

INTRODUCTION AUX FORMES MODULAIRES

GAËTAN CHENEVIER

LEÇON À L'ÉCOLE NORMALE SUPÉRIEURE (4H), MARS 2015

INTRODUCTION

Les ¹ formes modulaires sont des fonctions holomorphes sur le demi-plan de Poincaré qui se transforment de manière particulière sous l'action du groupe modulaire $SL_2(\mathbb{Z})$. Elles interviennent de façon plus ou moins naturelle dans plusieurs domaines assez différents des mathématiques : théorie des fonctions elliptiques, théorie des formes quadratiques à coefficients entiers, théorie des représentations unitaires du groupe de Lie $SL_2(\mathbb{R})$, fonctions L et représentations du groupe de Galois absolu de \mathbb{Q} ... Elles ont aussi été l'objet de plusieurs conjectures célèbres, comme la conjecture de Ramanujan ou la conjecture de Shimura-Taniyama-Weil. Aborder chacun de ces thèmes dans une si courte leçon est bien entendu impossible. Aussi, l'objectif que nous avons choisi est de montrer par des exemples que les coefficients de Fourier des formes modulaires renferment des informations arithmétiques intéressantes. En particulier, nous verrons comment utiliser des formes modulaires pour déterminer le nombre des représentations d'un entier comme somme de 8 carrés (Jacobi). On rapporte qu'Eichler aurait dit un jour que les formes modulaires constituent la 5ème opération de l'arithmétique (après l'addition, la soustraction, la multiplication et la division). Certains exemples, on l'espère!, illustreront la pensée d'Eichler.

TABLE DES MATIÈRES

Introduction	1
1. Action de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré	3
2. Formes modulaires pour $SL_2(\mathbb{Z})$	5
3. Sur les zéros des formes modulaires	7
4. Quelques q-développements	10
5. La fonction ϑ de Jacobi	11
6. Formes modulaires pour un sous-groupe de $SL_2(\mathbb{Z})$	14
7. Le ϑ -groupe est de congruence	15
8. Sommes de 8 carrés	16

Références : R. Busam & E. Freitag, *Funktionentheorie*,
Henri Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*,
Jean-Pierre Serre, *Cours d'arithmétique*,
Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*.

1. Je remercie A. Minguez pour ses remarques sur ce texte. L'auteur est financé par le CNRS.

1. ACTION DE $\mathrm{SL}_2(\mathbb{Z})$ SUR LE DEMI-PLAN DE POINCARÉ

1.1. Rappelons que pour tout corps K le groupe $\mathrm{GL}_2(K)$ agit naturellement sur K^2 , puis sur l'ensemble $\mathbb{P}^1(K)$ des droites vectorielles de ce dernier. Une application linéaire préservant toutes les droites étant une homothétie, cette action se factorise en une action fidèle du groupe quotient $\mathrm{PGL}_2(K)$ de $\mathrm{GL}_2(K)$ par K^\times . On pose

$$\widehat{K} = K \coprod \{\infty\}.$$

Cet ensemble s'identifie à $\mathbb{P}^1(K)$ en envoyant tout élément $z \in K$ sur la droite engendrée par $\begin{pmatrix} z \\ 1 \end{pmatrix}$, et le symbole ∞ sur celle engendrée par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Par transport de structure, on en déduit une action de $\mathrm{GL}_2(K)$ sur \widehat{K} , que l'on notera $(\gamma, z) \mapsto \gamma z$. Concrètement, si γ désigne l'élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(K)$, et si $z \in K$ est tel que $cz + d \neq 0$, on constate les égalités

$$(1) \quad \gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az + b \\ cz + d \end{pmatrix} = (cz + d) \begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix},$$

et l'on retrouve la formule bien connue $\gamma z = \frac{az+b}{cz+d}$. De plus, si on a $c \neq 0$ (resp. $c = 0$) alors on a $\gamma \infty = a/c$ et $\gamma(-d/c) = \infty$ (resp. $d \neq 0$ et $\gamma \infty = \infty$). Ces bijections de \widehat{K} sont appelées homographies, et forment donc un sous-groupe isomorphe à $\mathrm{PGL}_2(K)$. Par exemple $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ correspond à l'homographie "affine" $z \mapsto az + b$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ à l'inversion $z \mapsto -1/z$.

Pour utilisation future, mentionnons que l'élément $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(K)$ étant donné, l'application $z \mapsto cz + d, K \rightarrow K$, sera notée $j(\gamma, z)$. La formule (1) ci-dessus montre la relation dite de "cocycle" :

$$j(\gamma\gamma', z) = j(\gamma, \gamma'z)j(\gamma', z),$$

valable pour tout $\gamma, \gamma' \in \mathrm{GL}_2(K)$ et tout $z \in K$.

1.2. Ces rappels s'appliquent à $K = \mathbb{C}$, auquel cas $\widehat{\mathbb{C}}$ n'est autre que la *sphère de Riemann*. Le sous-groupe $\mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ agit par restriction sur cette sphère, en préservant \mathbb{R} , ainsi donc son complémentaire $\mathbb{C} - \mathbb{R}$. Cet ouvert de \mathbb{C} a deux composantes connexes, l'une d'elles étant l'ouvert

$$\mathbb{H} = \{\tau \in \mathbb{C}, \mathrm{Im} \tau > 0\},$$

appelé *demi-plan de Poincaré*. Si γ est l'élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(\mathbb{R})$, et si $z \in \mathbb{C} - \mathbb{R}$, alors on a $cz + d \neq 0$ et un calcul immédiat montre l'égalité

$$(2) \quad \mathrm{Im} \gamma z = \det \gamma \frac{\mathrm{Im} z}{|cz + d|^2}.$$

En particulier, l'action par homographies du groupe $\mathrm{SL}_2(\mathbb{R})$ préserve le demi-plan de Poincaré. L'action des homographies de la forme $a\tau + b$ avec $a \in \mathbb{R}_{>0}$ et $b \in \mathbb{R}$, montre que l'action de $\mathrm{SL}_2(\mathbb{R})$ sur \mathbb{H} est transitive. Nous n'en aurons pas besoin, mais signalons que l'on vérifierait sans difficulté que le stabilisateur de l'élément $i \in \mathbb{H}$ est le sous-groupe $\mathrm{SO}_2(\mathbb{R})$ usuel, et donc que $\gamma \mapsto \gamma i$ induit une bijection $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \xrightarrow{\sim} \mathbb{H}$.

Ces homographies ont des propriétés géométriques remarquables, particulièrement lumineuses lorsqu'on les étudie du point de vue de la géométrie hyperbolique (où nous ne nous aventurerons pas!). Par exemple, notons \mathcal{C} l'ensemble des parties de \mathbb{H} qui sont soit de la forme $\mathrm{Re} \tau = a$ (droites verticales), soit un demi-cercle de centre dans \mathbb{R} . Alors $\mathrm{SL}_2(\mathbb{R})$ préserve \mathcal{C} . Pour le voir, il suffit d'observer que les éléments de \mathcal{C} sont exactement les parties non vides de \mathbb{H} de la forme $\alpha + \beta \mathrm{Re} \tau + \gamma |\tau|^2 = 0$ avec $(\alpha, \beta, \gamma) \in \mathbb{R}^3 - \{0\}$. La vérification de l'assertion précédente est alors un simple exercice; il suffit même de le vérifier pour les homographies $\tau \mapsto \tau + \lambda$ et $\tau \mapsto -1/\tau$, auquel cas c'est immédiat.

1.3. Analysons l'action du sous-groupe $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ sur \mathbb{H} . Deux éléments importants de ce groupe sont

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

i.e. $S\tau = -1/\tau$ et $T\tau = \tau + 1$. On a $S^2 = -I_2$ et $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, ainsi donc que l'identité $(ST)^3 = -I_2$. On a $Si = i$ et $ST\rho = -1/(\rho + 1) = \rho$ où $\rho = e^{2i\pi/3}$. On pose $\mathcal{F} = \{\tau \in \mathbb{H}, |\mathrm{Re}\tau| \leq \frac{1}{2} \text{ et } |\tau| \geq 1\}$.

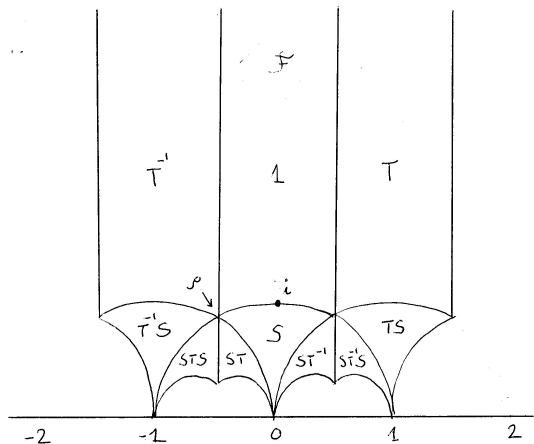


FIGURE 1. Le pavage de \mathbb{H} par la Γ -orbite de \mathcal{F}

Théorème 1.4. (i) Pour tout $\tau \in \mathbb{H}$, l'orbite $\Gamma\tau$ rencontre \mathcal{F} .

(ii) Si τ et τ' sont deux points distincts de \mathcal{F} tels que $\Gamma\tau = \Gamma\tau'$ alors :

- soit $\mathrm{Re}\tau = \pm\frac{1}{2}$ et $\tau' = \tau \pm 1$,
- soit $|\tau| = 1$ et $\tau' = -1/\tau$.

(iii) Si $\tau \in \mathcal{F}$ alors le stabilisateur de τ dans Γ est $\{\pm 1\}$, sauf si $\tau = i$ (resp. $\tau = \rho, -\rho^2$), auquel cas c'est le sous-groupe engendré par S (resp. ST).

