a les isomophismes suivants :

$$\mathbf{Z}[i]/(p) \simeq \mathbf{Z}[X]/(X^2+1, p) \simeq (\mathbf{Z}[X]/(p))/(X^2+1) \simeq \mathbf{F}_p[X]/(X^2+1)$$

donc

$$\begin{aligned} p \text{ réductible} &\iff \mathbf{F}_p[X]/(X^2+1) \text{ non intègre} \\ &\iff X^2+1 \text{ réductible dans } \mathbf{F}_p[X] \\ &\iff -1 \text{ est un carré} \mod p \\ &\iff p = 2 \text{ ou } p \equiv 1 \pmod 4. \end{aligned}$$

Finalement, les premiers dans Σ sont exactement ceux qui ne valent pas $3 \pmod 4$.

Si n est tel que $2 \mid v_p(n)$ pour chaque $p \equiv 3 \pmod 4$, alors $n \in \Sigma$ car les carrés sont dans Σ. Supposons maintenant que $n \in \Sigma$, et montrons que $2 \mid v_p(n)$ pour $p \equiv 3 \pmod 4$. Soit p un tel premier.

- Si $v_p(n) = 0$, alors $2 \mid v_p(n)$.
- Si $v_p(n) > 0$, alors $p | n = a^2 + b^2 = (a+ib)(a-ib)$ or p est irréductible dans $\mathbf{Z}[i]$ donc p^2 divise n et

$$\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$$

  satisfait l'hypothèse de récurrence donc

$$2 \mid v_p(n) = 2 + v_p\left(\frac{n}{p^2}\right)$$

□

2 Théorie des formes modulaires : résultats élémentaires

Les formes modulaires forment une théorie puissante de théorie des nombres. Les formes modulaires sont des fonctions complexes qui respectent des conditions fortes de symétrie (invariance par l'action de certains groupes d'homographies). Cette forte contrainte donne lieu à des objets algébriques et géométriques qui se comportent bien (au moins dans les petites dimensions).

Une telle étude est motivée par des résultats de géométrie hyperbolique : en un certain sens les homographies que l'on considère sont des isométries.

On détaille cette motivation dans l'annexe A.2 (page 25).

En effet, chaque forme modulaire admet un poids (entier), et pour un poids k fixé, les formes modulaires de poids k forment un espace vectoriel de dimension finie. Lorsque k est petit, on sait expliciter une base de cet espace, ce qui permet de réduire la détermination d'une forme modulaire de poids donné à une donnée finie sur cette forme modulaire.

Pour trouver une formule pour r_4, nous allons montrer que sa fonction génératrice exponentielle

$$\sum_{n\in\mathbf{Z}} r_4(n)\exp(2i\pi nz)$$

est une forme modulaire dans un espace dont on connaît une base explicite. La connaissance des quelques premiers coefficients de ce développement permettra alors de trouver une formule générale pour r_4.

Il nous faut donc introduire les notions nécessaires et des résultats élémentaires sur l'action des homographies sur le demi-plan de poincaré $\mathfrak{h} = \{\mathfrak{Im}z > 0\}$, sur les groupes et sous-groupes d'homographies, sur les quotients de tels groupes, et les conséquences sur les espaces de formes modulaires.

2.1 Formes modulaires

Définition (Groupe modulaire).

On appelle groupe modulaire le groupe $\mathrm{SL}_2(\mathbf{Z})$. Il agit à gauche par homographie sur le demi-plan de Poincaré

$$\mathfrak{h} = \{\mathfrak{Im}z > 0\} \subset \mathbf{C},$$

c'est à dire que pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, l'opération suivante définit une action de groupe :

$$\gamma \cdot z = \frac{az+b}{cz+d}.$$

La relation $\gamma \cdot z = (-\gamma)\cdot z$ nous invite dans certaines situations à travailler avec le groupe projectif (spécial) linéaire.

Définition (Groupe projectif linéaire).

On appelle groupe projectif (spécial) linéaire le groupe

$$\mathrm{PSL}_2(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}.$$

On définit de la même manière que pour le groupe modulaire l'action par homographie. Lorsque Γ est un sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$, on notera $\overline{\Gamma}$ le sous-groupe $\Gamma/\{\pm 1\}$ de $\mathrm{PSL}_2(\mathbf{Z})$.

Définition (Forme faiblement modulaire).

On peut aussi faire agir $\mathrm{GL}_2(\mathbf{R})$ (et donc $\mathrm{SL}_2(\mathbf{Z})$) sur l'ensemble des fonctions $\mathfrak{h} \longrightarrow \mathbf{C}$ avec, pour un entier k fixé,

$$f^{[\gamma]_k}(z) = (\det\gamma)^{k/2} j(\gamma,z)^{-k} f(\gamma\cdot z)$$

où $j(\gamma,z) = cz+d$ est appelé facteur de modularité. On dit qu'une fonction méromorphe $f : \mathfrak{h} \longrightarrow \mathbf{C}$ est faiblement modulaire de poids k lorsque $f^{[\gamma]_k} = f$ pour tout $\gamma \in \mathrm{SL}_2(\mathbf{Z})$

Proposition 2.1.1.

Le groupe modulaire est engendré par les matrices

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

Preuve. Une preuve constructive (et calculatoire) est donnée dans [Ser73]. □

Vérifier qu'une fonction méromorphe est faiblement modulaire revient donc à vérifier les deux relations suivantes :

$$\forall z \in \mathfrak{h}, \quad f(z+1) = f(z)$$
$$\forall z \in \mathfrak{h}, \quad f\left(-\frac{1}{z}\right) = (-z)^k f(z)$$

Remarque.

Il n'y a pas de forme faiblement modulaire non nulle de poids impair car si c'est le cas,

$$f(z) = f(-1 \cdot z) = (-1)^k f(z) = -f(z)$$

donc $f(z) = 0$. Plus généralement, il n'y a pas de fonction non nulle satsifaisant $f^{[-1]_k} = f$ lorsque k est impair.

Comme les formes faiblement modulaires sont 1-périodiques, ce sont des fonctions de $q = \exp(2i\pi z)$. Si f est faiblement modulaire et holomorphe, alors par inversion locale il existe $\widetilde{f}$ tel que $\widetilde{f}(q) = f(z)$ et $\widetilde{f}$ est holomorphe au voisinage épointé de 0 et par prolongement analytique, sur $\mathbf{B}(0,1) \setminus \{0\}$

Définition (Forme modulaire).

On dit qu'une forme faiblement modulaire f est une forme modulaire lorsqu'elle est holomorphe et que $\widetilde{f}$ est holomorphe en 0. On dit alors que f est holomorphe à l'infini.

2.2 Sous-groupes de congruence

Définition.

On dit que Γ est un sous-groupe de congruence si c'est un sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$ qui contient

$$\Gamma(N) = \ker(\mathrm{SL}_2(\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}))$$

pour un entier naturel $N \geqslant 2$. Les sous-groupes suivants sont des sous-groupes de congruence :

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), \quad a \equiv d \equiv 1 \pmod{N} \right\}.$$

L'entier N minimal tel que $\Gamma(N) \subset \Gamma$ est appelé *niveau* du sous-groupe de congruence Γ.

Remarque.

On désignera de manière équivalente le groupe modulaire par $\mathrm{SL}_2(\mathbf{Z})$ et par $\Gamma(1)$. De même, on utilisera la notation $\mathrm{PSL}_2(\mathbf{Z}) = \overline{\Gamma(1)}$

Il est clair que les sous-groupes de congruence ont un indice fini : ils contiennent $\Gamma(N)$ pour un certain N, et celui ci est un sous-groupe normal (c'est un noyau) tel que $\mathrm{SL}_2(\mathbf{Z})/\Gamma(N)$ s'injecte naturellement dans $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ qui est fini (le lemme suivant montre qu'il s'agit en fait d'un isomorphisme). On va calculer les indices des trois sous-groupes de congruence définis ci dessus (d'après [DS16, exercice 1.2.3]).

Lemme 1.

Si $f : \mathcal{M}_2(\mathbf{Z}) \longrightarrow \mathcal{M}_2(\mathbf{Z}/N\mathbf{Z})$ est l'application canonique de réduction modulo N (qui s'applique sur chaque coefficient), alors la suite suivante est exacte :

$$1 \longrightarrow \Gamma(N) \longrightarrow \mathrm{SL}_2(\mathbf{Z}) \xrightarrow{f} \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \longrightarrow 1.$$

Preuve. La seule difficulté est de montrer la surjectivité de la surjection canonique $\mathrm{SL}_2(\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ qu'on note f. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbf{Z})$ telle que $\overline{A} \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, c'est à dire telle que $ad - bc \equiv 1 \pmod{N}$. Alors, le théorème de Bézout donne $c \wedge d \wedge N = 1$. On pose

$$t = \prod_{\substack{p \mid c \\ p \nmid d}} p$$

et on se donne p premier divisant c.

Montrons que p ne divise pas $d' = d + tN$. Si p divise d, alors $p \nmid t$ et comme $p \mid c \wedge d$, $p \wedge N = 1$ donc p ne divise pas $d' = d + tN$.

Supposons à présent que $p \nmid d$, de sorte que $p \mid t$ donc $d' \equiv d \pmod{p}$ donc $p \mid d' \iff p \mid d$ donc p ne divise pas d'. Finalement, $c \wedge d' = 1$. Puis,

$$ad' - bc \equiv ad - bc \equiv 1 \pmod{N}$$

donc il existe k tel que

$$ad' - bc = 1 + kN$$

et il existe (u, v) tels que $cu + d'v = 1$, donc

$$d'(a - vkN) - c(b - ukN) = 1$$

et

$$A' = \begin{pmatrix} a - vkN & b + ukN \\ c & d + tN \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

est bien telle que $f(A') = f(A)$. □

Lemme 2.

Si p est premier et $\alpha > 0$ est un entier, alors

$$\#\,\mathrm{SL}_2(\mathbf{Z}/p^\alpha\mathbf{Z}) = p^{3\alpha}(1 - p^{-2})$$

Preuve. On procède par récurrence sur α.

