Milan Berger-Guesneau

Notes pour la sixième séance du groupe de lecture

On notera dans la suite $\mathcal{H}$ le demi-plan de Poincaré.

Définition 1. *Un réseau Λ de $\mathbb{R}^d$ est un sous-groupe discret de $\mathbb{R}^d$ qui engendre $\mathbb{R}^d$ (en tant que $\mathbb{R}$-espace vectoriel). De manière équivalente, c'est l'ensemble des combinaisons linéaires entières d'éléments d'une base de $\mathbb{R}^d$.*

Voici un outil utile dans l'étude des réseaux.

Définition 2. *Soit Λ un réseau de $\mathbb{R}^d$. On définit sa fonction thêta par*

$$\theta_\Lambda(z) = \sum_{\lambda \in \Lambda} e^{i\pi z \|\lambda\|^2} = \sum_{n=0}^{+\infty} \#\{\lambda \in \Lambda |\ \|\lambda\|^2 = n\}\, e^{i\pi z n}$$

pour tout $z \in \mathcal{H}$.

On se demande si la donnée d'une fonction thêta détermine le réseau.

Définition 3. *Soit Γ un sous-groupe d'indice fini de $SL_2(\mathbb{Z})$, soit $k \in \mathbb{Z}$. Une forme modulaire de poids k pour Γ est une fonction holomorphe $f : \mathcal{H} \to \mathbb{C}$ telle que*

1. *pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, pour tout $z \in \mathcal{H}$,*

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

2. *pour tout $z \in \mathcal{H}$, $f(z)$ est bornée quand $Im(z) \to +\infty$.*

On note $M_k(\Gamma)$ l'espace vectoriel des formes modulaires de poids k pour Γ.

Remarque. On peut déjà faire quelques observations faciles mais utiles.

— Si $-I_2 \in \Gamma$, la première condition donne $f = (-1)^k f$. Ainsi, si k est impair,

$$M_k(\Gamma) = \{0\}$$

— Il suffit de vérifier la première identité sur les générateurs de Γ. Par exemple, pour $\Gamma = SL_2(\mathbb{Z})$, la condition de modularité est équivalente à dire que f est 1-périodique et vérifie

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

— Si $f \in M_k(\Gamma)$ et $g \in M_l(\Gamma)$, alors $fg \in M_{k+l}(\Gamma)$.

— Le fait que Γ soit d'indice fini dans $SL_2(\mathbb{Z})$ implique qu'il contient un sous-groupe de la forme

$$\left\{ \begin{pmatrix} 1 & hn \\ 0 & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \right\}$$

où $h \in \mathbb{N}^*$. Une forme modulaire est donc toujours périodique de période entière.

Définition 4. *On pose, pour $N \geqslant 1$,*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| N \mid c \right\}$$

C'est un sous-groupe d'indice fini de $SL_2(\mathbb{Z})$.

Remarque. Supposons que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$. Les formes modulaires pour Γ sont 1-périodiques ; on peut donc les développer en série de Fourier. Si f est une forme modulaire, il existe une suite $(a_n) \subset \mathbb{C}$ telle que

$$f(z) = \sum_{n=0}^{+\infty} a_n q^n$$

où $q = e^{2i\pi z}$. On peut donc voir une forme modulaire comme une série entière sur le disque unité ouvert.

Exemple. On définit, pour $k \geqslant 4$ (pair), la série d'Eisenstein de poids k par

$$G_k(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k}$$

C'est une série absolument convergente pour tout $z \in \mathcal{H}$, qui converge uniformément sur tout compact et qui est donc holomorphe sur $\mathcal{H}$. C'est en fait une forme modulaire de poids k pour $SL_2(\mathbb{Z})$; son développement en série entière est

$$\begin{aligned} G_k(z) &= 2\zeta(k) + \frac{2(2i\pi)^k}{(k-1)!} \sum_{n=1}^{+\infty} \sigma_{k-1}(n)\, q^n \\ &= 2\zeta(k) - \frac{4k\zeta(k)}{B_k} \sum_{n=1}^{+\infty} \sigma_{k-1}(n)\, q^n \end{aligned}$$

où $\sigma_m(n) = \sum_{d|n} d^m$.
Par analogie avec le cas $k \geqslant 4$, on définit

$$\begin{aligned} G_2(z) &= 2\zeta(2) + \frac{2(2i\pi)^2}{(2-1)!} \sum_{n=1}^{+\infty} \sigma_{2-1}(n)\, q^n \\ &= \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma(n)\, q^n \end{aligned}$$

G_2 n'est pas une forme modulaire, mais pas loin : elle vérifie, pour tout $z \in \mathcal{H}$,

$$G_2\left(-\frac{1}{z}\right) = z^2 G(z) - 2i\pi z$$

On normalise souvent les G_k en posant $E_k = G_k / 2\zeta(k)$.