DÉMONSTRATION — Soit $\tau \in \mathbb{H}$. La forme quadratique $\mathbb{R}^2 \rightarrow \mathbb{R}$, $(c, d) \mapsto |c\tau + d|^2$ est définie positive, elle admet donc un minimum sur $\mathbb{Z}^2 - \{0\}$. D'après la formule (2), il y a donc un sens à considérer l'ensemble $E \subset \Gamma\tau$ des éléments τ' tels que $\mathrm{Im}\tau'$ est maximal. Il est invariant par $\tau' \mapsto \tau' + 1$, de sorte qu'il existe $\tau' \in E$ tel que $|\mathrm{Re}\tau'| \leq \frac{1}{2}$. Mais $-1/\tau' \in \Gamma\tau$ et $\mathrm{Im}(-1/\tau') = \frac{\mathrm{Im}\tau'}{|\tau'|^2}$, donc $|\tau'| \geq 1$. Ainsi, $\tau' \in \Gamma\tau \cap \mathcal{F}$. Observons que cette démonstration montre en fait $G\tau \cap \mathcal{F} \neq \emptyset$ où G désigne le sous-groupe de Γ engendré par S et T .

Pour montrer (ii) et (iii), considérons $\tau, \tau' \in \mathcal{F}$ (non nécessairement distincts) tels que $\mathrm{Im}\tau' \geq \mathrm{Im}\tau$ et tels que $\tau' = \gamma\tau$ où

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

On a alors $|c\tau + d| \leq 1$. En particulier, $|c\mathrm{Im}\tau| \leq 1$ et donc $|c| \leq 1$. Si $c = 0$ alors $d = a = \pm 1$ et donc $\pm\gamma$ est une puissance de T et on est dans le premier cas du (ii). Sinon on peut supposer $c = 1$, quitte à remplacer γ par $-\gamma$. On voit sur le dessin que $|\tau + d| \leq 1$ entraîne $|\tau| = 1$, et que l'on est dans l'un des cas suivants :

1. $\tau \neq \rho, -\rho^2$ et $d = 0$. Dans ce cas, $b = -1$ et $\tau' = a - 1/\tau$ puis $a = 0$ car $|\mathrm{Re}(-1/\tau)| < 1/2$. Ainsi, $\gamma = S$ et $\tau' = \tau = i$.

2. $\tau = \rho$ et $d = 0, -1$. Si $d = 0$ on a encore $b = -1$ et $\tau' = a - 1/\rho = a - \rho^2$. Cela montre que soit $\tau' = -\rho^2$, $a = 0$ et $\gamma = \pm S$, soit $\tau' = \tau$, $a = -1$ et $\gamma = (ST)^2$.

3. Le cas $\tau = -\rho^2$ et $d = 0, 1$ se traite de manière similaire au cas 2. □

Soit E l'ensemble des $\tau \in \mathcal{F}$ tels que l'on ait soit $\operatorname{Re} \tau = \frac{1}{2}$, soit $|\tau| = 1$ et $\operatorname{Re} \tau > 0$. Soit $\mathcal{F}' = \mathcal{F} - E$. Les points (i) et (ii) du théorème ci-dessus montrent que pour tout $\tau \in \mathcal{H}$, l'orbite $\Gamma\tau$ rencontre \mathcal{F}' en un et un seul point. On dit aussi que \mathcal{F}' est *un domaine fondamental* de l'action de Γ sur \mathbb{H} .

Corollaire 1.5. Γ est engendré par S et T .

DÉMONSTRATION — Il ne serait pas difficile de démontrer ce corollaire de manière directe en utilisant des opérations sur les lignes et les colonnes. Dédouons-le plutôt du théorème. Soit G le sous-groupe de Γ engendré par S et T . Soit τ un point de l'intérieur de \mathcal{F} . Soit $\gamma \in \Gamma$. D'après la démonstration du (i) ci-dessus (dernière remarque), il existe $g \in G$ tel que $g^{-1}\gamma\tau \in \mathcal{F}$. Ainsi, $g^{-1}\gamma \in \operatorname{SL}_2(\mathbb{Z})$ fixe τ , c'est donc $\pm I_2$ d'après le (iii). Au final, on a $\gamma \in G$ car $-I_2 = S^2 \in G$. \square

2. FORMES MODULAIRES POUR $\operatorname{SL}_2(\mathbb{Z})$

L'application $(f, \gamma) \mapsto (\tau \mapsto f(\gamma\tau))$ définit une action à droite du groupe $\operatorname{SL}_2(\mathbb{R})$ sur le \mathbb{C} -espace vectoriel des fonctions $\mathbb{H} \rightarrow \mathbb{C}$, c'est même une représentation linéaire. Plus généralement, si $k \in \mathbb{Z}$, $f : \mathbb{H} \rightarrow \mathbb{C}$ et $\gamma \in \operatorname{SL}_2(\mathbb{R})$, on définit une fonction $f|_k \gamma : \mathbb{H} \rightarrow \mathbb{C}$ en posant

$$f|_k \gamma (\tau) = j(\gamma, \tau)^{-k} f(\gamma\tau).$$

Cela a un sens car $j(\gamma, \tau) \neq 0$ pour tout $\gamma \in \operatorname{SL}_2(\mathbb{R})$ et tout $\tau \in \mathbb{H}$. On vérifie immédiatement que la relation de cocycle satisfaite par j équivaut à dire que $(f, \gamma) \mapsto f|_k \gamma$ est une action à droite de $\operatorname{SL}_2(\mathbb{R})$ sur l'espace des fonctions $\mathbb{H} \rightarrow \mathbb{C}$, appelée *action de poids k* . L'action précédente en est alors le cas particulier $k = 0$.

Proposition-Définition 2.1. Une fonction $f : \mathbb{H} \rightarrow \mathbb{C}$ est dite faiblement modulaire de poids $k \in \mathbb{Z}$ si

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad \forall \tau \in \mathbb{H}, \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_2(\mathbb{Z})$$

ou ce qui revient au même si $f(\tau + 1) = f(\tau)$ et $f(-1/\tau) = \tau^k f(\tau)$ pour tout $\tau \in \mathbb{H}$.

DÉMONSTRATION — Par définition, f est faiblement modulaire si f est fixée par Γ pour l'action de poids k . Comme Γ est engendré par S et T (corollaire 1.5), il est équivalent de demander que f est fixée par S et T . \square

Notons $\mathcal{O}(\mathbb{H})$ l'espace vectoriel des fonctions holomorphes $\mathbb{H} \rightarrow \mathbb{C}$. Les homographies de \mathbb{H} étant des transformations biholomorphes, l'action de poids k de $\operatorname{SL}_2(\mathbb{R})$ préserve le sous-espace $\mathcal{O}(\mathbb{H})$.

Définition 2.2. Une forme modulaire de poids $k \in \mathbb{Z}$ est une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbb{C}$ telle que :

- (i) f est faiblement modulaire de poids k ,
- (ii) $f(\tau)$ admet une limite finie quand $\operatorname{Im} \tau \rightarrow +\infty$; on la note $f(\infty)$.

L'ensemble des formes modulaires de poids k est un sous-espace de $\mathcal{O}(\mathbb{H})$. Suivant Serre, nous le noterons M_k . Les relations $S^2 = -I_2$ et $f|_k - I_2 = (-1)^k f$ montrent que si $f \in M_k$ alors $f = (-1)^k f$, de sorte que $M_k = 0$ si k est impair. Les fonctions constantes sont modulaires de poids 0 : nous verrons plus loin que ce sont les seules. Un premier exemple intéressant de forme modulaire est donné par les *séries d'Eisenstein*.

Proposition 2.3. Soit $k \geq 4$ un entier pair. La série $\sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{(m\tau + n)^k}$ est absolument convergente sur \mathbb{H} ; on note $G_k(\tau)$ sa somme. Alors $G_k \in M_k$ et $G_k(\infty) = 2\zeta(k)$. En particulier $G_k \neq 0$.

DÉMONSTRATION — Fixons $A, B \in \mathbb{R}_{>0}$ et notons $\mathcal{D}_{A,B}$ l'ensemble des $\tau \in \mathbb{H}$ tels que $\operatorname{Im} \tau > A$ et $|\operatorname{Re} \tau| < B$. Vérifions qu'il existe un réel $C > 0$ tel que pour tout $(\mu, \nu) \in \mathbb{R}^2 - \{0\}$ et tout $\tau \in \mathcal{D}_{A,B}$ alors

$$|\mu\tau + \nu| > C \sup(|\mu|, |\nu|).$$

Soit $\tau \in \mathcal{D}_{A,B}$. D'une part, on a $|\tau - \lambda| > A$ pour tout $\lambda \in \mathbb{R}$. D'autre part, le cône $\{\lambda x, x \in \mathcal{D}_{A,B}, \lambda \in \mathbb{R}\}$ a pour frontière les droites vectorielles engendrées respectivement par $B + iA$ et $-B + iA$. En particulier, il existe $\delta > 0$ tel que $|\lambda\tau + 1| > \delta$ pour tout $\lambda \in \mathbb{R}$. Ainsi, $C = \text{Min}(A, \delta)$ convient.

Si $s \geq 1$, il y a exactement $8s$ couples $(m, n) \in \mathbb{Z}^2$ tels que $\sup(|m|, |n|) = s$. On en déduit la majoration

$$\sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{|m\tau + n|^k} < \frac{1}{C^k} \sum_{s \geq 1} \frac{8s}{s^k}$$

pour tout $\tau \in \mathcal{D}_{A,B}$. Ainsi, la série de l'énoncé est normalement convergente sur $\mathcal{D}_{A,B}$. En particulier, $G_k(\tau)$ est une fonction holomorphe de τ . Par convergence absolue de $G_k(\tau)$, les bijections $(m, n) \mapsto (m, n + m)$ et $(m, n) \mapsto (n, -m)$ de $\mathbb{Z}^2 - \{0\}$ entraînent les identités $G_k(\tau + 1) = G_k(\tau)$ et $G_k(-1/\tau) = \tau^k G_k(\tau)$ pour tout $\tau \in \mathbb{H}$.