- Si $\alpha = 1$, la suite
$$1 \longrightarrow \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \xrightarrow{\det} (\mathbf{Z}/p\mathbf{Z})^\times \longrightarrow 1$$
est exacte et $\#\,\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) = (p^2 - 1)(p^2 - p)$ (il suffit de compter les bases) donc
$$\#\,\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) = \frac{\#\,\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})}{\#(\mathbf{Z}/p\mathbf{Z})^\times} = p^3(1 - p^{-2})$$

- Si $\alpha > 1$, on note
$$\pi : \mathrm{SL}_2(\mathbf{Z}/p^\alpha\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/p^{\alpha-1}\mathbf{Z})$$
la réduction canonique (surjective par le lemme précédent). Les matrices de $\ker \pi$ sont de la forme
$$\begin{pmatrix} mp^{\alpha-1} + 1 & lp^{\alpha-1} \\ kp^{\alpha-1} & np^{\alpha-1} + 1 \end{pmatrix}$$
et telle que le déterminant vaut 1 modulo p^α, c'est à dire
$$(mp^{\alpha-1} + 1)(np^{\alpha-1} + 1) - klp^{2\alpha-2} \equiv p^{\alpha-1}(m + n) + 1 \equiv 1 \pmod{p^\alpha}$$

soit encore de manière équivalente, $p \mid m+n$. Cela laisse p choix pour $(mp^{\alpha-1}, np^{\alpha-1})$ (m et n sont déterminés mod p et la condition donne p^2/p solutions). Il y a p^2 choix pour $(lp^{\alpha-1}, kp^{\alpha-1})$ donc au total

$$\#\ker\pi = p^3$$

et

$$\#\,\mathrm{SL}_2(\mathbf{Z}/p^\alpha\mathbf{Z}) = p^3 p^{3\alpha-3}(1-p^{-2}) = p^{3\alpha}(1-p^{-2})$$

□

Proposition 2.2.1.

$$[\Gamma(1):\Gamma(N)] = N^3\prod_{p\mid N}(1-p^{-2})$$

$$[\Gamma(1):\Gamma_0(N)] = N\prod_{p\mid N}(1+p^{-1})$$

Preuve. Par définition de $\Gamma(N)$, $\mathrm{SL}_2(\mathbf{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Puis, si $N = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, le théorème chinois donne

$$\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \simeq \prod_{p_i\mid N}\mathrm{SL}_2(\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})$$

d'où on déduit immédiatement le premier indice avec le deuxième lemme.

Pour le second indice, on considère :

$$\begin{array}{rccc} \alpha: & \Gamma_1(N) & \longrightarrow & \mathbf{Z}/N\mathbf{Z} \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & b \pmod N \end{array}$$

$$\begin{array}{rccc} \beta: & \Gamma_0(N) & \longrightarrow & (\mathbf{Z}/N\mathbf{Z})^\times \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & a \pmod N \end{array}$$

qui sont des morphismes surjectifs de noyaux respectifs $\Gamma(N)$ et $\Gamma_1(N)$ de sorte que

$$[\mathrm{SL}_2(\mathbf{Z}):\Gamma_0(N)] = \frac{[\mathrm{SL}_2(\mathbf{Z}):\Gamma(N)]}{[\Gamma_0(N):\Gamma_1(N)][\Gamma_1(N):\Gamma(N)]} = \frac{N^3}{N\varphi(N)}\prod_{p\mid N}(1-p^{-2})$$

où φ est l'indicatrice d'Euler, qui s'exprime de la manière suivante :

$$\varphi(N) = N\prod_{p\mid N}(1-p^{-1}).$$

Un calcul immédiat permet de conclure. □

Remarque.

Comme $-1 \in \Gamma_0(N)$, le passage aux groupes projectifs ne modifie pas l'indice :

$$[\Gamma(1):\Gamma_0(N)] = [\overline{\Gamma(1)}:\overline{\Gamma_0(N)}].$$

On s'intéresse maintenant à la construction de représentants de classes à droite de $\Gamma(1)$ suivant $\Gamma_0(N)$. La proposition suivante (tirée de [Cre97] et [Ste07]) donne une méthode de construction.

Proposition 2.2.2.

Soient $M_1, M_2 \in \Gamma(1)$. Il y a équivalence entre

(1) $\Gamma_0(N)M_1 = \Gamma_0(N)M_2$

(2) $c_1d_2 \equiv c_2d_1 \pmod N$

(3) Il existe $u \in (\mathbf{Z}/N\mathbf{Z})^\times$ tel que $(c_1,d_1) \equiv (uc_2, ud_2) \pmod N$.

Preuve.

$$(1) \iff M_1 M_2^{-1} \in \Gamma_0(N)$$

or

$$M_1 M_2^{-1} = \begin{pmatrix} a_1 d_2 - b_1 c_2 & \star \\ c_1 d_2 - d_1 c_2 & a_2 d_1 - b_2 c_1 \end{pmatrix}$$

donc la condition d'appartenance à $\Gamma_0(N)$ pour le coefficient en bas à gauche donne directement (1) $\iff$ (2). On va montrer (1) $\implies$ (3). Vu les coefficients de $M_1 M_2^{-1}$ et son déterminant, $u = a_2 d_1 - b_2 c_1$ est premier avec N (il y a une relation de Bézout). Puis,

$$uc_2 = a_2 d_1 c_2 - b_2 c_1 c_2 \equiv a_2 d_2 c_2 - b_2 c_2 c_1 \pmod{N}$$

car $d_1 c_2 \equiv d_2 c_1 \pmod{N}$, puis en factorisant par c_1, le terme restant vaut 1. On fait la même chose pour $ud_2 \equiv d_1 \pmod{N}$.

Finalement, (3) $\implies$ (2) est immédiat. □

Définition (Symboles de Manin).

On appelle droite projective sur un anneau A l'ensemble

$$\mathbf{P}^1(A) = \{(a, b) \in A^2, \quad aA + bA = A\} / \sim$$

où $\sim$ est la relation d'équivalence définie par

$$(a, b) \sim (a', b') \iff \exists u \in A^\times, \quad (a', b') = (ua, ub).$$

On note $(a : b)$ la classe de (a, b) dans le quotient. On appelle **symboles de Manin** les éléments de $\mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$ lorsque N est fixé.

La proposition précédente a donc permi de mettre en évidence que pour tout système de représentants S, l'application

$$\psi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S \longmapsto (c : d) \in \mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$$

est bijective. Cela fournit donc une construction explicite de systèmes de représentants dès que l'on sait décrire $\mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$. On fera un tel calcul explicitement pour $N = 4$ plus tard.

Définition (Forme modulaire pour Γ).

Soit Γ un sous-groupe de congruence. On dit qu'une fonction $f : \mathfrak{h} \longrightarrow \mathfrak{h}$ est une forme faiblement modulaire de poids k pour Γ si

$$\forall \gamma \in \Gamma, \quad f^{[\gamma]_k} = f.$$

2.3 Pointes sous l'action d'un sous-groupe

Définition.

Soit Γ un sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$. On définit son action sur $\mathbf{P}^1(\mathbf{Q})$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \mathfrak{a} = \begin{cases} \dfrac{a}{d} & \text{si } \mathfrak{a} = \infty, \\ \infty & \text{si } c\,\mathfrak{a} + d = 0, \\ \dfrac{a\,\mathfrak{a} + b}{c\,\mathfrak{a} + d} & \text{sinon.} \end{cases}$$

Cette action est transitive.

Définition.

On note $\mathfrak{h}^\star = \mathfrak{h} \cup \mathbf{P}^1(\mathbf{Q})$ le demi-plan de Poincaré étendu. On muni cet ensemble de la topologie engendrée par les $B \cup \mathfrak{a}$ où $\mathfrak{a}$ est un rationnel et B est une boule ouverte tangente à la droite réelle en $\mathfrak{a}$.

Définition (Pointes pour un sous-groupe).

On note $C(\Gamma \setminus \mathfrak{h}^\star)$ l'ensemble des orbites de $\mathbf{P}^1(\mathbf{Q})$ sous l'action de Γ. On dit que c'est l'ensemble des pointes sous l'action de Γ.

Proposition 2.3.1.

Si Γ est un sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbf{Z})$, alors $C(\Gamma \setminus \mathfrak{h}^\star)$ est un ensemble fini.

Preuve. Le groupe $\mathrm{SL}_2(\mathbf{Z})$ est l'union (disjointe) de ses classes (à droite par exemple) modulo Γ. L'action de $\mathrm{SL}_2(\mathbf{Z})$ est transitive sur $\mathbf{P}^1(\mathbf{Q})$ donc

$$\mathbf{P}^1(\mathbf{Q}) = \mathrm{SL}_2(\mathbf{Z}).0 = \left(\bigcup_{i=1}^{m} \Gamma\gamma_i\right).0 = \bigcup_{i=1}^{m} \Gamma.(\gamma_i.0), \qquad m = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma],\ \{\gamma_i\} \text{ représentants}$$

et chacun des éléments de cette union est une orbite, l'union vaut tout l'ensemble de départ donc on les a toutes, il y en a donc au plus m. □

Définition (Largeur d'une pointe).

Lorsque Γ est un sous-groupe de congruence, on appelle largeur de la pointe $\alpha \in C(\Gamma)$ relativement à Γ l'entier

$$w_{\mathfrak{a}} = \min\{N \in \mathbf{N}^\star, \quad T^N \in \delta^{-1}\Gamma\delta\}$$

où $\delta \in \Gamma(1)$ est tel que $\delta(\infty) = \mathfrak{a}$.

Dans le cas des formes modulaires sur $\mathrm{SL}_2(\mathbf{Z})$, on avait trouvé un développement en série de Fourier à l'infini en utilisant que ces fonctions sont 1-périodiques. Si f est une forme faiblement modulaire de poids k pour Γ un sous-groupe de congruence, alors $f^{[\delta]_k}$ est une forme faiblement modulaire de poids k pour $\delta^{-1}\Gamma\delta$. Si $\mathfrak{a}$ est une pointe pour Γ, il existe $\delta \in \Gamma(1)$ tel que $\delta(\infty) = \mathfrak{a}$, donc $f^{[\delta]_k}$ est $w_{\mathfrak{a}}$-périodique et il existe $\widetilde{f}$ holomorphe sur un voisinage épointé de 0 telle que $\widetilde{f}(q^{\frac{1}{w_{\mathfrak{a}}}}) = f^{[\delta]_k}(z)$. On dit que f est holomorphe en $\mathfrak{a}$ si $\widetilde{f}$ est holomorphe en 0.