Posons

$$\Delta = \frac{1}{1728}\left(E_4^3 - E_6^2\right)$$

C'est une forme modulaire de poids 12 pour $SL_2(\mathbb{Z})$. On remarque que $\Delta(z) \to 0$ quand $\mathrm{Im}(z) \to +\infty$. On peut montrer que Δ ne s'annule pas sur $\mathcal{H}$ en démontrant l'identité

$$\Delta(z) = q \prod_{n=1}^{+\infty} (q^n - 1)^{24}$$

On va à présent prouver un théorème fondamental.

Théorème 1. *Pour tout $k \in \mathbb{Z}$, $M_k = M_k(SL_2(\mathbb{Z}))$ est de dimension finie. De plus, si k est pair,*

$$\dim M_k = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 \ \textit{si } k \geqslant 0 \textit{ et } k \equiv 2\,[12] \\ \lfloor \frac{k}{12} \rfloor \ \textit{si } k \geqslant 0 \textit{ et } k \not\equiv 2\,[12] \\ 0 \ \textit{si } k < 0 \end{cases}$$

Séparons la preuve du théorème en trois lemmes.

Lemme 1. *Si $k < 0$, alors $M_k = \{0\}$.*

Démonstration. Soit $f(z) = \sum_{n=0}^{+\infty} a_n q^n \in M_k$ avec $k < 0$. Rappelons que si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, alors

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

La condition de modularité de f implique

$$\begin{aligned} \left|f\left(\frac{az+b}{cz+d}\right)\right| \mathrm{Im}\left(\frac{az+b}{cz+d}\right)^{\frac{k}{2}} &= |cz+d|^k\,|f(z)|\,\frac{\mathrm{Im}(z)^{\frac{k}{2}}}{|cz+d|^k} \\ &= |f(z)|\,\mathrm{Im}(z)^{\frac{k}{2}} \end{aligned}$$

La fonction $z \mapsto |f(z)|\,\mathrm{Im}(z)^{\frac{k}{2}}$ est donc invariante sous l'action de $SL_2(\mathbb{Z})$. Il suffit donc d'étudier ses valeurs sur le domaine fondamental

$$\mathcal{D} = \left\{ z \in \mathcal{H} \,\middle|\, |\mathrm{Re}(z)| \leqslant \frac{1}{2}, |z| \geqslant 1 \right\}$$

On sait que $|f(z)|\,\mathrm{Im}(z)^{k/2} \to 0$ quand $\mathrm{Im}(z) \to +\infty$. Il existe donc $\alpha > 0$ tel que si $\mathrm{Im}(z) > \alpha$ alors $|f(z)|\,\mathrm{Im}(z)^{k/2} \leqslant 1$. De plus cette même fonction est bornée sur le compact $\{z \in \mathcal{D} \mid \mathrm{Im}(z) \leqslant \alpha\}$. Il existe donc $C > 0$ tel que pour tout $z \in \mathcal{D}$ (et donc pour tout $z \in \mathcal{H}$),

$$|f(z)|\,\mathrm{Im}(z)^{k/2} \leqslant C$$

Soit $y > 0$, soit $m \in \mathbb{N}$. On a

$$f(x+iy) = \sum_{n=0}^{+\infty} a_n q^n = \sum_{n=0}^{+\infty} a_n e^{-2\pi n y} e^{2i\pi n x}$$

et donc

$$\begin{aligned} \int_0^1 f(x+iy)\, e^{-2i\pi m x}\, dx &= \sum_{n=0}^{+\infty} a_n e^{-2\pi n y} \underbrace{\int_0^1 e^{2i\pi(n-m)x}\, dx}_{\delta_{m,n}} \\ &= a_m e^{-2\pi m y} \end{aligned}$$

i.e.