Enfin, faisons tendre $\text{Im } \tau$ vers l'infini quand $\tau \in \mathcal{D}_{1,1}$. La fonction $\tau \mapsto \frac{1}{(m\tau + n)^k}$ tend vers $\frac{1}{n^k}$ ou 0 selon que $m = 0$ ou non. Par convergence uniforme de G_k sur $\mathcal{D}_{1,1}$, on peut intervertir limite et sommation et l'on obtient que $G_k(\tau) \rightarrow 2\zeta(k)$. On conclut par 1-périodicité de G_k . \square

Si $k \geq 4$ est pair, on pose $E_k = \frac{1}{2\zeta(k)} G_k \in M_k$ (série d'Eisenstein "normalisée"), de sorte que l'on ait $E_k(\infty) = 1$. Bien entendu, cette définition a un sens puisque $\zeta(k) \neq 0$. L'application $M_k \rightarrow \mathbb{C}$, $f \mapsto f(\infty)$, est une application linéaire. Son noyau, noté S_k , est le sous-espace des formes modulaires *paraboliques* ("cuspidal" en anglais). Si $k \geq 4$, il est donc engendré par les éléments de la forme $f - f(\infty)E_k$.

Corollaire 2.4. *Pour tout entier pair $k \geq 4$, on a $M_k = S_k \oplus \mathbb{C}E_k$.*

Observons que si $f \in M_k$ et $g \in M_{k'}$ alors $fg \in M_{k+k'}$. On peut donc fabriquer tout un tas de formes modulaires à l'aide des séries d'Eisenstein. Par exemple, si r et s sont des entiers ≥ 0 alors $E_4^r E_6^s \in M_{4r+6s}$.

Théorème 2.5. *Soit $k \in \mathbb{Z}$. L'espace M_k admet pour base les $E_4^r E_6^s$, avec $(r, s) \in \mathbb{N}^2$ vérifiant $4r + 6s = k$.*

Observons d'abord que si $f \in M_k$ alors $f(i) = f|_k S(i) = i^{-k} f(i)$. Ainsi, $f(i) = 0$ si $k \not\equiv 0 \pmod{4}$. De même $f(\rho) = 0$ si $k \not\equiv 0 \pmod{3}$. En particulier, $E_6(i) = 0$ et $E_4(\rho) = 0$. Nous démontrerons $E_4(i) \neq 0$ dans la section suivante (pouvez-vous le démontrer directement?) et que la famille de l'énoncé est génératrice : admettons-le pour l'instant. Vérifions ici qu'elle est libre. On procède par récurrence sur $k \geq 0$, le cas $k = 0$ étant trivial. Supposons donc pour $k \geq 0$ donné que l'on ait une relation de dépendance linéaire

$$\sum_{4r+6s=k} \lambda_{r,s} E_4^r E_6^s = 0.$$

Si k est multiple de 4, l'évaluation en $\tau = i$ de cette formule donne $\lambda_{k/4,0} = 0$ (car on a $E_4(i) \neq 0$). Dans tous les cas, on a donc " $\lambda_{r,s} \neq 0$ implique $s \neq 0$ ". Ainsi, soit tous les $\lambda_{r,s}$ sont nuls, soit on a $k \geq 6$ et on peut simplifier l'égalité ci-dessus par E_6 (l'anneau des fonctions holomorphes sur \mathbb{H} étant intègre...), puis conclure par récurrence sur k . \square

Définition 2.6. (*Fonction Δ de Jacobi*) La fonction $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ est une forme modulaire parabolique de poids 12.

L'apparition du facteur 1728 sera expliquée plus loin. D'après ce que nous avons dit ci-dessus, $\Delta \neq 0$ car $\Delta(i) = \frac{1}{1728} E_4(i)^3$.

3. SUR LES ZÉROS DES FORMES MODULAIRES

3.1. q -développement d'une forme modulaire. Observons que si $z \in \mathbb{C}$ alors $|e^{2i\pi z}| = e^{-2\pi \text{Im} z}$. Soit $D = \{z \in \mathbb{C}, |z| < 1\}$. On considère l'application

$$q : \mathbb{H} \longrightarrow D - \{0\}, \quad \tau \mapsto e^{2i\pi\tau}.$$

Cette application induit une bijection $\langle \mathbb{T} \rangle \backslash \mathbb{H} \xrightarrow{\sim} D - \{0\}$. Autrement dit, si $f : \mathbb{H} \rightarrow \mathbb{C}$ est telle que $f(\tau + 1) = f(\tau)$, il existe une unique fonction $\tilde{f} : D - \{0\} \rightarrow \mathbb{C}$ telle que $f(\tau) = \tilde{f}(q)$.

Soit $f : \mathbb{H} \rightarrow \mathbb{C}$ telle que $f(\tau + 1) = f(\tau)$. Observons que f est une fonction holomorphe si, et seulement si, \tilde{f} est une fonction holomorphe sur $D - \{0\}$. En effet, pour tout $\tau_0 \in \mathbb{H}$, l'application q induit une bijection bi-holomorphe entre le voisinage ouvert $\{\tau \in \mathbb{H}, |\operatorname{Re}(\tau - \tau_0)| < 1/2\}$ de τ_0 dans \mathbb{H} , et le voisinage ouvert $D - \mathbb{R}_{\leq 0} e^{2i\pi\tau_0}$ (un inverse s'obtient en considérant une branche du logarithme complexe). Si f est holomorphe il y a donc équivalence entre :

- $f(\tau)$ admet une limite quand $\operatorname{Im} \tau \rightarrow \infty$,
- $|f(\tau)|$ est bornée sur $\{\tau \in \mathbb{H}, \operatorname{Im} \tau > 1\}$,
- $|\widetilde{f(q)}|$ est bornée au voisinage de $q = 0$,
- \tilde{f} se prolonge en une fonction holomorphe sur tout D ,
- \tilde{f} admet un développement en série entière en 0 de rayon de convergence ≥ 1 .

(L'implication assertion 3 \Rightarrow assertion 4 est le lemme de prolongement de Riemann). Cela justifie à la proposition-définition suivante.

Proposition-Définition 3.2. *Soit $f \in M_k$. La forme f admet un unique développement*

$$f(\tau) = \sum_{n \geq 0} a_n(f) q^n,$$

avec $a_n(f) \in \mathbb{C}$ pour tout entier $n \geq 0$, normalement convergent sur toute partie de \mathbb{H} de la forme $\operatorname{Im} \tau > A$, $A \in \mathbb{R}_{>0}$. Ce développement est appelé développement de Fourier, ou q -développement, de la forme f , et les $a_n(f)$ sont ses coefficients de Fourier. On a $a_0(f) = f(\infty)$.

Comme nous le verrons, et de manière un peu surprenante, la suite des coefficients de Fourier de chaque forme modulaire est en général d'un intérêt arithmétique considérable.

3.3. Formule $k/12$. Soient $f \in M_k$ et $P \in \mathbb{H}$. On note $v_P(f)$ l'ordre d'annulation de f au point P et e_P le cardinal du stabilisateur de P dans $\operatorname{SL}_2(\mathbb{Z})/\{\pm I_2\}$. Ces deux quantités, des entiers ≥ 0 , ne dépendent que de la Γ -orbite de P (pour $v_P(f)$, cela vient de la non annulation des $j(\gamma, \tau)$ quand $\gamma \in \Gamma$ et $\tau \in \mathbb{H}$). De plus, d'après le théorème 1.4 (iii) on a $e_i = 2$, $e_\rho = 3$, et si P n'est pas dans l'orbite de i ou ρ alors $e_P = 1$. On note aussi $v_\infty(f)$ l'ordre d'annulation de f en 0.

Proposition 3.4. (Formule $k/12$) *Soient $k \in \mathbb{Z}$ et $f \in M_k$ non nulle. On a la relation*

$$v_\infty(f) + \sum_{P \in \Gamma \backslash \mathbb{H}} \frac{v_P(f)}{e_P} = \frac{k}{12}.$$

Il fait partie de l'énoncé que la somme de gauche est en fait une somme finie (nécessairement ≥ 0). Le lecteur préférant voir d'abord comment utiliser cette formule, et par exemple terminer la démonstration du théorème 2.5, peut commencer par lire la sous-section suivante.

DÉMONSTRATION — Soit $f \in M_k$ non nulle. Rappelons que la Γ -orbite de tout zéro de f rencontre le domaine \mathcal{F} . Si r est un réel > 0 posons $\Omega_r = \{\tau \in \mathbb{H}, \operatorname{Im} \tau > r\}$. La fonction \tilde{f} étant holomorphe en 0, il existe $r > 0$ tel que f n'admet pas de zéro dans Ω_r . La partie $\mathcal{F} - \Omega_r$ étant compacte, la fonction holomorphe f n'y admet qu'un nombre fini de zéros (qui sont isolés). Cela montre que le nombre des Γ -orbites de points constituées de zéros de f est fini (et donc que la somme apparaissant dans la formule $k/12$ a tous ses termes nuls sauf au plus un nombre fini d'entre eux).

Considérons le contour \mathcal{C} indiqué par la figure 2. Sur cette figure, les zéros éventuels de f qui sont dans $\partial\mathcal{F} - \{i, \rho, -\rho^2\}$ et de partie réelle 1/2 (resp. de module 1) sont notés λ (resp. μ). En particulier, ce contour ne contient aucun zéro de f . On suppose que chaque portion de cercle dessinée est de rayon suffisamment petit de sorte que le disque bordé ne contienne que le point indiqué pour éventuel zéro (i.e $i, \rho, -\rho^2$, l'un des $\lambda, \lambda + 1$, ou l'un des $\mu, -1/\mu$). Nous noterons γ_{XY} le chemin portion de \mathcal{C} allant de X à Y (dans ce sens). Le chemin $\gamma_{D'E}$ est par définition le chemin $\Gamma \gamma_{AB}^{\text{opp}}$. De même, on a choisi $\gamma_{C'D} = S \gamma_{B'C}^{\text{opp}}$. Enfin, on

suppose que γ_{EA} est de partie imaginaire r suffisamment grande de sorte qu'aucun zéro de f ne soit de partie imaginaire $> r$. L'existence d'un tel contour est justifiée par le paragraphe précédent (zéros isolés).