Définition (Forme modulaire).

Soit Γ un sous-groupe de congruence. On dit d'une fonction $f : \mathfrak{h} \longrightarrow \mathbf{C}$ que c'est une forme modulaire sur Γ si c'est une forme faiblement modulaire sur Γ qui est holomorphe en toutes les pointes $C(\Gamma)$.

Remarque.

De manière équivalente, une fonction $f : \mathfrak{h} \longrightarrow \mathbf{C}$ est une forme modulaire pour un sous-groupe de congruence Γ si elle satisfait aux trois conditions

(1) f est holomorphe.

(2) f est Γ-invariante pour un poids k.

(3) $f^{[\gamma]_k}$ est holomorphe à l'infini pour tout $\gamma \in \Gamma(1)$.

La condition (2) permet d'assurer que pour satisfaire (3), il suffit de vérifier l'holomorphie pour $\#C(\Gamma)$ matrices de $\Gamma(1)$ (des représentants de classes).

Proposition 2.3.2.

Soit f une forme faiblement modulaire de poids k pour le groupe de congruence Γ de niveau N. Alors, f admet un développement à l'infini du type

$$f(z) = \sum_{n \geqslant n_0} a_n q^{n/N}$$

On peut remplacer la condition (3) par

(3′) $n_0 \geqslant 0$ et $a_n = O(n^r)$ pour un $r > 0$.

Dans ce cas, la conjonction de (1), (2), et (3′) implique que f est une forme modulaire

Preuve. Voir [DS16, Exercice 1.2.6] □

2.4 Domaine fondamental

Définition (Domaine fondamental).

Soit Γ un sous-groupe de $\Gamma(1)$. On dit que $\mathcal{F}$ est un domaine fondamental pour Γ si c'est un ouvert qui s'intersecte au plus une fois avec chaque orbite pour l'action de Γ sur $\mathfrak{h}$, et dont l'adhérence s'intersecte au moins une fois avec chaque orbite.

Proposition 2.4.1.

L'ensemble décrit par

$$\mathcal{F} = \{|\mathfrak{Re}(z)| < 1/2\} \cap \{|z| > 1\}$$

est un domaine fondamental pour l'action du groupe modulaire $\Gamma(1)$.

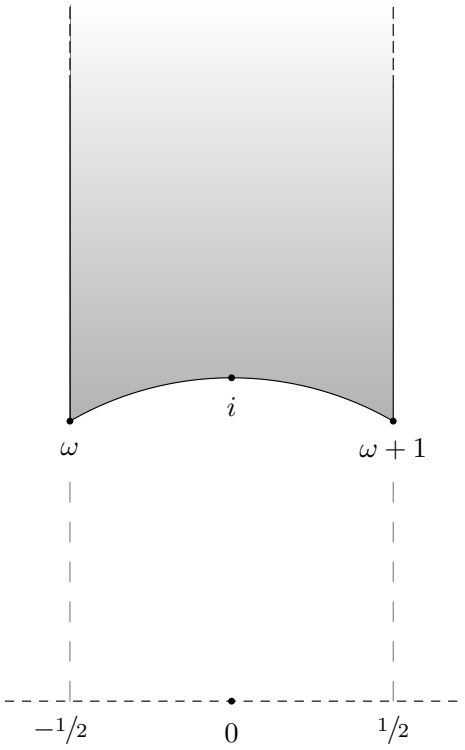


FIGURE 1 – Région $\mathcal{F}$ – Domaine fondamental canonique

Preuve. Soit $z \in \mathfrak{h}$. On note $c, d \in \mathbf{Z}$ des entiers tels que $cz + d$ est de norme minimale. Alors, c et d sont premiers entre eux et il existe $a, b \in \mathbf{Z}$ tels que $ad - bc = 1$ (Bézout) donc $\gamma_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \overline{\Gamma(1)}$. La quantité

$$\mathfrak{Im}(\gamma_1 z) = \frac{\mathfrak{Im}(z)}{|j(\gamma_1, z)|^2}$$

est maximale dans $\{\mathfrak{Im}(\gamma z), \quad \gamma \in \overline{\Gamma(1)}\}$. On pose $z^\star = T^n \gamma_1 z = \gamma_1 z + n$ avec $n \in \mathbf{Z}$ choisi tel que $|\mathfrak{Re}(z^\star)| \leqslant \frac{1}{2}$. Puis, $|z^\star| \geqslant 1$ car

$$\mathfrak{Im}\left(-\frac{1}{z^\star}\right) = \frac{\mathfrak{Im}(z^\star)}{|z^\star|^2} \leqslant \mathfrak{Im}(z^\star).$$

Ainsi, l'adhérence de D s'intersecte au moins une fois avec chaque orbite.

Soient $z_1, z_2 \in \mathcal{F}$ tels que $z_2 = \gamma z_1$ avec $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 1$. Vu la condition sur la partie réelle, γ n'est pas de la forme T^n donc $c \neq 0$ et

$$\frac{\sqrt{3}}{2} \leqslant \mathfrak{Im}(z_2) = \frac{\mathfrak{Im}(z_1)}{|j(\gamma, z_1)|^2} \leqslant \frac{\mathfrak{Im}(z_1)}{c^2 \mathfrak{Im}(z_1)^2} \leqslant \frac{2}{c^2\sqrt{3}}$$

donc $c = \pm 1$. On peut supposer que $\mathfrak{Im}(z_1) \leqslant \mathfrak{Im}(z_2)$ donc $|\pm z_1 + d| \geqslant |z_1| > 1$ et

$$\mathfrak{Im}(z_2) = \frac{\mathfrak{Im}(z_1)}{|\pm z_1 + d|^2} < \mathfrak{Im}(z_1)$$

ce qui est absurde. On en déduit que D s'intersecte au plus une fois avec chaque orbite. □

Proposition 2.4.2.

Soit Γ un sous-groupe d'indice fini dans $\Gamma(1)$. Alors,

$$\mathcal{F}_\Gamma = \bigcup_{i=1}^{m} \gamma_i \mathcal{F}, \quad m = [\overline{\Gamma(1)} : \overline{\Gamma}]$$

est un domaine fondamental pour Γ, lorsque les $\{\gamma_i\}$ forment un système de représentants de $\overline{\Gamma} \setminus \overline{\Gamma(1)}$.

Preuve. Pour un tel système de représentants, on écrit l'union disjointe

$$\overline{\Gamma(1)} = \bigcup_{i=1}^{m} \overline{\Gamma}\gamma_i$$

de sorte que chaque orbite pour $\Gamma(1)$ s'écrit

$$\overline{\Gamma(1)} \cdot z = \bigcup_{i=1}^{m} \overline{\Gamma}\gamma_i z$$

et on reconnaît les orbites de $\gamma_i z$ pour l'action de $\overline{\Gamma}$. Puis, l'orbite de $\gamma_i z$ sous l'action de $\overline{\Gamma(1)}$ s'intersecte au plus une fois avec $\gamma_i \mathcal{F}$, et cela reste vrai pour l'action de Γ (puisque c'est un sous-groupe de $\overline{\Gamma(1)}$). Si cette dernière s'intersecte avec $\gamma_j \mathcal{F}$, alors il existe $\gamma \in \Gamma$ tel que $\gamma\gamma_i z \in \gamma_j \mathcal{F}$ soit encore $\gamma_i \cdot z \in \gamma^{-1}\gamma_j \mathcal{F}$ et ce dernier domaine est un domaine fondamental pour $\overline{\Gamma(1)}$, donc par unicité, $\gamma_j \gamma_i^{-1} = \gamma \in \overline{\Gamma}$ et comme $\{\gamma_i\}$ est un système de représentants, $\gamma_i = \gamma_j$ et $i = j$. L'autre condition est immédiatement remplie, vu la description des orbites. □

On s'intéresse au cas particulier du sous-groupe de congruence $\Gamma_0(4)$, qui apparaît naturellement dans l'étude de la fonction θ de Jacobi. On a vu qu'un système de représentants des classes modulo $\Gamma_0(4)$ est en bijection naturelle avec $\mathbf{P}^1(\mathbf{Z}/4\mathbf{Z})$ (symboles de Manin) que l'on peut décrire ainsi :

$$\mathbf{P}^1(\mathbf{Z}/4\mathbf{Z}) = \{(0:1), (1:0), (1:1), (1:2), (1:3), (2:1)\}$$

Cela donne par exemple le système de représentants [1]

$$\begin{aligned} S &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\} \\ &= \{1, S^{-1}, S^{-1}T, S^{-1}T^{-2}, S^{-1}T^{-1}, S^{-1}T^{-2}S\} \end{aligned}$$

On peut ensuite représenter le domaine fondamental associé à ce système de représentants dans le demi plan de poincaré (Figure 2 page suivante)