$$a_m = e^{2\pi m y} \int_0^1 f(x+iy)\, e^{-2i\pi m x}\, dx$$

On en déduit

$$|a_m| \leqslant e^{2\pi m y} \int_0^1 C y^{-\frac{k}{2}} \, dx = C e^{2\pi m y} y^{-\frac{k}{2}}$$

Comme cette quantité tend vers 0 quand y tend vers 0, on a $a_m = 0$. On a montré que tous les coefficients de Fourier de f sont nuls, i.e. $f = 0$. □

Lemme 2. *Le théorème est vrai pour* $k \in \{0, 2, 4, 6, 8, 10\}$.

Démonstration. On commence par traiter le cas $k \in \{4, 6, 8, 10\}$. Soit $f \in M_k$. On remarque que $f - a_0 E_k \in M_k$ et que son coefficient constant dans sa décomposition en série entière est nul. La fonction $(f - a_0 E_k)/\Delta$ est holomorphe sur $\mathcal{H}$, et reste bornée quand $\mathrm{Im}(z) \to +\infty$. Elle vérifie de plus les conditions de modularité pour $k - 12$; c'est donc une forme modulaire de poids $k - 12 < 0$. Par le lemme précédent, $f = a_0 E_k$ ce qui montre $M_k = \mathbb{C} E_k$.
Le cas $k = 0$ est identique au précédent, il suffit de remplacer E_k par 1. On montre alors $M_0 = \mathbb{C}$.
Il reste à voir le cas $k = 2$. Soit $f \in M_2$. La condition de modularité donne

$$f(i) = f\left(-\frac{1}{i}\right) = i^2 f(i) = -f(i)$$

donc $f(i) = 0$. Or $f^2 \in M_4 = \mathbb{C} E_4$; il existe donc $\lambda \in \mathbb{C}$ tel que $f^2 = \lambda E_4$. Évaluons cette égalité en i : on obtient

$$\begin{aligned} 0 &= \lambda E_4(i) \\ &= \lambda \left(1 - \frac{8}{B_4} \sum_{n=0}^{+\infty} \sigma_3(n) e^{2i\pi n i}\right) \\ &= \lambda \underbrace{\left(1 + 240 \sum_{n=0}^{+\infty} \sigma_3(n) e^{-2\pi n}\right)}_{>0} \end{aligned}$$

Il en découle $\lambda = 0$ puis $f = 0$. □

Lemme 3. *Soit* $k \geqslant 12$ *pair. On a un isomorphisme* $\mathbb{C} \oplus M_{k-12} \cong M_k$

Démonstration. Soit $f \in M_k$, avec $k \geqslant 12$ pair. On sait $(f - a_0 E_k)/\Delta \in M_{k-12}$; on peut donc écrire

$$f = a_0 E_k + g\Delta$$

avec $g \in M_{k-12}$. L'application linéaire

$$\begin{aligned}\mathbb{C} \oplus M_{k-12} &\to M_k \\ (\lambda, g) &\mapsto \lambda E_k + g\Delta\end{aligned}$$

est donc surjective. Il reste à montrer qu'elle est injective : supposons $\lambda E_k + g\Delta = 0$. En regardant les coefficients constants on voit $\lambda = 0$. On a donc $\Delta g = 0$ puis $g = 0$. $\square$

Terminons la preuve du théorème : on a montré $\dim M_k = \dim M_{k-12} + 1$ si $k \geqslant 12$. De plus, le terme de droite du théorème vérifie la même formule de récurrence et coïncide avec $\dim M_k$ pour $0 \leqslant k < 12$. D'où le résultat.

On pose

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

de telle sorte que pour tout $k \geqslant 1$,

$$\theta(z)^k = \theta_{\mathbb{Z}^k}(2z) = \sum_{n=0}^{+\infty} r_k(n) q^n$$

où $r_k(n)$ est le nombre d'écritures de n comme somme de k carrés d'entiers relatifs. Voyons comment on peut donner une formule explicite pour $r_4(n)$.

On commence par rappeler la formule de Poisson.