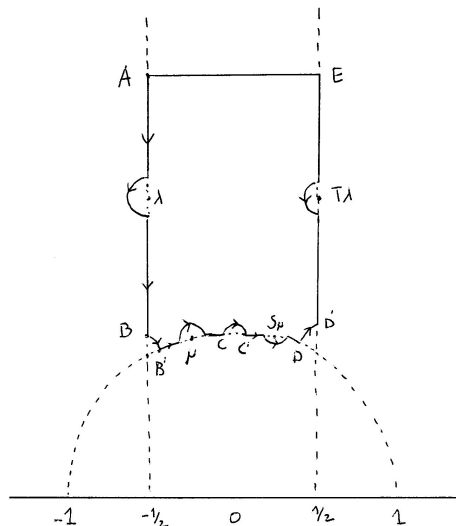


FIGURE 2. Le chemin d'intégration dans la démonstration de la formule $k/12$

La formule des résidus appliquée à la 1-forme méromorphe $\frac{df}{f} = \frac{f'(\tau)}{f(\tau)} d\tau$ s'écrit donc

$$\frac{1}{2i\pi} \int_C \frac{f'(\tau)}{f(\tau)} d\tau = \sum_P v_P(f)$$

la somme portant sur les Γ -orbites de zéros de f ne contenant ni i ni ρ . Examinons maintenant les contributions des diverses portions du contour. Les fonctions f et f' étant T -invariantes on observe d'abord

$$\int_{\gamma_{AB}} \frac{f'(\tau)}{f(\tau)} d\tau = \int_{T\gamma_{AB}} \frac{f'(\tau)}{f(\tau)} d\tau = - \int_{\gamma_{D'E}} \frac{f'(\tau)}{f(\tau)} d\tau.$$

Le chemin $\omega(t) := e^{2i\pi\gamma_{EA}(t)}$ est un cercle de centre 0 dans D faisant un tour dans le sens indirect. On a alors

$$\frac{1}{2i\pi} \int_{\gamma_{EA}} \frac{f'(\tau)}{f(\tau)} d\tau = \frac{1}{2i\pi} \int_{\omega} \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq = -v_{\infty}(f).$$

En effet, la première égalité est un simple changement de variables, et la seconde est le théorème des résidus appliqué à \tilde{f} , sachant que par hypothèse 0 est le seul zéro éventuel de \tilde{f} dans le disque de D bordé par ω . De plus, par modularité de f on a $\frac{f'}{f} = -\frac{k}{\tau} + \frac{(f \circ S)'}{f \circ S}$, de sorte que

$$\frac{1}{2i\pi} \int_{\gamma_{B'C}} \frac{f'(\tau)}{f(\tau)} d\tau = -\frac{1}{2i\pi} \int_{\gamma_{B'C}} \frac{k}{\tau} d\tau + \int_{S\gamma_{B'C}} \frac{f'(\tau)}{f(\tau)} d\tau,$$

avec rappelons-le $S\gamma_{B'C} = \gamma_{C'D}^{\text{opp}}$. Lorsque le point B' tend vers ρ , C tend vers i , et lorsque les portions de cercles autour des points notés μ sont de rayon tendant vers 0, alors l'intégrale de chemin $\frac{1}{i} \int_{\gamma_{B'C}} \frac{d\tau}{\tau}$ tend vers l'angle orienté défini par ρ , 0 et i , i.e. $-(\frac{2\pi}{3} - \frac{2\pi}{4}) = -\frac{\pi}{6}$. De même, lorsque B et B' tendent vers ρ alors l'intégrale de chemin $\frac{1}{i} \int_{\gamma_{BB'}} \frac{f'(\tau)}{f(\tau)} d\tau$ tend vers l'angle orienté $\widehat{B\rho B'}$ = $-\frac{\pi}{3}$ multiplié par $v_{\rho}(f)$. Enfin, lorsque C et C' tendent vers i alors l'intégrale de chemin $\frac{1}{i} \int_{\gamma_{CC'}} \frac{f'(\tau)}{f(\tau)} d\tau$ tend vers $-\pi v_i(f)$. On conclut en mettant toutes ces identités bout à bout. \square

3.5. Conséquences de la formule $k/12$. La première conséquence évidente de la formule $k/12$ est l'annulation $M_k = 0$ si $k < 0$. De plus, on a $S_k = 0$ si $k < 12$, car $v_\infty(f) \geq 1$ si $f \in S_k - \{0\}$. En particulier, on a donc $M_0 = \mathbb{C} 1$ (les constantes). Séparant les orbites de i et ρ des autres, la formule $k/12$ s'écrit aussi

$$(3) \quad v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_P v_P(f) = \frac{k}{12},$$

la somme portant sur les Γ -orbites de points de \mathbb{H} distinctes de Γi et $\Gamma \rho$. En particulier on a $M_2 = 0$ car chaque terme de gauche est soit $> 1/6$, soit nul. On a donc montré le :

Corollaire 3.6. (i) Si $k < 0$ ou $k = 2$ alors $M_k = 0$.

(ii) $M_0 = \mathbb{C} 1$ et si $k = 4, 6, 8, 10$ alors $M_k = \mathbb{C} E_k$.

Appliquons la formule (3) à $k = 4$ et $f = E_4$. Dans ce cas on a $\frac{k}{12} = \frac{1}{3}$, mais l'annulation évidente $E_4(\rho) = 0$ entraîne $\frac{1}{3}v_\rho(f) \geq 1/3$. Ainsi, la seule Γ -orbite de points qui sont des zéros de E_4 est celle de ρ . En particulier, cela démontre la non-nullité annoncée

$$E_4(i) \neq 0,$$

puis $\Delta \neq 0$ car on a $\Delta(i) = \frac{1}{1728}E_4(i)^3$. Appliquant maintenant (3) à $k = 12$ et $f = \Delta$, on en déduit que Δ ne s'annule pas sur \mathbb{H} et que l'inégalité $v_\infty(\Delta) \geq 1$ est une égalité. En particulier, si k est quelconque et si $f \in S_k$ alors la fonction $\frac{f}{\Delta}$ est une forme modulaire de poids $k - 12$. On a démontré le corollaire suivant.

Corollaire 3.7. (i) La fonction Δ ne s'annule pas sur \mathbb{H} et l'on a $v_\infty(\Delta) = 1$.

(ii) Si $k \in \mathbb{Z}$ alors $S_k = \Delta M_{k-12}$. En particulier, $S_{12} = \mathbb{C} \Delta$ est de dimension 1.

Démontrons enfin que M_k est engendré par les $E_4^r E_6^s$, où r, s sont des entiers ≥ 0 tels que $4r + 6s = k$. D'après le corollaire 3.6, on peut supposer $k \geq 4$. On procède par récurrence sur k . Observons que k étant pair ≥ 4 , il existe des entiers positifs r, s tels que $k = 4r + 6s$: on a soit $k \equiv 0 \pmod{4}$, soit $k \equiv 6 \pmod{4}$ et $k \geq 6$. Un tel couple (r, s) étant fixé, observons que pour tout $f \in M_k$ alors $f - f(\infty)E_4^r E_6^s \in S_k$. Mais $S_k = \Delta M_{k-12}$ d'après le corollaire 3.7, et $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$. Cela termine la démonstration, ainsi donc que celle du théorème 2.5. \square

Les corollaires 3.6 et 3.7 entraînent également immédiatement le corollaire suivant :

Corollaire 3.8. Supposons $k \geq 0$ pair. La dimension de S_k vaut $[k/12]$ si $k \not\equiv 2 \pmod{12}$, $[k/12] - 1$ sinon.

4. QUELQUES q-DÉVELOPPEMENTS

4.1. Séries d'Eisenstein. Si $k \in \mathbb{Z}$ et $n \geq 1$ est un entier, on pose $\sigma_k(n) = \sum_{d|n} d^k$. On rappelle que les nombres de Bernoulli sont définis par la série formelle $\frac{t}{e^t - 1} = \sum_{n \geq 0} \frac{B_n}{n!} t^n$. L'identité suivante est essentiellement due à Euler.

Proposition 4.2. Soit k un entier pair ≥ 4 . On a $E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 0} \sigma_{k-1}(n) q^n$.

DÉMONSTRATION — Rappelons qu'Euler a démontré que pour tout $z \in \mathbb{C} - \mathbb{Z}$, on a

$$(4) \quad \frac{\pi}{\tan \pi z} = \frac{1}{z} + \sum_{n \in \mathbb{Z} - \{0\}} \left(\frac{1}{z - n} + \frac{1}{n} \right)$$

Justifions brièvement cette identité. Notons $g(z)$ la série de fonctions de droite et posons $f(z) = \frac{\pi}{\tan \pi z}$. Si $|z| \leq r$ et $|n| > r$ alors l'inégalité

$$\left| \frac{1}{z - n} + \frac{1}{n} \right| = \frac{|z|}{|n||z - n|} \leq \frac{r}{|n|(|n| - r)}$$

montre que la série de fonctions méromorphes $g(z)$ converge normalement sur tout compact de \mathbb{C} . C'est donc une fonction méromorphe sur \mathbb{C} , holomorphe sur $\mathbb{C} - \mathbb{Z}$, dont les pôles en les entiers sont simples de résidu 1. La fonction f a les mêmes propriétés que g , de sorte que $f - g$ est holomorphe sur \mathbb{C} . Mais f et

g , et donc $f - g$, sont 1-périodiques et impaires (c'est un exercice pour g). Pour en déduire que $f - g$ est nulle il suffit d'après Liouville de montrer que f et g restent bornées quand $\text{Im}\tau \rightarrow \infty$. C'est clair pour f . Pour g , on observe que $qg(\tau) \rightarrow 0$ quand $\text{Im}(\tau) \rightarrow +\infty$, d'où l'on tire que \tilde{g} est holomorphe en 0 (lemme de prolongement de Riemann), ce qui conclut.