1. Rappel : $(1:2) = (1:-2), (1:3) = (1:-1)$

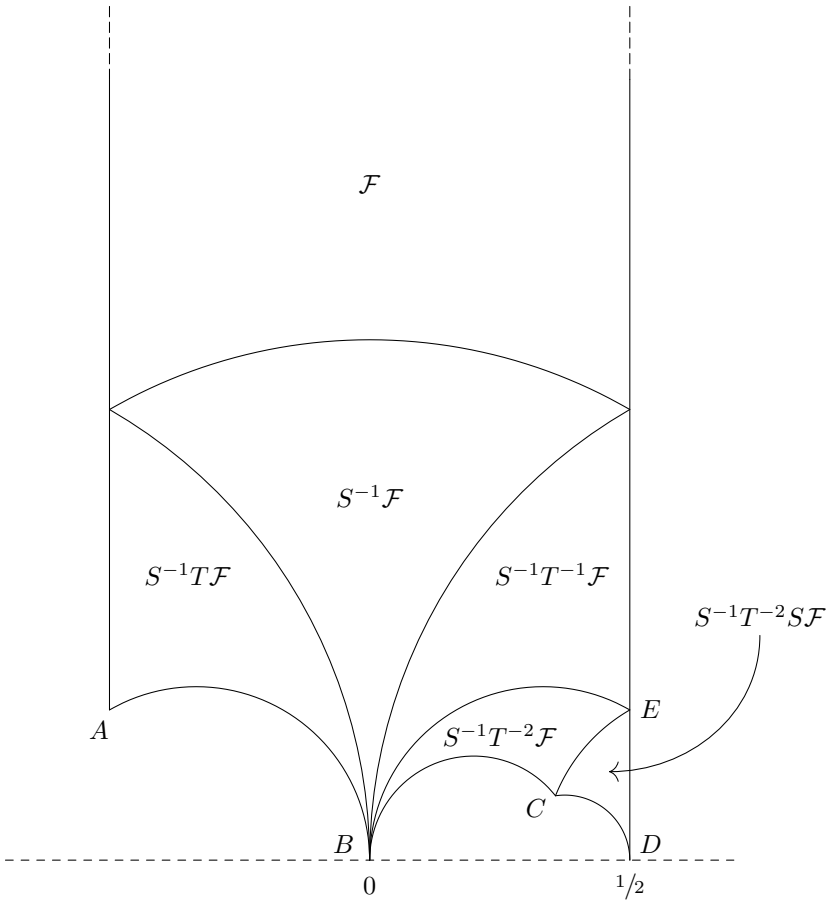


FIGURE 2 – Domaine fondamental pour $\Gamma_0(4)$

2.5 Formules de valence

Lorsque f est holomorphe, on appelle valuation au point P la quantité

$$v_P(f) = \min\{k \in \mathbf{N}, f^{(k)}(P) \neq 0\}.$$

Si de plus f est une forme modulaire pour Γ, cette valuation est invariante sur les orbites (par un rapide calcul de dérivée).

Si f est une forme modulaire pour Γ, alors elle est w_∞-périodique et donc admet un développement en série de Fourier en q^{1/w_∞}, c'est à dire qu'il existe $\widetilde{f} : \mathbf{B}(0,1) \longrightarrow \mathbf{C}$ holomorphe en 0 telle que $\widetilde{f}(q^{1/w_\infty}) = f(z)$ où $q = \exp(2i\pi z)$. On définit alors

$$v_\infty(f) = w_\infty v_0(\widetilde{f})$$

Si f est une forme modulaire pour Γ, et $\mathfrak{a} \in \mathbf{P}^1(\mathbf{Q})$ est une pointe, on se donne $\gamma \in \Gamma(1)$ tel que $\gamma(\infty) = \mathfrak{a}$ et l'on sait que $f^{[\gamma]_k}$ est holomorphe à l'infini. On définit alors

$$v_\mathfrak{a}(f) = \frac{w_\mathfrak{a}}{w_\infty} v_\infty(f^{[\gamma]_k}).$$

Il n'est pas évident que cette définition est indépendante du choix de γ. Pour le voir, on se donne $\beta \in \Gamma(1)$ tel que $\beta(\infty) = \mathfrak{a}$. Alors, $\gamma^{-1}\beta \in \mathrm{Stab}_{\Gamma(1)}(\infty)$ donc il existe j tel que $\gamma^{-1}\beta = \pm T^j$ et $\beta = \pm\gamma T^j$. Il reste à montrer que pour tout j, $v_\infty(f^{[\pm\gamma T^j]_k}) = v_\infty(f^{[\gamma]_k})$. Il suffit de remarquer

$$f^{[\pm\gamma T^j]_k}(z) = (\pm 1)^k f^{[\gamma]_k}(z + j),$$

d'où on peut exprimer le développement en série de Fourier de $f^{[\pm\gamma T^j]_k}$ en fonction de celui de $f^{[\gamma]_k}$ (voir [DS16, p. 17-18])

Proposition 2.5.1 (Formule de valence usuelle).

Pour toute forme modulaire non nulle de poids k sur $\Gamma(1)$, on a

$$\sum_{\substack{P\in\Gamma\backslash\mathfrak{h}\\ P\neq i,\omega}} v_P(f)+\frac{1}{3}v_\omega(f)+\frac{1}{2}v_i(f)+v_\infty(f)=\frac{k}{12}.$$

où $\omega=e^{2i\pi/3}$.

Preuve. Cette preuve est adaptée de [Zag08] et [Ser73]. Soit $\varepsilon>0$ tel que :

- L'ensemble des zéros de $\widetilde{f}$ sur $\mathbf{B}(0,e^{-2\pi\varepsilon^{-1}})$ est réduit à $\{0\}$ (toujours possible par locale finitude des zéros)
- Les $\mathbf{B}(z,\varepsilon)$ pour $z\in(Z(f)\cap\partial\mathcal{F})\cup\{\omega,i,\omega+1\}$ sont disjoints.

On considère le domaine

$$D=\overline{\mathcal{F}}\cap\{z\in\mathfrak{h},\quad \mathfrak{Im}(z)\leqslant\varepsilon^{-1}\}\setminus\left(\bigcup_{z\in Z(f)\cap\partial\mathcal{F}}\mathbf{B}(z,\varepsilon)\cup\{\omega,i,\omega+1\}\right)$$

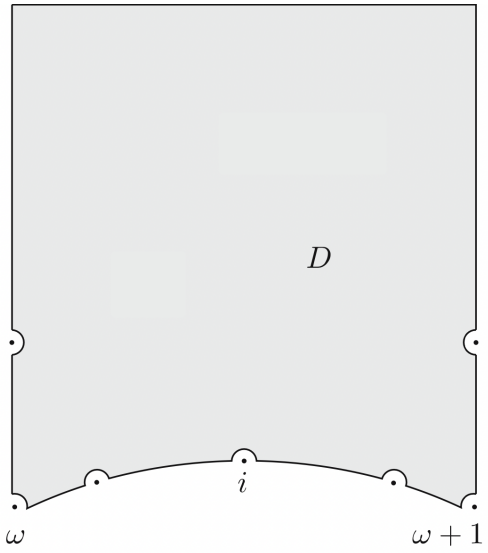


FIGURE 3 – Chemin d'intégration ∂D

de sorte que la fonction $\dfrac{f'}{f}$ est méromorphe sur D, qui est simplement connexe. On note γ le bord de D, orienté dans le sens trigonométrique, de sorte que le théorème des résidus donne

$$\frac{1}{2\pi i}\int_\gamma\frac{f'}{f}=\sum_{P\in D}\mathrm{Rés}_P\left(\frac{f'}{f}\right)=\sum_{P\in D}v_P(f).$$

On va calculer cette intégrale d'une autre manière.

- L'intégrale sur une demi-droite verticale (où l'on a enlevé les ε-boules autour des zéros) vaut l'opposé de l'intégrale sur l'autre, la somme des deux est donc nulle.
- L'intégrale sur le segment $S=i\varepsilon^{-1}+[-1/2,1/2]$ vaut

$$\frac{1}{2\pi i}\int_S\frac{f'}{f}=\frac{1}{2\pi i}\int_0^1\frac{\omega'(t)\widetilde{f}'(\omega(t))}{\widetilde{f}(\omega(t))}\mathrm{d}t=-\frac{1}{2\pi i}\int_{C(0,e^{-2\pi\varepsilon^{-1}})}\frac{\widetilde{f}}{f}=-v_0(\widetilde{f})=-v_\infty(f)$$

où $\omega(t)=e^{-2\pi\varepsilon^{-1}-2i\pi t}$ (le cercle est parcouru dans le sens horaire, d'où le signe)

- On paramètre l'arc de cercle autour de ω par $\rho(t) = \omega + e^{-2\pi\varepsilon^{-1} - i(2\pi t/6 + \theta(\varepsilon)) + i\pi/2}$ avec $\theta(\varepsilon) = o_{\varepsilon\to 0}(\varepsilon)$, et on note
$$\frac{f'}{f}(\omega + h) = \sum_{k=n}^{+\infty} \alpha_k h^k$$
le développement en série de Laurent au voisinage de ω, avec $n \leqslant 0$. Si $n = 0$,
$$\frac{1}{2i\pi}\int_0^1 \frac{f'}{f}(\rho(t))\rho'(t)\mathrm{d}t = O_{\varepsilon\to 0}(e^{-2\pi\varepsilon^{-1}})$$
car la fonction intégrée est holomorphe donc bornée au voisinage de ω. Sinon,
$$\begin{aligned}\frac{1}{2i\pi}\int_0^1 \frac{f'}{f}(\rho(t))\rho'(t)\mathrm{d}t &= \frac{1}{2i\pi}\int_0^1 \mathrm{Rés}_\omega\left(\frac{f'}{f}\right)\rho(t)^{-1}\rho'(t)\mathrm{d}t + O_{\varepsilon\to 0}(e^{-2\pi\varepsilon^{-1}}) \\ &= -\left(\frac{1}{6} + \frac{\theta(\varepsilon)}{2i\pi}\right)v_\omega(f) + O_{\varepsilon\to 0}(e^{-2\pi\varepsilon^{-1}}) \xrightarrow[\varepsilon\to 0]{} -\frac{1}{6}v_\omega(f)\end{aligned}$$
donc l'intégrale sur l'arc de cercle autour de ω tend vers $-\frac{1}{6}v_\omega(f)$. On retrouve une deuxième fois cette quantité pour $\omega + 1$, et pour i on trouve $-\frac{1}{2}v_i(f)$.
- Par le même principe, l'intégrale autour d'un zéro que l'on a enlevé tend vers
$$v_P(f)$$
car on intègre sur tout le cercle ou bien deux fois sur le demi cercle.
- Il reste à calculer l'intégrale sur l'arc de cercle entre ω et i (où l'on a enlevé les ε-voisinages des zéros de f). On a
$$\frac{(f\circ S)'(z)}{f(Sz)} = \frac{k}{z} + \frac{f'}{f}$$
et S envoie précisément cet arc sur l'arc entre i et $\omega + 1$ (en inversant le sens de parcours) donc
$$\frac{1}{2\pi i}\int_{\omega\to i}\frac{f'}{f} + \frac{1}{2\pi i}\int_{i\to\omega+1}\frac{f'}{f} = \frac{1}{2\pi i}\int_{\omega\to i}\underbrace{\left(\frac{f'(z)}{f(z)} - \frac{(f\circ S)'(z)}{f(Sz)}\right)}_{=-k/z} \xrightarrow[\varepsilon\to 0]{} \frac{k}{12}$$

Finalement, on a trouvé :
$$\sum_{\substack{P\in\Gamma_1\backslash\mathfrak{h}\\ P\notin\{\omega,i\}}} v_P(f) + \frac{1}{3}v_\omega(f) + \frac{1}{2}v_i(f) + v_\infty(f) = \frac{k}{12}$$
ce qui correspond bien à la formule recherchée. □

Cette version classique de la formule de valence est valable pour les formes modulaires non nulles sur $\Gamma(1)$. Pour chaque sous-groupe de congruence Γ, on peut trouver une telle formule. Pour ce faire, il est intéressant de remarquer le point suivant : dans la preuve du cas classique, nous avons perçu le domaine fondamental comme un quadrilatère hyperbolique dont les sommets sont $\{\infty, \omega, i, \omega + 1\}$. Puis, on a trouvé des éléments de $\Gamma(1)$ qui mettent en correspondance deux à deux les côtés de ce quadrilatère (S et T). Cela a donné lieu à des simplifications avantageuses pour le calcul de l'intégrale sur le bord.