Proposition 1. *Soit $f : \mathbb{R} \to \mathbb{C}$ intégrable et continue. Si $g : x \mapsto \sum_{n\in\mathbb{Z}} f(x+n)$ est $\mathcal{C}^\infty$, converge absolument et uniformément sur tout compact, alors*

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

Démonstration. g est périodique et $\mathcal{C}^\infty$ donc on peut écrire $g(x) = \sum_{n\in\mathbb{Z}} c_n e^{2i\pi nx}$. Or

$$\begin{aligned}c_n &= \int_0^1 g(u)e^{-2i\pi nu}\,du \\ &= \sum_{k\in\mathbb{Z}} \int_0^1 f(u+k)e^{-2i\pi n(u+k)}\,du \\ &= \sum_{k\in\mathbb{Z}} \int_k^{k+1} f(v)e^{-2i\pi nv}\,dv \\ &= \widehat{f}(n)\end{aligned}$$

On a montré

$$g(x) = \sum_{n \in \mathbb{Z}} \widehat{f}(n) e^{2i\pi n x}$$

Le choix $x = 0$ permet de conclure. $\square$

Lemme 4. $\Gamma_0(4)$ *est engendré par* $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$.

Théorème 2. $\theta^4 \in M_2(\Gamma_0(4))$

Démonstration. Il suffit de vérifier que θ^4 vérifie la condition de modularité pour les trois générateurs de $\Gamma_0(4)$, qui sont triviales pour les deux premiers. Il reste donc à voir

$$\theta^2 \left(\frac{z}{4z+1} \right) = (4z+1)\theta^2(z)$$

Posons $x = -\frac{4z+1}{4z} = -(1 + 1/4z)$. On a $z = -1/4(x+1)$ et donc $4z+1 = 1 - 1/(x+1) = x/(x+1)$. Supposons temporairement que

$$\theta^2 \left(-\frac{1}{4x} \right) = -2ix\theta^2(x) \tag{$*$}$$

On aura alors

$$\begin{aligned} (4z+1)\theta^2(z) &= \frac{x}{x+1} \theta^2 \left(-\frac{1}{4(x+1)} \right) \\ &= \frac{x}{x+1} \left(-2i(x+1) \right) \theta^2(x+1) \\ &= -2ix\theta^2(x) \\ &= \theta^2 \left(-\frac{1}{4x} \right) \\ &= \theta^2 \left(\frac{z}{4z+1} \right) \end{aligned}$$

Montrons donc $(*)$. Posons $s = i/2x$, de telle sorte que $(*)$ se réécrive

$$\frac{1}{s} \theta^2 \left(\frac{i}{2s} \right) = \theta^2 \left(\frac{is}{2} \right)$$

Par prolongement analytique, il suffit de montrer cette formule pour $s \in \mathbb{R}_+^*$. On s'est donc ramenés à montrer

$$\theta \left(\frac{is}{2} \right) = \frac{1}{\sqrt{s}} \theta \left(\frac{i}{2s} \right)$$

i.e.

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

pour tout $s > 0$.
Soit $f(s) = e^{-\pi s x^2}$. On a

$$\begin{aligned}
\widehat{f}(n) &= \int_{\mathbb{R}} e^{-\pi s x^2 + 2i\pi x n}\, dx \\
&= \int_{\mathbb{R}} e^{-\pi s \left(x - \frac{in}{s}\right)^2} e^{\frac{\pi n^2}{s}}\, dx \\
&= e^{\frac{\pi n^2}{s}} \int_{\mathbb{R}+\frac{in}{s}} e^{-\pi s x^2}\, dx \\
&= e^{\frac{\pi n^2}{s}} \int_{\mathbb{R}} e^{-\pi s x^2}\, dx \\
&= \frac{1}{\sqrt{s}} e^{\frac{\pi n^2}{s}}
\end{aligned}$$

La formule de Poisson appliquée à f donne immédiatement le résultat. □

La proposition suivante est le dernier ingrédient dont nous aurons besoin.

Proposition 2. *On a* $\dim M_2(\Gamma_0(4)) = 2$. *De plus, une base en est donnée par les fonctions*

$$\varphi(z) = 2E_2(2z) - E_2(z) = 1 + 24 \sum_{n=1}^{+\infty} \left(\sum_{\substack{d \mid n \\ 2 \nmid d}} d \right) q^n$$

et

$$\psi(z) = 4E_2(4z) - E_2(z) = 3 + 24 \sum_{n=1}^{+\infty} \left(\sum_{\substack{d \mid n \\ 4 \nmid d}} d \right) q^n$$

On peut à présent montrer le théorème de Jacobi.