Si $\tau \in \mathbb{H}$ on a le développement évident $\frac{\pi}{\tan \pi\tau} = i\pi \frac{q+1}{q-1} = i\pi - 2i\pi \sum_{n \geq 0} q^n$. Soit $k \geq 2$. En dérivant $k - 1$ fois par rapport à τ la formule d'Euler, on trouve l'identité

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

Supposons k pair ≥ 4 . On applique cette identité à $m\tau$ pour tout m entier ≥ 1 , ce qui a pour effet de remplacer q par q^m , et on fait la somme (la convergence absolue du terme de droite ayant déjà été vérifiée). On en déduit, pour $k \geq 4$ pair :

$$\frac{1}{2} G_k(\tau) - \zeta(k) = \frac{(2i\pi)^k}{(k-1)!} \sum_{n \geq 0} \sigma_{k-1}(n) q^n.$$

Pour conclure, on utilise une identité fameuse due à Euler :

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

En fait, cette formule est aussi conséquence de l'identité (4). En effet, cette dernière dérivée $k - 1$ fois s'écrit

$$\left(\frac{2i\pi}{e^{2i\pi z} - 1} - \frac{1}{z}\right)^{(k-1)} = (-1)^{k-1} (k-1)! \sum_{n \neq 0} \frac{1}{(z+n)^k}.$$

Par définition des nombres de Bernoulli on a $\frac{2i\pi}{e^{2i\pi z} - 1} - \frac{1}{z} = \sum_{n \geq 1} (2i\pi)^n \frac{B_n}{n!} z^{n-1}$ au voisinage de $z = 0$. On conclut par évaluation en $z = 0$. \square

Observons que le q -développement de E_k est à coefficients dans \mathbb{Q} . Mieux, E_4 et E_6 sont à coefficients entiers, comme le montre le tableau suivant. Ainsi, le théorème 2.5 entraîne que S_k possède une \mathbb{C} -base constituée de formes modulaires à coefficients entiers, un phénomène inattendu.

k	2	4	6	8	10	12	14	16
$-\frac{2k}{B_k}$	-24	240	-504	480	-264	65520/691	-24	16320/3617

4.3. La magie des formes modulaires. En guise d'exemple, considérons E_4^2 . C'est un élément de $M_8 = \mathbb{C} E_8$ (Corollaire 3.6). Comme $E_4^2(\infty) = E_8(\infty) = 1$, on a nécessairement

$$E_4^2 = E_8.$$

Cette identité est tout à fait non triviale ! En effet, une fois les coefficients de Fourier égalisés elle s'écrit

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m), \quad \forall n \geq 1.$$

Par exemple, $1 + 2^7 = 129 = 1 + 2^3 + 120$. Cette méthode de raisonnement est de portée très générale, et nous en verrons d'autres applications spectaculaires dans la suite.

4.4. La fonction Δ . La formule $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$, combinée aux q -développements de E_4 et E_6 , permet d'exprimer les coefficients de Fourier de Δ . On trouve (en notant $1728 = 3 \cdot 240 + 2 \cdot 504$)

$$\Delta = q - 24q^2 + 252q^3 + \dots$$

Théorème 4.5. (Jacobi) $\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$.

Pour une démonstration, voir le livre de Serre référencé. Les coefficients de Fourier $a_n(\Delta)$ de Δ sont notés $\tau(n)$: c'est la fonction τ de Ramanujan. Elle possède une riche histoire, sur laquelle nous reviendrons dans les exposés.

5. LA FONCTION ϑ DE JACOBI

5.1. L'identité de Poisson. Considérons la fonction d'une variable réelle $t > 0$ définie par la somme

$$\theta(t) = \sum_{n \in \mathbb{Z}} e^{-t\pi n^2}.$$

Cette série (à termes positifs) est bien évidemment convergente, et fonction décroissante de $t > 0$. Elle satisfait l'équation fonctionnelle curieuse suivante, due à Poisson, que nous allons d'abord démontrer.

Proposition 5.2. *Pour tout réel $t > 0$ on a $\theta(1/t) = \sqrt{t} \theta(t)$.*

On rappelle que l'espace de Schwartz $\mathcal{S}(\mathbb{R})$ est l'espace des fonctions $f : \mathbb{R} \rightarrow \mathbb{C}$ de classe \mathcal{C}^∞ telles que pour tous entiers $n, m \geq 1$, on ait $x^n f^{(m)}(x) \rightarrow 0$ quand $|x| \rightarrow \infty$. Si $f \in \mathcal{S}(\mathbb{R})$, f est en particulier sommable de sorte que sa transformée de Fourier $\hat{f} : \mathbb{R} \rightarrow \mathbb{C}$, $y \mapsto \int_{\mathbb{R}} f(x) e^{-2i\pi xy} dx$, est bien définie.

Lemme 5.3. (Formule de Poisson) *Pour tout $f \in \mathcal{S}(\mathbb{R})$ on a l'égalité de séries absolument convergentes*

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

DÉMONSTRATION — Soit $\psi(x) = \sum_{m \in \mathbb{Z}} f(x + m)$. Cette série de fonctions converge normalement sur tout segment, ainsi que toutes ses dérivées, par hypothèse sur f . Elle définit donc une fonction \mathcal{C}^∞ et 1-périodique de la variable réelle x . Ses coefficients de Fourier sont donnés par la formule

$$c_n = \int_0^1 \psi(x) e^{-2i\pi nx} dx = \sum_{m \in \mathbb{Z}} \int_m^{m+1} f(x) e^{-2i\pi nx} dx = \hat{f}(n).$$

L'intervertion somme/intégrale est bien sûr loisible car f est sommable sur \mathbb{R} . La fonction ψ étant \mathcal{C}^∞ , sa série de Fourier $\sum_{n \in \mathbb{Z}} \hat{f}(n) e^{2i\pi nx}$ est absolument convergente vers $\psi(x)$ pour tout $x \in \mathbb{R}$. On conclut en prenant $x = 0$, et montre au passage que les deux sommes de l'énoncé sont absolument convergentes. \square

Lemme 5.4. *Si $t \in \mathbb{R}_{>0}$, la fonction $x \mapsto f_t(x) = e^{-\pi t x^2}$ est dans $\mathcal{S}(\mathbb{R})$, et vérifie*

$$\hat{f}_t(y) = \frac{1}{\sqrt{t}} f_{1/t}(y) \quad \forall y \in \mathbb{R}.$$

DÉMONSTRATION — L'assertion $f_t \in \mathcal{S}(\mathbb{R})$ est facile, et laissée au lecteur. Un simple changement de variables montre $\hat{f}_t(y) = \frac{1}{\sqrt{t}} \hat{f}_1(y/\sqrt{t})$. Il suffit donc de démontrer $\hat{f}_1 = f_1$, i.e. que $x \mapsto e^{-\pi x^2}$ est égale à sa transformée de Fourier. C'est un fait bien connu dû à Gauss. Donnons un argument. On constate que

$$\frac{\partial}{\partial y} \hat{f}_1(y) = i \int_{\mathbb{R}} (e^{-\pi x^2})' e^{-2i\pi xy} dx = -2\pi y \hat{f}_1(y)$$

d'où l'on tire $\hat{f}_1(y) = e^{-\pi y^2} \mathbf{I}$, avec $\mathbf{I} = \hat{f}_1(0) = \int_{\mathbb{R}} e^{-\pi x^2} dx$. Mais Gauss a démontré $\mathbf{I} = 1$: par exemple par passage aux coordonnées polaires on a l'identité $\mathbf{I}^2 = \int_0^{2\pi} d\theta \int_0^\infty e^{-\pi r^2} r dr = 1$, et $\mathbf{I} > 0$. \square

Pour conclure la démonstration de la proposition 5.2, il suffit d'appliquer la formule de Poisson à la fonction f_t . Mentionnons que cette identité de Poisson est l'ingrédient clé dans la démonstration par Riemann de l'équation fonctionnelle de la fonction $\zeta(s)$.

5.5. La fonction Θ de Jacobi. Jacobi a introduit une variante à deux variables de la fonction θ : si $z \in \mathbb{C}$ et $\tau \in \mathbb{H}$, il pose

$$\Theta(z; \tau) = \sum_{n \in \mathbb{Z}} e^{i\pi\tau n^2 + 2i\pi n z}.$$

Cette série est manifestement normalement convergente sur toute partie de $\mathbb{C} \times \mathbb{H}$ de la forme $\{(z, \tau), \operatorname{Im} z > A, \operatorname{Im} \tau > B\}$, où $A \in \mathbb{R}$ et $B \in \mathbb{R}_{>0}$. Cela justifie la définition, et montre que la fonction $(z, \tau) \mapsto \Theta(z; \tau)$ est holomorphe en chacune de ses variables, l'autre étant fixée (et même en les deux variables si l'on sait ce que cela signifie). On observe que si $t > 0$ alors $\Theta(0, it) = \theta(t)$: on retrouve la fonction précédente sur l'axe imaginaire, quand $z = 0$. Des manipulations évidentes montrent que la fonction $\Theta(z; \tau)$ satisfait les équations fonctionnelles suivantes :

$$\Theta(z + 1; \tau) = \Theta(z; \tau) \quad \text{et} \quad \Theta(z + \tau; \tau) = e^{-i\pi\tau - 2i\pi z} \Theta(z; \tau).$$

Ainsi, à τ fixé, ces formules expriment le comportement de la fonction $z \mapsto \Theta(z; \tau)$ par rapport au réseau $\mathbb{Z} + \tau\mathbb{Z}$ de \mathbb{C} ; leur application originale est d'ailleurs à la construction de fonctions méromorphes sur \mathbb{C} invariantes par un tel réseau. Leur dépendance en la variable τ , que l'on peut voir comme paramétrant le réseau $\mathbb{Z} + \tau\mathbb{Z}$, est encore plus remarquable :

Théorème 5.6. *Pour tout $z \in \mathbb{C}$ et tout $\tau \in \mathbb{H}$, on a les relations*

$$\Theta(z; \tau + 2) = \Theta(z; \tau) \quad \text{et} \quad \Theta(z; -1/\tau) = \sqrt{-i\tau} e^{i\pi\tau z^2} \Theta(\tau z; \tau).$$

Dans cette formule la notation $\sqrt{-i\tau}$ désigne la racine carrée de $-i\tau$ dont la partie réelle est > 0 .