Par ailleurs, les coefficients qui sont apparus devant la valuation de ω et i ont été perçus comme provenant des angles qui apparaissent dans le domaine fondamental. Ces angles sont directement liés au cardinaux des stabilisateurs dans $\overline{\Gamma(1)}$. Ces stabilisateurs sont tous conjugués au sein d'une même orbite $P \in \overline{\Gamma(1)}\backslash\mathfrak{h}$ et ont donc le même cardinal $n_{\overline{\Gamma(1)}}(P)$. On peut montrer que $n_{\overline{\Gamma(1)}}(P) = 1$ pour toutes les orbites sauf pour les exceptions suivantes : $n_{\overline{\Gamma(1)}}(\overline{\Gamma(1)}.i) = 2$ et $n_{\overline{\Gamma(1)}}(\overline{\Gamma(1)}.\omega) = 3$. On dit que les points de $\mathfrak{h}$ dont l'orbite n'a pas des stabilisateurs triviaux sont des *points elliptiques*. La formule s'écrit donc
$$v_\infty(f) + \sum_{P\in\overline{\Gamma(1)}\backslash\mathfrak{h}} \frac{v_P(f)}{n_{\overline{\Gamma(1)}}(P)} = \frac{k}{12}.$$

Lemme 1.

Si $M \in \Gamma$ et $f \in M_k(\Gamma)$, alors

$$\frac{(z \mapsto f(Mz))'(z)}{f(Mz)} = \frac{k}{j(M,z)} + \frac{f'}{f}(z)$$

Ce lemme permet le calcul suivant : si a et b sont des chemins tels qu'il existe $\gamma \in \overline{\Gamma}$ tel que γb est le chemin a parcouru dans le sens inverse, alors

$$\int_a \frac{f'}{f} + \int_b \frac{f'}{f} = -k \int_b j(\gamma, z)^{-1} \, \mathrm{d}z.$$

Dans le cas général, on peut toujours prendre pour domaine fondamental un polygone hyperbolique avec un nombre pair de côtés dont les côtés sont deux à deux Γ-équivalents (voir [Kat92], en particulier la fin de section 3.5 à partir du théorème 3.5.3), ce qui permet de dériver une formule de valence pour chaque sous-groupe Γ avec la même méthode de preuve que dans le cas général [Cha18, lemme 2.2.2 et remarque 2.2.1].

On peut, par ailleurs, trouver une formule de valence générale en appliquant la formule de valence usuelle à une forme modulaire bien choisie [Cha18, théorème 2.2.3] ou [Mas15, théorème 2.6.1]. C'est ce que l'on fait dans le théorème suivant.

Théorème 2.5.1 (Formule de valence généralisée).

Si f est une forme modulaire *non nulle* de poids k sur $\overline{\Gamma}$ sous-groupe de $\overline{\Gamma(1)}$, alors

$$\sum_{\mathfrak{a} \in C(\overline{\Gamma} \backslash \mathfrak{h})} v_{\mathfrak{a}}(f) + \sum_{P \in \overline{\Gamma} \backslash \mathfrak{h}} \frac{v_P(f)}{n_{\overline{\Gamma}}(P)} = \frac{k}{12} [\overline{\Gamma(1)} : \overline{\Gamma}]$$

Preuve. On pose

$$F = \prod_{\gamma \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} f^{[\gamma]_k}.$$

Dans le produit, le choix de représentant n'a pas d'importance car tous les $\gamma \in \Gamma$ stabilisent f pour l'action $f^{[\gamma]_k}$. F est une forme modulaire de poids $k[\overline{\Gamma(1)} : \overline{\Gamma}]$ sur $\Gamma(1)$ car $F(z+1) = F(z)$ et

$$\begin{aligned}
F^{[S]_{k[\overline{\Gamma(1)}:\overline{\Gamma}]}}(z) &= (-z)^{-k[\overline{\Gamma(1)}:\overline{\Gamma}]} \prod_{\gamma \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} (-\frac{c_\gamma}{z} + d_\gamma)^{-k} f(\gamma S z) \\
&= \prod_{\gamma \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} (-d_\gamma z + c_\gamma)^{-k} f(\gamma S z) \\
&= \prod_{\gamma \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} f^{[\gamma S]_k} \\
&= \prod_{\gamma S \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} f^{[\gamma]_k} = F(z)
\end{aligned}$$

car $\gamma_1 \gamma_2^{-1} \in \overline{\Gamma} \iff (\gamma_1 S)(\gamma_2 S)^{-1} \in \overline{\Gamma}$. Il reste maintenant à appliquer la formule de valence sur $\Gamma(1)$ à F. Pour $z \in \overline{\Gamma(1)} \setminus \mathfrak{h} = \mathcal{F}$,

$$\begin{aligned}
v_z(F) = v_z\left(\prod_{\gamma \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} f^{[\gamma]_k} \right) &= \sum_{\gamma \in \overline{\Gamma} \backslash \overline{\Gamma(1)}} v_z(f^{[\gamma]_k}) \\
&= \sum_{\omega \in (\overline{\Gamma} \backslash \overline{\Gamma(1)}) \cdot z} v_\omega(f) \times [\mathrm{Stab}_{\overline{\Gamma(1)}}(\omega) : \mathrm{Stab}_{\overline{\Gamma}}(\omega)]
\end{aligned}$$

Dans la dernière égalité, on a regroupé les γ tels que $\gamma z = \omega$. Puis,

$$[\mathrm{Stab}_{\overline{\Gamma(1)}}(\omega) : \mathrm{Stab}_{\overline{\Gamma}}(\omega)] = \frac{n_{\overline{\Gamma(1)}}(z)}{n_{\overline{\Gamma}}(\omega)}$$

d'où

$$\sum_{P\in\overline{\Gamma(1)}\backslash\mathfrak{h}} \frac{v_P(F)}{n_{\overline{\Gamma(1)}}(P)} = \sum_{P\in\overline{\Gamma}\backslash h} \frac{v_P(f)}{n_{\overline{\Gamma}}(P)}$$

Ensuite, comme $w_{\mathfrak{a}}/w_\infty$ est exactement $\#\{\gamma \in \overline{\Gamma} \setminus \overline{\Gamma(1)} \mid \gamma.\infty = \mathfrak{a}\}$

$$v_\infty(F) = \sum_{\gamma\in\overline{\Gamma}\setminus\overline{\Gamma(1)}} v_\infty(f^{[\gamma]_k}) = \sum_{\mathfrak{a}\in C(\Gamma)} \frac{w_{\mathfrak{a}}}{w_\infty} v_\infty(f^{[\delta]_k}) = \sum_{\mathfrak{a}\in C(\Gamma)} v_{\mathfrak{a}}(f).$$

□

2.6 Dimension des espaces de formes modulaires

Définition.

On note $M_k(\Gamma)$ l'ensemble des formes modulaires de poids k pour le groupe Γ. C'est un $\mathbf{C}$-espace vectoriel.

Proposition 2.6.1.

Soit Γ un sous-groupe de congruence. Alors,

$$\dim M_k(\Gamma) \leqslant \left\lfloor \frac{k[\overline{\Gamma(1)} : \overline{\Gamma}]}{12} \right\rfloor + 1.$$

Preuve. Notons $m = \lfloor k[\overline{\Gamma(1)} : \overline{\Gamma}]/12 \rfloor + 1$. Prenons m éléments de $\overline{\Gamma} \setminus \mathfrak{h}$ qui ne sont pas elliptiques (c'est-à-dire qu'on choisit des éléments dont les stabilisateurs sont triviaux), que l'on note $P_1, \cdots, P_m$. On se donne $z_1, \cdots, z_m$ des représentants des orbites que l'on a sélectionnées. Soient $f_1, \cdots, f_{m+1} \in M_k(\Gamma)$. La famille

$$\left(\begin{pmatrix} f_1(z_1) \\ \vdots \\ f_1(z_m) \end{pmatrix}, \cdots, \begin{pmatrix} f_{m+1}(z_1) \\ \vdots \\ f_{m+1}(z_m) \end{pmatrix} \right)$$

est liée (par un argument de dimension). Ainsi, il existe une combinaison linéaire non triviale des $(f_i)_{1\leqslant i\leqslant m+1}$ qui est nulle en tous les z_i (et donc sur tous les P_i), on la note f. Si f est non nulle, alors la formule de valence s'applique, et on obtient

$$\frac{k}{12}[\overline{\Gamma(1)} : \overline{\Gamma}] \geqslant m$$

ce qui est absurde. Donc, $f = 0$ et la famille des $(f_i)_{1\leqslant i\leqslant m+1}$ est liée. On en déduit que $M_k(\Gamma)$ est de dimension au plus m. □

3 Application à la détermination de r_k : la fonction θ

3.1 Fonction θ

La fonction θ introduite par Jacobi est définie par

$$\theta(z) = \sum_{n\in\mathbf{Z}} q^{n^2},$$

convergente sur le disque ouvert unité pour q (c'est à dire $\mathfrak{h}$ pour la variable z). Pour $k \in \mathbf{N}$, on note

$$\theta(z,k) = \theta(z)^k$$

de sorte que

$$\theta(z,k) = \sum_{n=0}^{+\infty} r_k(n) q^n.$$

Pour étudier les propriétés de modularité de cette fonction, on va utiliser la formule de sommation de Poisson [Sar90, énoncé 1.3.1].