DÉMONSTRATION — L'identité $\Theta(z; \tau + 2) = \Theta(z; \tau)$ est immédiate. Pour la seconde, on applique la formule de Poisson à la fonction du lemme suivant, dans lequel le complexe $\sqrt{-i\tau}$ pour $\tau \in \mathbb{H}$ est à prendre au même sens que dans l'énoncé du théorème. On obtient $\Theta(z; \tau) = (-i\tau)^{-1/2} e^{-i\pi z^2/\tau} \Theta(z/\tau; -1/\tau)$. On conclut en remplaçant z par τz . \square

Lemme 5.7. *Si $z \in \mathbb{C}$ et $\tau \in \mathbb{H}$, la fonction $x \mapsto e^{i\pi\tau x^2 + 2i\pi x z}$ est dans $\mathcal{S}(\mathbb{R})$, et de transformée de Fourier*

$$y \mapsto \frac{1}{\sqrt{-i\tau}} e^{-\frac{i\pi}{\tau}(x-z)^2}.$$

DÉMONSTRATION — Posons $g_\tau(x) = e^{i\pi\tau x^2}$. La transformée de Fourier de $x \mapsto g_\tau(x) e^{2i\pi x z}$ étant $y \mapsto \widehat{g}_\tau(y - z)$, on peut supposer $z = 0$. Fixons $y \in \mathbb{R}$. On veut démontrer l'égalité

$$\widehat{g}_\tau(y) = \frac{1}{\sqrt{-i\tau}} g_{-1/\tau}(y).$$

Lorsque $\tau = it$ avec t réel > 0 , c'est exactement le lemme 5.4. D'après le principe des zéros isolés, il suffit donc de vérifier que les deux termes de cette égalité sont des fonctions holomorphes de la variable τ dans \mathbb{H} . C'est clair pour $\tau \mapsto g_{-1/\tau}(y)$ et $\tau \mapsto \sqrt{-i\tau}$ (cette dernière est une racine carrée continue de la fonction $\tau \mapsto -i\tau$ qui ne s'annule pas sur \mathbb{H}). En ce qui concerne l'intégrale à paramètre $\tau \mapsto g_\tau(y)$, cela se déduit de l'holomorphie de $\tau \mapsto g_\tau(x)$ pour tout $x \in \mathbb{R}$ et de l'inégalité $|e^{i\pi\tau x^2}| \leq e^{-\pi \operatorname{Im} \tau x^2}$. \square

5.8. La fonction ϑ . Notons $J \subset \operatorname{SL}_2(\mathbb{Z})$ le sous-groupe engendré par les éléments T^2 et S . Certains auteurs, comme Busam & Freitag, appellent J le “ ϑ -groupe”. Notons $\vartheta : \mathbb{H} \rightarrow \mathbb{C}$ la fonction

$$\vartheta(\tau) = \Theta(0; \tau) = \sum_{n \in \mathbb{Z}} e^{i\pi\tau n^2}.$$

Elle est non identiquement nulle car $\vartheta(it) = \theta(t) > 0$ si t est un réel > 0 .

Corollaire 5.9. *Il existe un unique morphisme de groupes $\chi : J \rightarrow \{\pm 1, \pm i\}$ tel que $\chi(S) = -i$ et $\chi(T^2) = 1$. De plus, pour tout $\gamma \in J$ on a la relation $\vartheta^2|_1 \gamma = \chi(\gamma) \vartheta^2$.*

DÉMONSTRATION — Le Théorème 5.6 entraîne $\vartheta^2|_1 S = -i\vartheta^2$ et aussi $\vartheta^2|_1 T^2 = \vartheta^2$. Autrement dit, la fonction ϑ^2 est vecteur propre pour l'action de poids 1 de S et T^2 , de valeurs propres respectives $-i$ et 1. Ces éléments engendrant J , on en déduit d'une part l'existence et l'unicité de χ comme dans l'énoncé, et d'autre part la seconde assertion. \square

Observons que l'existence même d'un morphisme $\chi : J \rightarrow \mathbb{C}^*$ tel que $\chi(S) = -i$ et $\chi(T^2) = 1$ n'était pas du tout évidente a priori ! Ainsi, la fonction ϑ^2 apparaît comme une forme modulaire *généralisée*, en un sens que nous précisons dans la partie suivante. Avant d'en arriver là, observons que l'on a manifestement $\vartheta(2\tau) = \sum_{n \in \mathbb{Z}} q^{n^2}$, de sorte que pour tout entier $k \geq 1$ on a la relation

$$\vartheta^k(2\tau) = \sum_{(n_1, \dots, n_k) \in \mathbb{Z}^k} q^{n_1^2 + \dots + n_k^2} = \sum_{n \geq 0} r_k(n) q^n$$

où $r_k(n)$ désigne le nombre de k -uples $(n_1, \dots, n_k) \in \mathbb{Z}^k$ tels que $n = \sum_{i=1}^k n_i^2$. Autrement dit, comme série en q , la fonction $\vartheta^k(2\tau)$ n'est rien d'autre que la série génératrice du nombre des façons d'écrire un entier $n \geq 0$ comme somme de k carrés d'entiers. C'est le point de départ du lien entre formes quadratiques entières et formes modulaires.

5.10. ... et ses compagnons $\tilde{\vartheta}$ et $\tilde{\tilde{\vartheta}}$. Jacobi a également introduit les fonctions $\mathbb{H} \rightarrow \mathbb{C}$:

$$\tilde{\vartheta}(\tau) = \sum_{n \in \mathbb{Z}} (-1)^n e^{i\pi\tau n^2} \quad \text{et} \quad \tilde{\tilde{\vartheta}}(\tau) = \sum_{n \in \mathbb{Z}} e^{i\pi\tau(n+1/2)^2} = e^{\frac{i\pi\tau}{4}} \sum_{n \in \mathbb{Z}} q^{\frac{n(n+1)}{2}}.$$

Par définition, on a donc $\tilde{\vartheta}(\tau) = \Theta(1/2; \tau)$ et $\tilde{\tilde{\vartheta}}(\tau) = e^{\frac{i\pi\tau}{4}} \Theta(\tau/2; \tau)$. Elles sont reliées à ϑ par les formules

$$\tilde{\vartheta}(\tau) = \vartheta(\tau + 1) \quad \text{et} \quad \tilde{\tilde{\vartheta}}(\tau) = \frac{1}{\sqrt{-i\tau}} \vartheta(1 - 1/\tau).$$

(Pour la première utiliser $n^2 \equiv n \pmod{2}$ et pour la seconde appliquer l'identité de Jacobi à $z = 1/2$.)

6. FORMES MODULAIRES POUR UN SOUS-GROUPE DE $SL_2(\mathbb{Z})$

Dans cette partie, Γ désigne un sous-groupe de $SL_2(\mathbb{Z})$. Un *caractère* de Γ est un morphisme de groupes $\Gamma \rightarrow \mathbb{C}^*$.

Définition 6.1. Soient $k \in \mathbb{Z}$ et χ un caractère de Γ . Une *forme modulaire de poids k et de caractère χ* pour le groupe Γ est une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbb{C}$ telle que :

- (i) $f|_k \gamma = \chi(\gamma) f$ pour tout $\gamma \in \Gamma$,
- (ii) pour tout $\gamma \in SL_2(\mathbb{Z})$, la fonction $(f|_k \gamma)(\tau)$ admet une limite finie quand $\text{Im } \tau \rightarrow \infty$.

Lorsque χ est le caractère trivial, on parle simplement de *forme modulaire de poids k pour le groupe Γ* .

On note $M_k(\Gamma, \chi) \subset \mathcal{O}(\mathbb{H})$ le sous-espace des formes modulaires de poids k et caractère χ ; on pose aussi $M_k(\Gamma) = M_k(\Gamma, 1)$. Par exemple, $M_k = M_k(SL_2(\mathbb{Z}))$. Discutons un peu la seconde condition. Observons que si une fonction f satisfait la condition (i), alors pour tout $\gamma' \in \Gamma$, $\gamma \in SL_2(\mathbb{Z})$, et $m \in \mathbb{Z}$ on a

$$(f|_k \pm \gamma' \gamma T^m)(\tau) = \pm \chi(\gamma') (f|_k \gamma)(\tau + m).$$

Ainsi, $f|_k \pm \gamma' \gamma T^m$ admet une limite quand $\text{Im } \tau \rightarrow +\infty$ si, et seulement si, $f|_k \gamma$ a cette propriété. Autrement dit, pour vérifier la condition (ii) il suffit de le faire pour un ensemble de représentants γ des doubles classes $\Gamma \backslash SL_2(\mathbb{Z}) / \langle \pm I_2, T \rangle$.

Remarque 6.2. Bien que nous ne l'utiliserons pas, mentionnons que la condition (ii) admet une signification plus claire s'il on introduit les *pointes* de \mathbb{H} ("cusps" en anglais). Ce sont les éléments de $\hat{\mathbb{Q}}$. On vérifie que le groupe $SL_2(\mathbb{Z})$ agit transitivement sur $\hat{\mathbb{Q}}$, avec $\langle T, \pm I_2 \rangle$ pour stabilisateur de ∞ . L'ensemble $\Gamma \backslash SL_2(\mathbb{Z}) / \langle \pm I_2, T \rangle$ s'identifie alors à l'ensemble des orbites de Γ sur $\hat{\mathbb{Q}}$. La condition (ii) précise le comportement de $f(\tau)$ lorsque τ tend vers chacune des pointes selon le filtre des disques tangents à la pointe.

Lorsque l'on suppose que le groupe Γ est d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$, et que le caractère χ est d'image finie, on dispose d'une majoration intéressante de la dimension de $M_k(\Gamma, \chi)$. Si le caractère χ est d'image finie, on appelle ordre de χ le plus petit entier $e \geq 1$ tel que $\chi^e = 1$. Tout sous-groupe fini de \mathbb{C}^* étant cyclique, on a bien sûr $e = |\chi(\Gamma)|$.

Proposition 6.3. *Supposons Γ d'indice fini m dans $\mathrm{SL}_2(\mathbb{Z})$ et le caractère χ d'image finie. On a*

$$\dim M_k(\Gamma, \chi) \leq \frac{km}{12} + 1$$

pour tout entier $k \geq 0$. De plus, on a $M_k(\Gamma, \chi) = 0$ si $k < 0$.

Commençons par quelques remarques. La formule évidente $f|_k \gamma \times g|_k \gamma = (fg)|_{k+k'} \gamma$ entraîne que si $f \in M_k(\Gamma, \chi)$ et $g \in M_{k'}(\Gamma, \chi')$ alors $fg \in M_{k+k'}(\Gamma, \chi\chi')$. On en déduit que si $\chi^e = 1$ et $f \in M_k(\Gamma, \chi)$ alors $f^e \in M_{ke}(\Gamma)$. Pour la même raison, on constate que si $f \in M_k(\Gamma)$ et $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, alors $f|_k \gamma$ ne dépend que de la classe $\bar{\gamma}$ de γ dans $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$, nous la noterons $f|_k \bar{\gamma}$. En particulier, si $f \in M_k(\Gamma)$ il y a un sens à poser

$$\text{Norme } f = \prod_{x \in \Gamma \backslash \mathrm{SL}_2(\mathbb{Z})} f|_k x.$$

Lemme 6.4. *Supposons Γ d'indice fini m dans $\mathrm{SL}_2(\mathbb{Z})$, $k \in \mathbb{Z}$ et $f \in M_k(\Gamma)$. Alors $\text{Norme } f \in M_{km}$. De plus, $\text{Norme } f = 0$ si, et seulement si, $f = 0$.*

DÉMONSTRATION — Norme f est une fonction holomorphe sur \mathbb{H} , qui admet une limite quand $\mathrm{Im} \tau \rightarrow \infty$ par hypothèses sur f . Si $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, la multiplication à droite par γ sur l'ensemble fini $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$ est bien entendu bijective, de sorte $(\text{Norme } f)|_{mk} \gamma = \text{Norme } f$. On a montré $\text{Norme } f \in M_{mk}$. Par intégrité de l'anneau des fonctions holomorphes sur le connexe \mathbb{H} (i.e. par le principe des zéros isolés), $\text{Norme } f = 0$ entraîne qu'il existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $f|_k \gamma = 0$, puis $f = (f|_k \gamma)|_k \gamma^{-1} = 0$. \square

DÉMONSTRATION — (de la proposition 6.3) Soit N un entier ≥ 0 tel que $N > \frac{mk}{12}$. Soit $P \subset \mathcal{F}$ une partie arbitraire de l'intérieur de \mathcal{F} telle que $|P| = N$. Considérons l'application linéaire

$$M_k(\Gamma, \chi) \rightarrow \mathbb{C}^P, f \mapsto (f(p))_{p \in P}.$$

Il suffit de démontrer qu'elle est injective pour en déduire la proposition. Soient f dans son noyau et e l'ordre de χ . D'après le lemme ci-dessus, la fonction $g = \text{Norme } f^e$ est dans M_{ekm} . De plus, g est produit de f^e par une fonction holomorphe, et s'annule donc en chacun des N points de P avec un ordre d'annulation $\geq e$. La formule $k/12$, appliquée à la forme g de poids ekm , montre donc $g = \text{Norme } f^e = 0$, puis $f^e = f = 0$. \square

Remarque 6.5. Lorsque $k \neq 1$, le théorème de Riemann-Roch permet de donner une formule exacte pour la dimension de $M_k(\Gamma)$, en fonction d'un petit nombre d'invariants associés à Γ : voir le livre de Shimura référencé. Il n'existe pas en revanche de description générale des $M_k(\Gamma)$ qui soit aussi explicite que celle obtenue pour $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ et $\chi = 1$: chaque groupe Γ a son histoire. Nous examinerons ci-après le cas $\Gamma = J$.

7. LE ϑ -GROUPE EST DE CONGRUENCE

Si $N \geq 1$ est un entier on dispose d'un morphisme de groupes $\varepsilon_N : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ obtenu en réduisant les coefficients modulo N . Le noyau de ce morphisme est un sous-groupe noté $\Gamma(N)$ et appelé *sous-groupe de congruence principal de niveau N* . Il est un distingué et d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$. On dit qu'un sous-groupe $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ est de congruence s'il existe un entier $N \geq 1$ tel que $\Gamma(N) \subset \Gamma$.

Il ne serait pas difficile de démontrer que ε_N est surjectif, et qu'il induit donc un isomorphisme $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Vérifions-le pour $N = 2$. L'ensemble $\widehat{\mathbb{Z}/2\mathbb{Z}} = \{0, 1, \infty\}$ a trois éléments, et l'on dispose d'un homomorphisme $h : \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathfrak{S}(\widehat{\mathbb{Z}/2\mathbb{Z}})$ donné par l'action par homographies (§1.1). Il est injectif car la seule homothétie de $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ est I_2 . Les éléments $h\varepsilon_2(S)$ et $h\varepsilon_2(T)$ sont deux transpositions, la première fixant le point 1, la seconde le point ∞ . Ces dernières engendrant $\mathfrak{S}(\widehat{\mathbb{Z}/2\mathbb{Z}})$, on en déduit que h est un isomorphisme et que ε_2 est surjectif.

Proposition 7.1. (i) $J = \Gamma(2) \cup S\Gamma(2)$. En particulier, on a $\Gamma(2) \subset J$, et J est de congruence.

(ii) Les éléments $1, T$ et TS forment un système de représentants de $J \backslash \mathrm{SL}_2(\mathbb{Z})$. En particulier, J est d'indice 3 dans $\mathrm{SL}_2(\mathbb{Z})$.

(iii) Pour tout $\tau \in \mathbb{H}$, il existe $g \in J$ tel que $g\tau \in \mathcal{F} \cup T\mathcal{F} \cup TS\mathcal{F}$.

DÉMONSTRATION — Vérifions d'abord le (iii). Observons que $\mathcal{F} \cup T\mathcal{F} \cup TS\mathcal{F}$ est l'ensemble des $\tau \in \mathbb{H}$ tels que $-1/2 \leq \mathrm{Re} \tau \leq 3/2$, $|\tau| \geq 1$ et $|\tau - 2| \geq 1$ (figure 1.3). Comme les éléments S et ST^2 , d'homographies associées $\tau \mapsto -1/\tau$ et $\tau \mapsto -1/(\tau - 2)$ sont dans J , l'argument de maximalité donné dans la démonstration du théorème 1.4 (i) démontre le (iii).

Montrons maintenant le (ii). Choisissons un point τ dans l'intérieur de \mathcal{F} (ou simplement, qui n'est pas dans la $\mathrm{SL}_2(\mathbb{Z})$ -orbite de i ou ρ). Rappelons que d'après le théorème 1.4, les seuls éléments $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tels que $\gamma\tau \in \mathcal{F}$ sont $\pm I_2$. Soit $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. D'après le (iii) appliqué à $\gamma\tau$, il existe $g \in J$ tel que $g\gamma\tau$ soit dans $\mathcal{F}, T\mathcal{F}$ ou $TS\mathcal{F}$. Ainsi, le théorème 1.4 entraîne $\pm g\gamma = I_2, T$ ou TS . Comme $-I_2 = S^2 \in J$ on a montré

$$\mathrm{SL}_2(\mathbb{Z}) = J \cup JT \cup JTS.$$

Cette réunion est disjointe. En effet, si $g \in J$ (resp. JT, JTS) alors $\varepsilon_2(g^{-1})$ envoie $1 \in \widehat{\mathbb{Z}/2\mathbb{Z}}$ sur 1 (resp. $0, \infty$). Cela termine la démonstration du (ii), et démontre que J est l'ensemble des éléments $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tels que $\varepsilon_2(\gamma)$ fixe 1 . Autrement dit, on a $J = \Gamma(2) \cup S\Gamma(2)$. \square

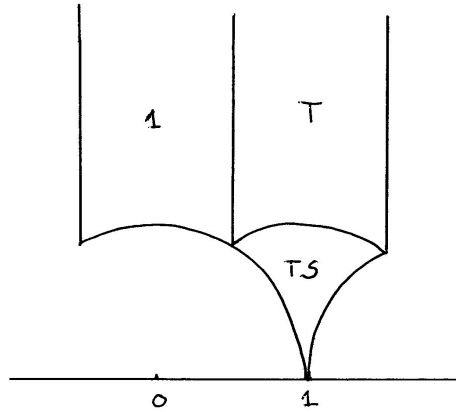


FIGURE 3. Le domaine $\mathcal{F} \cup T\mathcal{F} \cup TS\mathcal{F}$

8. SOMMES DE 8 CARRÉS

Observons que d'après la proposition 7.1, les classes des éléments 1 et

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

recouvrent $J \backslash \mathrm{SL}_2(\mathbb{Z}) / \langle \pm T \rangle$. Ainsi, si une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbb{C}$ satisfait la condition (i), elle satisfait (ii) si et seulement si les fonctions $f(\tau)$ et $(f|_k TS)(\tau) = \tau^{-k} f(1 - 1/\tau)$ admettent toutes deux des limites quand $\mathrm{Im} \tau \rightarrow \infty$. Pour des raisons de clarté, et tout en s'imposant une certaine prudence, ces limites seront notées respectivement $f(\infty)$ et $f(1)$, si elles existent. Soit $\chi : J \rightarrow \mathbb{C}^*$ le caractère introduit au §5.8.

Proposition 8.1. La fonction ϑ^2 est modulaire de poids 1 et caractère χ pour J . De plus, on a

$$\vartheta^2(\infty) = 1 \quad \text{et} \quad \vartheta^2(1) = 0.$$

Plus précisément, $\vartheta^2|_1 TS(\tau) = -i e^{\frac{i\pi\tau}{2}} \left(\sum_{n \in \mathbb{Z}} q^{\frac{n^2+n}{2}} \right)^2 = -i \tilde{\vartheta}(\tau)^2$.