Théorème 3.1.1 (Formule de sommation de Poisson).

Si $f : \mathbf{R}^d \longmapsto \mathbf{C}$ est une fonction de Schwartz, alors

$$\sum_{n\in\mathbf{Z}^d} f(n) = \sum_{n\in\mathbf{Z}^d} \widehat{f}(n)$$

où

$$\widehat{f}(\xi) = \int_{\mathbf{R}^d} e^{-2i\pi\langle t|\xi\rangle} f(t)\,\mathrm{d}t$$

Si $f(t) = \exp(-\pi t^2)$, alors $\widehat{f}(\xi) = \exp(-\pi\xi^2)$ (on dérive sous le signe $\int$ puis on résout l'équation différentielle). Puis, les $t \longmapsto f(\sqrt{y}t)$ pour $y > 0$ sont de Schwartz donc la formule de sommation donne, avec les règles de calcul sur les transformées de Fourier,

$$\sum_{n\in\mathbf{Z}} e^{-\pi n^2 y} = \frac{1}{\sqrt{y}} \sum_{n\in\mathbf{Z}} e^{-\pi n^2/y}$$

donc

$$\theta\left(-\frac{1}{4z}\right) = \sqrt{-2iz}\,\theta(z)$$

lorsque $z = iy/2$ avec $y > 0$. Cette relation reste vraie sur $\mathfrak{h}$ par prolongement analytique. Cette règle de transoformation n'est pas satisfaisante pour notre étude, en tant que $z \mapsto -\frac{1}{4z}$ n'est pas une homographie représentée par une matrice de $\mathrm{SL}_2(\mathbf{Z})$. Pour y remédier, on s'intéresse à l'homographie $z \mapsto \frac{z}{4z+1}$. On a alors

$$\theta\left(\frac{z}{4z+1}\right) = \theta\left(-\frac{1}{4(-1/4z-1)}\right) = \sqrt{2i\left(\frac{1}{4z}+1\right)}\,\theta\left(-\frac{1}{4z}-1\right) = \underbrace{\sqrt{2i\left(\frac{1}{4z}+1\right)(-2iz)}}_{=\sqrt{4z+1}}\,\theta(z)$$

donc θ^4 est une forme faiblement modulaire de poids 2 sur le groupe

$$\Gamma = \left\langle \pm\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}, \pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\rangle.$$

Clairement, Γ est inclus dans $\Gamma_0(4)$. On va vérifier algorithmiquement que l'autre inclusion est vraie. Soit $\gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \Gamma_0(4)$. On note

$$A = \begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix} \qquad T = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Alors, si $c = 0$, $\gamma = \pm T^{\pm b}$. Sinon, on remarque

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b' \\ c & nc+d \end{pmatrix}$$

donc on peut se ramener avec une matrice de Γ à une matrice telle que $|d'| < |c'|/2$ (l'inégalité est stricte car $4 \mid c'$ et $2 \nmid d'$). Ensuite,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4n & 1 \end{pmatrix} = \begin{pmatrix} a' & b \\ c+4nd & d \end{pmatrix}$$

donc on peut se ramener avec une matrice de Γ à un matrice dans laquelle $|c'| < 2|d'|$. En itérant ce procédé, la quantité $\max\{|c|, 2|d|\}$ diminue, donc le processus termine et cela montre $\Gamma_0(4) \subseteq \Gamma$.

La fonction θ^4 est donc faiblement modulaire de poids 2 sur $\Gamma_0(4)$. θ^4 est clairement holomorphe à l'infini (vu son développement de Fourier). Puis,

$$\theta\left(-\frac{1}{4z}\right) = \sqrt{-2iz}\theta(z)$$

donc

$$\theta(z) = O_{z\to 0}(|z|^{-1/2}).$$

Puis,

$$(\theta^4)^{[S]_2}(z) = z^2\theta\left(-\frac{1}{z}\right)^4 = O_{z\to\infty}(1)$$

donc θ est holomorphe en la pointe 0. Finalement, pour montrer que θ est holomorphe en $1/2$, on remarque d'abord que

$$\theta\left(z-\frac{1}{2}\right) = \sum_{n\in\mathbf{Z}} q^{n^2}(-1)^{n^2} = \sum_{n\in\mathbf{Z}} q^{4n^2} - \sum_{n\in\mathbf{Z}} q^{(2n+1)^2} = \theta(4z) - (\theta(z) - \theta(4z)) = 2\theta(4z) - \theta(z)$$

On en déduit, avec

$$\gamma = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \Gamma(1),$$

on a $\gamma(\infty) = 1/2$ et

$$\begin{aligned}
(\theta^4)^{[\gamma]_2}(z) &= (2z+1)^2\theta\left(\frac{z}{2z+1}\right)^4 \\
&= (2z+1)^2\left(2i\left(\frac{1}{2}+\frac{1}{4z}\right)\right)^2\theta\left(-\frac{1}{2}-\frac{1}{4z}\right)^4 \\
&= (2z+1)^2\left(2i\left(\frac{1}{2}+\frac{1}{4z}\right)\right)^2\left(2\theta\left(-\frac{1}{8z}\right)-\theta\left(-\frac{1}{4z}\right)\right) \\
&= O_{z\to\infty}(|z^2|\cdot(|z|^{-1/2})^4) = O_{z\to\infty}(1)
\end{aligned}$$

donc θ^4 est bien holomorphe en $1/2$. On a ainsi vérifié que θ^4 est holomorphe à l'infini, en 0 et en $1/2$, qui sont trois pointes non-$\Gamma_0(4)$-équivalentes. Il y a trois pointes pour $\Gamma_0(4)$, donc on a bien vérifié la condition.

Ainsi, $\theta^4 \in M_2(\Gamma_0(4))$ et de manière générale, $\theta^{2k} \in M_k(\Gamma_0(4))$.

3.2 Séries d'Eisenstein

Les séries d'Eisenstein fournissent un ingrédient de base pour la construction de formes modulaires. On note

$$G_k(z) = \sum_{\substack{c,d\in\mathbf{Z} \\ (c,z)\neq(0,0)}} \frac{1}{(cz+d)^k}$$

pour $k > 2$. L'ensemble $J_N = (\mathbf{Z}z + \mathbf{Z}) \cap \overline{\mathbf{B}}(0, N+1) \setminus \mathbf{B}(0, N)$ est l'ensemble des points de $\mathbf{Z}z + \mathbf{Z}$ compris dans la couronne comprise entre les cercles de rayons N et $N+1$, et est donc de cardinal

majoré .par $\pi(N+1)^2 - \pi N^2 = O(N)$. Ainsi, la série est majorée (à constante multiplicative près) par $\sum_{N\in\mathbf{N}} N^{1-k}$ qui converge pour $k > 2$. Il y a donc convergence simple. Puis, il y a convergence normale sur $\overline{\mathcal{F}} = \{|\mathfrak{Im} z| \leqslant 1/2\} \cap \{|z| \geqslant 1\}$ puisque

$$|cz+d|^2 = (cz+d)(c\overline{z}+d) \geqslant c^2|\omega| + 2|c||d|\mathfrak{Re}(\omega) + d^2 = ||c|\omega + |d||^2$$

avec $\omega = \exp(2i\pi/3)$ et qu'on a la convergence simple en ce point. On en déduit que G_k converge normalement sur tout compact, car $\{\gamma\overline{\mathcal{F}}, \gamma \in \Gamma(1)\}$ recouvre $\mathfrak{h}$ et que chaque point du demi-plan admet un voisinage qui ne s'intersecte qu'avec un nombre fini de translatés de la forme $\gamma\overline{\mathcal{F}}$ (cela vient de la finitude des stabilisateurs, voir [Kat92] pour une description des éléments elliptiques).

Proposition 3.2.1.

Pour $k \geqslant 4$ pair, et pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$,

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

Preuve. Le calcul repose sur un réarrangement des termes de la somme (autorisé puisque la convergence est absolue). Pour cela, on écrit

$$G_k\left(\frac{az+b}{cz+d}\right) = \sum_{\substack{(c',d')\in\mathbf{Z} \\ (c',d')\neq 0}} \frac{(cz+d)^k}{\left((c'a+d'c)\,z + (c'b+d'd)\right)^k}$$

et lorsque (c',d') parcourt $\mathbf{Z}^2\setminus\{0\}$, $(c'a+d'c, c'b+d'd) = (c',d')\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ aussi. On trouve immédiatement la formule. □

Définition (Somme de puissances de diviseurs).

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

Par 1-périodicité, G_k admet un développement en série de Fourier.

Proposition 3.2.2 (Développement en série de Fourier).

Pour $k \geqslant 4$ pair,

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

Preuve issue de [Ser73]. On a l'identité

$$\pi \operatorname{cotg} \pi z = \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right)$$

mais aussi

$$\pi \operatorname{cotg} \pi z = \pi\frac{\cos \pi z}{\sin \pi z} = i\pi\frac{q+1}{q-1} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi\sum_{n=0}^{\infty} q^n$$

donc

$$\frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right) = i\pi - 2i\pi\sum_{n=0}^{\infty} q^n$$

ce qui donne, après dérivations successives (k fois)

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

Puis,

$$\begin{aligned} G_k(z) &= \sum_{(c,d)\neq(0,0)} \frac{1}{(cz+d)^k} \\ &= 2\zeta(k) + 2\sum_{c=1}^{\infty}\sum_{d\in\mathbf{Z}} \frac{1}{(cz+d)^k} \\ &= 2\zeta(k) + \frac{2(-2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty}\sum_{a=1}^{\infty} d^{k-1}q^{ad} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n \end{aligned}$$

□

On en déduit finalement que G_k est une forme modulaire de poids k, car elle est faiblement modulaire, holomorphe, holomorphe à l'infini vu son développement (explicite) en série de Fourier.