DÉMONSTRATION — Compte tenu du corollaire 5.9, la seule chose qu'il reste à démontrer est l'assertion sur les limites. Il est évident que $\vartheta(\tau) \rightarrow 1$ quand $\text{Im } \tau \rightarrow +\infty$. Par définition, on a $\vartheta^2|_1 \text{TS}(\tau) = \tau^{-1} \vartheta^2(1 - 1/\tau)$. On conclut par la relation déjà vue au §5.10 :

$$(-i\tau)^{-1/2} \vartheta(1 - 1/\tau) = \tilde{\vartheta}(\tau).$$

□

Corollaire 8.2. (i) Pour tout entier $k \geq 0$, on a $\vartheta^{2k} \in M_k(\mathbb{J}, \chi^k)$.

(ii) (Jacobi) On a l'identité $(\vartheta \tilde{\vartheta} \tilde{\vartheta})^8 = 2^8 \Delta$. En particulier, ϑ ne s'annule pas sur \mathbb{H} .

DÉMONSTRATION — D'après la proposition 8.1, $\vartheta^2 \in M_1(\mathbb{J}, \chi)$. Le (i) en est une conséquence immédiate. Pour le (ii), on constate que le terme de gauche est Norme ϑ^8 au sens du §5.10. On observe que c'est un élément non nul de S_{12} dont le coefficient de Fourier en q est 2^8 ; la présence du 2 vient de la relation $\tilde{\vartheta}(\tau) = 2e^{\frac{i\pi\tau}{4}} + O(e^{\frac{i\pi\tau}{2}})$ quand $\text{Im } \tau \rightarrow \infty$. D'après la proposition 3.7, c'est nécessairement $2^8 \Delta$. □

On a $E_k \in M_k(\mathbb{J})$ car $M_k \subset M_k(\mathbb{J})$ pour tout $k \in \mathbb{Z}$. Comme $E_k = E_{k|_k} \text{TS}$, on a de plus $E_k(\infty) = E_k(1) = 1$. La construction de séries d'Eisenstein effectuée pour $\text{SL}_2(\mathbb{Z})$ admet des variantes pour les groupes de congruences. Nous nous contenterons d'illustrer ce phénomène dans le cas du groupe \mathbb{J} .

Proposition 8.3. Soit $k \geq 4$ un entier pair. La série $\sum_{(m,n) \in \mathbb{Z}^2 - \{0\}, m \equiv n \pmod{2}} \frac{1}{(m\tau + n)^k}$ est absolument convergente sur \mathbb{H} ; on note $G_k^*(\tau)$ sa somme. On a $G_k^* \in M_k(\mathbb{J})$, $G_k^*(\infty) = 2^{1-k} \zeta(k)$ et $G_k^*(1) = 2\zeta(k)$. Enfin, on a

$$\frac{2^{k-1}}{\zeta(k)} G_k^*(\tau) = 1 - \frac{2k}{B_k} \sum_{n \geq 1} (-1)^n \sigma_{k-1}(n) e^{i\pi n \tau}.$$

DÉMONSTRATION — On procède de manière strictement identique à la démonstration de la proposition 4.2. La convergence absolue de $G_k^*(\tau)$ ainsi que son invariance par l'action de poids k de \mathbb{J} est claire. De même, $G_k(\tau)$ tend vers $2^{1-k} \zeta(k)$ quand $\text{Im } \tau \rightarrow \infty$. On constate enfin que

$$\tau^{-k} G_k(1 - 1/\tau) = \sum_{(m,n) \in \mathbb{Z}^2 - \{0\}, m \equiv n \pmod{2}} \frac{1}{((m+n)\tau - m)^k} = \sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{(2m\tau + n)^k},$$

qui tend vers $2\zeta(k)$ quand $\text{Im } \tau \rightarrow +\infty$. Pour le dernier point, on peut procéder comme dans la démonstration de la proposition 4.2. Mieux, on peut le déduire du q -développement de E_k en observant la relation (immédiate!) $G_k^*(\tau) = 2^{-k} G_k(\frac{\tau+1}{2})$. □

Si k est pair > 2 , on pose $E_k^* = \frac{2^{k-1}}{\zeta(k)} G_k^*$. On considère également $u : M_k(\mathbb{J}) \rightarrow \mathbb{C} \times \mathbb{C}$, $f \mapsto (f(\infty), f(1))$; c'est une application linéaire.

Proposition 8.4. (i) Si $k > 2$ est pair, l'application u est surjective.

(ii) $M_4(\mathbb{J})$ est de dimension 2 engendré par E_4 et E_4^* .

DÉMONSTRATION — La proposition précédente entraîne $u(E_k) = (1, 1)$ et $u(E_k^*) = (1, 2^k)$, d'où la surjectivité de u . Le groupe \mathbb{J} est d'indice 3 dans $\text{SL}_2(\mathbb{Z})$ (Prop. 7.1). La proposition 6.3 entraîne que $M_4(\mathbb{J})$ est de dimension ≤ 2 . On conclut car il contient E_4 et E_4^* , et $u(E_k)$ et $u(E_k^*)$ ne sont pas proportionnels. □

Théorème 8.5. (Jacobi, 1829) On a l'identité $\vartheta^8 = \frac{1}{15}(16E_4 - E_4^*)$. En particulier, si $r_8(n)$ désigne le nombre de $(n_1, \dots, n_8) \in \mathbb{Z}^8$ tels que $\sum_{i=1}^8 n_i^2 = n$, on a la relation

$$r_8(n) = 16 \sum_{d|n} (-1)^{n-d} d^3.$$

DÉMONSTRATION — Les propositions 8.1 et 8.4 montrent qu'il existe $a, b \in \mathbb{C}$ tels que $\vartheta^8 = aE_4 + bE_4^*$ et

$$u(\vartheta^8) = (1, 0) = (a + b, a + 16b).$$

On trouve $(a, b) = (\frac{16}{15}, \frac{-1}{15})$. Étant donné que $240 = 15 \cdot 16$, on a donc

$$\sum_{n \geq 0} r_8(n) q^n = \vartheta^8(2\tau) = 1 + 16 \sum_{n \geq 1} \sigma_3(n) (16q^{2n} - (-1)^n q^n).$$

Si n est impair, le coefficient de q^n dans la somme ci-dessus est $\sigma_3(n)$. Si n est pair, il s'agit plutôt de $-\sigma_3(n) + 16\sigma_3(n/2)$. Mais comme dans ce cas on a $16\sigma_3(n/2) = 2 \sum_{2|d|n} d^3$, on a aussi la relation $-\sigma_3(n) + 16\sigma_3(n/2) = \sum_{d|n} (-1)^d d^3$. \square

En particulier, si p est un nombre premier impair on a simplement $r_8(p) = 16(p^3 + 1)$. Par exemple pour $p = 3$ on a $r_8(3) = 2^3 C_8^3 = 8^2 \cdot 7 \dots$ qui vaut bien $16 \cdot 28$. De même, $2^5 \cdot C_8^5 + 8 \cdot 7 \cdot 2^2 = 2016 = 16(5^3 + 1)$ (!). On obtient bien d'autres formules fabuleuses pour les sommes de $8k$ carrés en étudiant plus généralement $M_{4k}(J)$. Un ingrédient clé, maintenant à notre portée, est alors le suivant :

Théorème 8.6. (i) Si $k \equiv 0 \pmod{4}$, l'espace $M_k(J)$ est de dimension $\frac{k}{4} + 1$. Il admet pour base les $E_4^r(E_4^*)^s$ avec $r + s = k/4$.

(ii) Si $k \not\equiv 0 \pmod{4}$ alors $M_k(J, \chi^k) = \vartheta^2 M_{k-1}(J, \chi^{k-1})$.

DÉMONSTRATION — Montrons le (i). La famille de l'énoncé est libre par un argument semblable (en plus simple) à celui de la proposition 2.5. Elle est de cardinal $\frac{k}{4} + 1$. On conclut car $\dim M_k(J) \leq \frac{k}{4} + 1$ d'après la proposition 6.3, le groupe J étant d'indice 3 dans $SL_2(\mathbb{Z})$. Pour démontrer le (ii), il suffit de démontrer que si $f \in M_k(J, \chi^k)$ avec $k \not\equiv 0 \pmod{4}$ alors $g(\tau)e^{-i\pi\tau/2}$ admet une limite quand $\text{Im } \tau$ tends vers $+\infty$, où $g = f|_k \text{TS}$. En effet, étant donné que $\vartheta(\tau)$ ne s'annule pas dans \mathbb{H} (Corollaire 8.2 (ii)), la proposition 8.1 permet de conclure $f/\vartheta^2 \in M_{k-1}(J, \chi^{k-1})$. Mais $\text{TSTS}^{-1}\text{T}^{-1} = -\text{ST}^{-1}\text{SS}^{-1}\text{T}^{-1} = -\text{ST}^{-2}$ est un élément de J de caractère i , et de sorte que $g(\tau + 1) = i^k g(\tau)$, ce qui conclut. \square

Pour aller plus loin, il nous resterait à définir une série d'Eisenstein vivant dans $M_k(J, \chi^k)$ avec k non nécessairement $\equiv 0 \pmod{4}$. C'est particulièrement difficile pour des raisons de convergence lorsque $k = 2$, et pire encore lorsque $k = 1$. Cela permettrait de démontrer par exemple les formules célèbres, valables pour tout $n \geq 1$,

$$r_2(n) = 4 \sum_{d|n} \psi(d), \quad r_4(n) = 8 \sum_{4 \nmid d|m} d^3.$$

La première est due à Gauss ; dans cette formule $\psi(d)$ vaut par définition 0 si d est pair, 1 si $d \equiv 1 \pmod{4}$ et -1 sinon. Il en existe une autre une preuve très simple utilisant l'arithmétique de $\mathbb{Z}[i]$. La seconde est due à Jacobi. De même, il en existe une preuve relativement transparente utilisant l'arithmétique des quaternions de Hurwitz. Signalons que Gauss a également trouvé une formule pour $r_3(n)$, d'apparence assez différente, dont l'établissement pourrait par exemple être obtenu par les principes étudiés ici si l'on avait introduit les formes modulaires de poids "demi-entier". Enfin, il existe des formules raisonnablement simples pour $r_k(n)$ pour tout $k \leq 10$ pair...