3.3 Séries d'Eisenstein de poids 2

Pour donner un sens à G_2, on adopte la définition suivante, motivée par la proposition 3.2.2.

Définition.

$$G_2(z) = 2\zeta(2) - 8\pi^2\sum_{n=1}^{\infty}\sigma(n)q^n$$

où $\sigma = \sigma_1$.

On définit ainsi une fonction holomorphe sur $\mathfrak{h}$ (puisque $\sigma(n) = O(n^2)$ donc il y a convergence sur le disque ouvert unité pour q).

La même preuve qu'en proposition 3.2.2 montre que G_2 est donnée par l'expression

$$G_2(z) = \sum_{d\neq 0}\frac{1}{d^2} + \sum_{c\neq 0}\sum_{d\in\mathbf{Z}}\frac{1}{(cz+d)^2}$$

qui s'écrit aussi

$$G_2(z) = 2\sum_{d>0}\frac{1}{d^2} + 2\sum_{c>0}\sum_{d\in\mathbf{Z}}\frac{1}{(cz+d)^2}$$

Pour déterminer le comportement de cette fonction sous l'action de $\Gamma(1)$, on introduit une déformation pour $\varepsilon > 0$:

$$G_2^{\varepsilon}(z) = \sum_{(m,n)\neq 0}\frac{1}{(mz+n)^2|mz+n|^{2\varepsilon}}.$$

et on définit [2]

$$G_2^{\star}(z) = \lim_{\varepsilon\searrow 0} G_2^{\varepsilon}(z).$$

Par le même argument que pour la proposition 3.2.1,

$$G_2^{\varepsilon}\left(\frac{az+b}{cz+d}\right) = (cz+d)^2|cz+d|^{2\varepsilon}G_2^{\varepsilon}(z)$$

donc

$$G_2^{\star}\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 G_2^{\star}(z).$$

2. L'existence de cette limite est donnée par un résultat de continuité sous la somme pour $\varepsilon > -1/2$, suivant le même principe que les raisonnement qui vont suivre.

On pose, pour $\varepsilon > -1/2$,

$$I_\varepsilon(z) = \int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{(z+t)^2|z+t|^{2\varepsilon}}.$$

Alors,

$$G_2^\varepsilon(z) - 2\sum_{c>0} I_\varepsilon(cz) = 2\sum_{d>0} \frac{1}{d^{2(1+\varepsilon)}} + 2\sum_{c>0}\sum_{d\in\mathbf{Z}} \underbrace{\left[\frac{1}{(cz+d)^2|cz+d|^{2\varepsilon}} - \int_d^{d+1} \frac{\mathrm{d}t}{(cz+t)^2|cz+t|^{2\varepsilon}}\right]}_{=O(|cz+d|^{-3-2\varepsilon})}.$$

Montrons que le membre de droite est une quantité continue par rapport à $\varepsilon > -1/2$. L'application

$$J_{c,d,z} : \varepsilon \longmapsto \int_d^{d+1} \frac{\mathrm{d}t}{(cz+t)^2|cz+t|^{2\varepsilon}}$$

où $c > 0, z \in \mathfrak{h}, d \in \mathbf{Z}$ est continue car l'intégration se fait sur un segment (et l'intégrande est continu). Le terme entre crochets, que l'on note $f_z((c,d),\varepsilon)$ est donc une fonction mesurable telle que pour tous $(c,d) \in \mathbf{Z}^2$,

$$\varepsilon \longmapsto f_z((c,d),\varepsilon)$$

est continue. Puis, à $z \in \mathfrak{h}$ fixé il n'y a qu'un nombre fini de couples $(c,d) \in \mathbf{Z}^2$ tels que $|cz+d| < 1$ donc

$$|f_z((c,d),\varepsilon)| = O(|cz+d|^{-3-2\varepsilon_0})$$

où l'on impose $\varepsilon > \varepsilon_0 > -1/2$. On a donc continuité sous la somme, et un raisonnement identique donne la continuité par rapport à ε de la première somme (sur $d > 0$). Le membre de droite étant continu par rapport à $\varepsilon > -1/2$, il admet une limite en $\varepsilon = 0$ et celle ci est donnée en remplaçant ε par 0 dans l'expression. On obtient alors

$$G_2^\star(z) - 2\lim_{\varepsilon\searrow 0}\sum_{c>0} I_\varepsilon(cz) = 2\sum_{d>0}\frac{1}{d^2} + 2\sum_{c>0}\sum_{d\in\mathbf{Z}}\left[\frac{1}{(cz+d)^2} - \int_d^{d+1}\frac{\mathrm{d}t}{(cz+t)^2}\right].$$

Or,

$$\sum_{c>0}\sum_{d\in\mathbf{Z}}\int_d^{d+1}\frac{\mathrm{d}t}{(cz+d)^2} = \sum_{c>0}\underbrace{\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{(cz+t)^2}}_{=0} = 0$$

d'où

$$G_2^\star(z) - 2\lim_{\varepsilon\searrow 0}\sum_{c>0} I_\varepsilon(cz) = G_2(z).$$

Par ailleurs,

$$\begin{aligned} I_\varepsilon(x+iy) &= \int_{-\infty}^{\infty}\frac{\mathrm{d}t}{(x+t+iy)^2\left((x+t)^2+y^2\right)^\varepsilon} \\ &= \int_{-\infty}^{\infty}\frac{\mathrm{d}t}{(t+iy)^2\left(t^2+y^2\right)^\varepsilon} = \frac{I(\varepsilon)}{y^{1+2\varepsilon}} \end{aligned}$$

où

$$I(\varepsilon) = \int_{-\infty}^{\infty}(t+i)^{-2}\left(t^2+1\right)^{-\varepsilon}\mathrm{d}t$$

donc

$$\sum_{c>0} I_\varepsilon(cz) = \sum_{c\neq 0}\frac{I(\varepsilon)}{c^{1+2\varepsilon}y^{1+2\varepsilon}} = \frac{I(\varepsilon)}{y^{1+2\varepsilon}}\zeta(1+2\varepsilon)$$

mais I étant une fonction $\mathcal{C}^1$ telle que $I(0) = 0, I'(0) = -\pi$ et avec $\zeta(1+2\varepsilon) = \dfrac{1}{2\varepsilon} + O(1)$ on obtient

$$\frac{I(\varepsilon)}{y^{1+2\varepsilon}}\zeta(1+2\varepsilon) \xrightarrow[\varepsilon\searrow 0]{} -\frac{\pi}{2y}$$

et finalement,

$$G_2^\star(z) = G_2(z) - \frac{\pi}{\mathfrak{Im}(z)}.$$

On vérifie par le calcul (avec $z = x + iy$) la relation

$$\frac{\pi}{j(\gamma,z)^2\mathfrak{Im}(\gamma z)} = \frac{\pi}{\mathfrak{Im}(z)} - \frac{2\pi i c}{j(\gamma,z)},$$

d'où la proposition suivante.

Proposition 3.3.1.

$$G_2^{[\gamma]_2}(z) = G_2(z) - \frac{2\pi i c}{j(\gamma,z)}.$$

Proposition 3.3.2.

Pour $N > 0$ entier,

$$G_{2,N}(z) = G_2(z) - NG_2(Nz)$$

définit une forme modulaire de $M_2(\Gamma_0(N))$.

Preuve. Soit $\gamma \in \Gamma_0(N)$. Alors,

$$N\gamma z = \frac{Naz + Nb}{cz + d} = \frac{a(Nz) + bN}{{}^c\!/_N(Nz) + d} = \underbrace{\begin{pmatrix} a & bN \\ {}^c\!/_N & d \end{pmatrix}}_{=\gamma'}(Nz)$$

où $\gamma' \in \Gamma(1)$. Donc,

$$\begin{aligned} G_{2,N}^{[\gamma]_2}(z) &= G_2(z) - \frac{2\pi i c}{j(\gamma,z)} - Nj(\gamma,z)^{-2}G_2(N\gamma z) \\ &= G_2(z) - \frac{2\pi i c}{j(\gamma,z)} - N\underbrace{j(\gamma,z)^{-2}j(\gamma',Nz)^2}_{=1}G_2(z) + \frac{2i\pi N^{c}\!/_N}{j(\gamma',Nz)} \\ &= G_{2,N}(z) \end{aligned}$$

La fonction est clairement holomorphe à l'infini (vu son développement de Fourier). Puis, les coefficients du développement de Fourier sont majorés (à une constante multiplicative près) par $\sigma(n) = O(n^2)$. Donc, par la propriété 2.3.2, $G_{2,N} \in M_2(\Gamma_0(N))$. □

3.4 Détermination de r_4

L'espace $M_2(\Gamma_0(4))$ est un espace de dimension majorée par

$$\left\lfloor \frac{k \cdot [\overline{\Gamma(1)} : \overline{\Gamma_0(4)}]}{12} \right\rfloor + 1 = \left\lfloor \frac{2 \cdot 6}{12} \right\rfloor + 1 = 2$$

Puis, on connaît l'existence de deux formes modulaires dans cet espace : $G_{2,2}$ et $G_{2,4}$ dont on vérifie facilement qu'elles forment une famille libre (en regardant par exemple les premiers coefficients du développement en série de Fourier). On a donc trouvé une base. Puis, on sait que

$$\theta(z,4) = 1 + 8q + \cdots$$

et on connaît les développements de Fourier de $G_{2,2}$ et $G_{2,4}$:

$$G_{2,2}(z) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{\substack{0<d|n \\ 2\nmid d}} d\right)q^n\right), \qquad G_{2,4}(z) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{\substack{0<d|n \\ 4\nmid d}} d\right)q^n\right)$$

donc on peut immédiatement identifier :

$$\theta^4 = -\frac{1}{\pi^2}G_{2,4}$$

d'où finalement pour n non nul,

$$r_4(n) = 8 \sum_{\substack{0<d|n \\ 4\nmid d}} d$$

Cela conclut la preuve du **Théorème de Jacobi**.

Annexe

A Éléments de géométrie hyperbolique

L'étude de l'action de $\mathrm{SL}_2(\mathbf{Z})$ sur le demi-plan de Poincaré est naturelle dès lors que l'on assimile ce groupe aux isométries du plan hyperbolique.

A.1 Distance hyperbolique

On se place dans le demi-plan de Poincaré $\mathfrak{h}$, que l'on munit de la métrique

$$\mathrm{d}s = \frac{\sqrt{\mathrm{d}x^2 + \mathrm{d}y^2}}{y}.$$

On dit alors que $\mathfrak{h}$ est un modèle du plan hyperbolique. La longueur d'un chemin $\gamma : [0,1] \to \mathfrak{h}$ dérivable par morceaux est donnée par

$$\ell(\gamma) = \int_\gamma |\,\mathrm{d}s| = \int_0^1 \frac{|\frac{\mathrm{d}z}{\mathrm{d}t}|\,\mathrm{d}t}{y(t)}.$$

La distance hyperbolique entre deux points est donc donnée par

$$d(a,b) = \min_{\gamma : a \to b} \ell(\gamma)$$

et ce minimum est atteint par les géodésiques qui sont exactement les demi-cercles (au sens euclidien) dont le centre est sur la droite réelle, ainsi que les droites verticales.

A.2 Isométries hyperboliques

Soit

$$T : z \in \mathfrak{h} \longmapsto \frac{az+b}{cz+d}$$

une homographie telle que a, b, c, d sont des réels qui satisfont à $\Delta = ad - bc > 0$. Remarquons qu'il est équivalent de supposer $\Delta = ad - bc = 1$ en divisant le numérateur et le dénominateur par $\sqrt{\Delta}$. Remarquons aussi que changer tous les signes de a, b, c, d ne change pas T. Il y a donc une surjection naturelle de $\mathrm{PSL}_2(\mathbf{R})$ dans l'ensemble des homographies du type de T. C'est aussi une bijection (une fonction rationnelle est déterminée par ses zéros et pôles, leur ordre et un coefficient réel qui est lui-même fixé par la condition sur le déterminant).

Alors, T est une isométrie hyperbolique, c'est-à-dire que T conserve la distance hyperbolique. Pour le voir, on se donne γ un chemin dérivable par morceaux, et l'on décompose γ et $T(\gamma)$ de la manière suivante :

$$\gamma : z(t) = x(t) + iy(t) \qquad\qquad T(\gamma) : w(t) = u(t) + iv(t).$$

Cela donne

$$\frac{\mathrm{d}w}{\mathrm{d}z}(z) = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{1}{(cz+d)^2}$$

et un calcul rapide donne

$$v = \frac{y}{(cz+d)^2}$$

donc

$$\left|\frac{\mathrm{d}w}{\mathrm{d}z}\right| = \frac{v}{y}$$

d'où finalement

$$\ell(T(\gamma)) = \int_0^1 \frac{|\frac{\mathrm{d}w}{\mathrm{d}t}|\,\mathrm{d}t}{v(t)} = \int_0^1 \frac{|\frac{\mathrm{d}w}{\mathrm{d}z}\frac{\mathrm{d}z}{\mathrm{d}t}|\,\mathrm{d}t}{v(t)} = \int_0^1 \frac{|\frac{\mathrm{d}z}{\mathrm{d}t}|\,\mathrm{d}t}{y(t)} = \ell(\gamma).$$

Ainsi, $\mathrm{PSL}_2(\mathbf{R})$ s'assimile naturellement à un sous-groupe du groupe des isométries hyperboliques (on dit que ce sont celles qui préservent l'orientation). On peut montrer (voir [Kat92, théorème 1.3.1]) que

les isométries hyperboliques sont engendrées par $\mathrm{PSL}_2(\mathbf{R})$ et par $z \mapsto -\overline{z}$ et que ce groupe est isomorphe à $\mathrm{PS}^\star\mathrm{L}_2(\mathbf{R}) = \mathrm{S}^\star\mathrm{L}_2(\mathbf{R})/\{\pm 1\}$ où $\mathrm{S}^\star\mathrm{L}_2(\mathbf{R}) = \ker(|\det|)$.

L'étude de l'action de $\mathrm{PSL}_2(\mathbf{R})$ sur $\mathfrak{h}$ est donc en réalité l'étude de l'action des isométries sur le plan hyperbolique.

Les isométries envoient les géodésiques sur des géodésiques, et conservent la mesure des angles en valeur absolue. Une isométrie est conforme lorsqu'elle conserve tous les angles, anticonforme si elle les renverse tous. Alors d'après [Kat92, thm 1.3.2], $\mathrm{PSL}_2(\mathbf{R})$ décrit toutes les isométries conformes, et les autres sont anticonformes.

A.3 Gauss-Bonnet et volume du domaine fondamental

Si $A \subset \mathfrak{h}$, on appelle volume de A (ou aire hyperbolique) la quantité

$$\mu(A) = \int_A \frac{\mathrm{d}x\,\mathrm{d}y}{y^2}$$

lorsque cette intégrale existe. Ce volume est invariant par isométrie hyperbolique.

On note $\widetilde{\mathfrak{h}} = \mathfrak{h} \cup \mathbf{R} \cup \{\infty\}$ que l'on appelle cloture de $\mathfrak{h}$. On dit d'une partie A que c'est un polygone hyperbolique si c'est une partie connexe et que sa frontière ∂A est une réunion finie de géodésiques. Les points d'intersection de ces géodésiques (dans $\widetilde{\mathfrak{h}}$) sont appelés sommets de A.

La formule de Gauss-Bonnet donne le volume d'un triangle hyperbolique

Théorème A.3.1 (Gauss-Bonnet).

L'aire d'un triangle hyperbolique dont les angles aux sommets ont les mesure α, β, γ est

$$\pi - \alpha - \beta - \gamma$$

Cela donne automatiquement l'aire du domaine fondamental canonique

$$\mu(\mathcal{F}) = \pi - \frac{2\pi}{3} = \frac{\pi}{3}$$

car $\mathcal{F}$ est le triangle hyperbolique de sommets $\omega, \omega+1, \infty$. Puis, on peut toujours décrire un domaine fondamental pour un sous-groupe de congruence Γ comme une réunion disjointe (sauf en un ensemble d'aire nulle : les bords des triangles) de translatés de $\mathcal{F}$ qui sont au nombre de $[\overline{\Gamma(1)} : \overline{\Gamma}]$ et qui ont tous le même volume (car les translatés sont des images par une isométrie). Ainsi, le volume d'un domaine fondamental pour Γ est

$$\frac{\pi}{3}[\overline{\Gamma(1)} : \overline{\Gamma}]$$

donc on pourraît réécrire la formule de valence

$$\sum_{\mathfrak{a} \in C(\overline{\Gamma}\backslash\mathfrak{h})} v_{\mathfrak{a}}(f) + \sum_{P \in \overline{\Gamma}\backslash\mathfrak{h}} \frac{v_P(f)}{n_{\overline{\Gamma}}(P)} = \frac{k\mu(\mathcal{F}_\Gamma)}{4\pi}.$$

Références

[Cha18] Lok-yin Chan. "Some results on modular forms : valence formulas, Eisenstein series, vector-valued L-functions". Pages : 991044046591503414. Master of Philosophy. Pokfulam Road, Hong Kong SAR : The University of Hong Kong, 2018. doi : 10.5353/th_991044046591503414. url : https://hdl.handle.net/10722/263184 (visité le 14/06/2022).

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. 2nd ed. Cambridge ; New York : Cambridge University Press, 1997. 376 p. isbn : 978-0-521-59820-0.

[DS16] Fred Diamond et Jerry Michael Shurman. *A first course in modular forms*. corrected 4th printing. Graduate texts in mathematics, 228. New York : Springer, 2016. 450 p. isbn : 978-0-387-23229-4 978-1-4419-2005-8.

[Kat92] Svetlana Katok. *Fuchsian Groups*. Chicago Lectures in Mathematics. Chicago, IL : University of Chicago Press, août 1992. 186 p. isbn : 978-0-226-42583-2. url : https://press.uchicago.edu/ucp/books/book/chicago/F/bo3621076.html (visité le 17/06/2022).

[Mas15] Marc Masdeu. *Modular Forms (MA4H9)*. Warwick University, 2015. URL : https://mat.uab.cat/~masdeu/wp-content/uploads/2020/02/ModularForms.pdf (visité le 17/06/2022).

[Per96] Daniel Perrin. *Cours d'algèbre*. CAPES-agrég mathématiques. Paris : Ellipses, 1996. 207 p. ISBN : 978-2-7298-5552-9.

[Sar90] Peter Sarnak. *Some Applications of Modular Forms*. Cambridge Tracts in Mathematics. Cambridge : Cambridge University Press, 1990. ISBN : 978-0-521-40245-3. DOI : 10.1017/CBO9780511895593. URL : https://www.cambridge.org/core/books/some-applications-of-modular-forms/0B35D286F528A1D15B2CF0300D60C25A (visité le 25/05/2022).

[Ser73] Jean-Pierre Serre. *A course in arithmetic*. Nachdr. Graduate texts in mathematics 7. New York Berlin Heidelberg : Springer, 1973. 115 p. ISBN : 978-3-540-90040-5 978-0-387-90040-7.

[Ste07] William A. Stein. *Modular forms, a computational approach*. Graduate studies in mathematics v. 79. OCLC : ocm72354890. Providence, R.I : American Mathematical Society, 2007. 268 p. ISBN : 978-0-8218-3960-7.

[Ven22] B Venkov. "Sur l'arithmétique des quaternions. (Première communication)". In : *Bulletin de l'Académie des Sciences de Russie* 16 (1922), p. 205-220. URL : http://mi.mathnet.ru/izv5706.

[Zag08] Don Zagier. "Elliptic Modular Forms and Their Applications". In : *The 1-2-3 of Modular Forms : Lectures at a Summer School in Nordfjordeid, Norway*. Sous la dir. de Jan Hendrik Bruinier et al. Universitext. Berlin, Heidelberg : Springer, 2008, p. 1-103. ISBN : 978-3-540-74119-0. DOI : 10.1007/978-3-540-74119-0_1. URL : https://doi.org/10.1007/978-3-540-74119-0_1 (visité le 12/06/2022).