Théorème 3. *Pour tout* $n \in \mathbb{N}$, *il y a*

$$\sum_{\substack{d \mid n \\ 4 \nmid d}} d$$

façons d'écrire n *comme somme de quatre carrés.*

Démonstration. Le théorème et la proposition précédents montrent qu'il existe $\lambda, \mu \in \mathbb{C}$ tel que

$$\sum_{n=0}^{+\infty} r_4(n)q^n = \theta^4(z) = \lambda\varphi(z) + \mu\psi(z)$$

En regardant les deux premiers coefficients dans les développements en série entière, on obtient

$$\begin{cases} 1 = \lambda + 3\mu \\ 8 = 24\lambda + 24\mu \end{cases}$$

ce qui équivaut à

$$\begin{cases} \lambda = 0 \\ \mu = \frac{1}{3} \end{cases}$$

On a donc $\theta^4 = (1/3)\psi$; on peut conclure en identifiant les coefficients. □

On répond à présent à la question originalement posée.

Définition 5. *Un réseau Λ de $\mathbb{R}^d$ est dit*

— *unimodulaire si $\lambda_d(\mathbb{R}^d/\Lambda) = 1$.*

— *pair si $\|\lambda\|^2 \in 2\mathbb{Z}$ pour tout $\lambda \in \Lambda$.*

Proposition 3. *Soit Λ un réseau unimodulaire pair de $\mathbb{R}^n$. Alors pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$,*

$$\theta_\Lambda\left(\frac{az+b}{cz+d}\right) = (cz+d)^{\frac{n}{2}}\theta_\Lambda(z)$$

Corollaire 6. *Si Λ est un réseau unimodulaire pair de $\mathbb{R}^d$, alors d est un multiple de 8.*

Démonstration. On a

$$\theta_\Lambda(i) = \theta_\Lambda\left(-\frac{1}{i}\right) = (-i)^{\frac{d}{2}}\theta_\Lambda(i)$$

ce qui implique $(-i)^{\frac{d}{2}} = 1$ i.e. 8 divise d. □

Corollaire 7. *Soit Λ un réseau unimodulaire pair de $\mathbb{R}^d$. Alors $\theta_\Lambda \in M_{\frac{d}{2}}(SL_2(\mathbb{Z}))$.*

Définition 8. *Soit $d \in \mathbb{N}$ multiple de 8. On définit le réseau Λ_d de $\mathbb{R}^d$ par*

$$\Lambda_d = \left\{ \lambda \in \mathbb{Z}^d \cup \left(\mathbb{Z}^d + \frac{1}{2}\right) \middle| \sum_i \lambda_i \in 2\mathbb{Z} \right\}$$

Une base en est donnée par les vecteurs

$$\begin{aligned}
&(2, 0, \ldots, 0)\\
&(-1, 1, 0, \ldots, 0)\\
&(0, -1, 1, 0, \ldots, 0)\\
&\vdots\\
&(0, \ldots, 0, -1, 1, 0, \ldots, 0)\\
&\vdots\\
&(0, \ldots, 0, -1, 1, 0)\\
&(1/2, \ldots, 1/2)
\end{aligned}$$

C'est un réseau unimodulaire ; en effet, la matrice dont les colonnes sont les coordonnées de ces vecteurs est de determinant 1.

C'est également un réseau pair.
Si $\lambda \in \Lambda_d \cap \mathbb{Z}^d$, la condition sur la parité de $\sum \lambda_i$ implique que les λ_i impairs sont en nombre pair. Ainsi

$$\|\lambda\|^2 = \sum_{\lambda_i \text{ pair}} \lambda_i^2 + \sum_{\lambda_i \text{ impair}} \lambda_i^2 \in 2\mathbb{Z}$$

Si $\lambda \in \Lambda_d \cap (\mathbb{Z}^d + 1/2)$, on a $\lambda = \mu + (1/2, \ldots, 1/2)$ avec $\mu \in \mathbb{Z}^d$. Écrivons $d = 8k$; on a

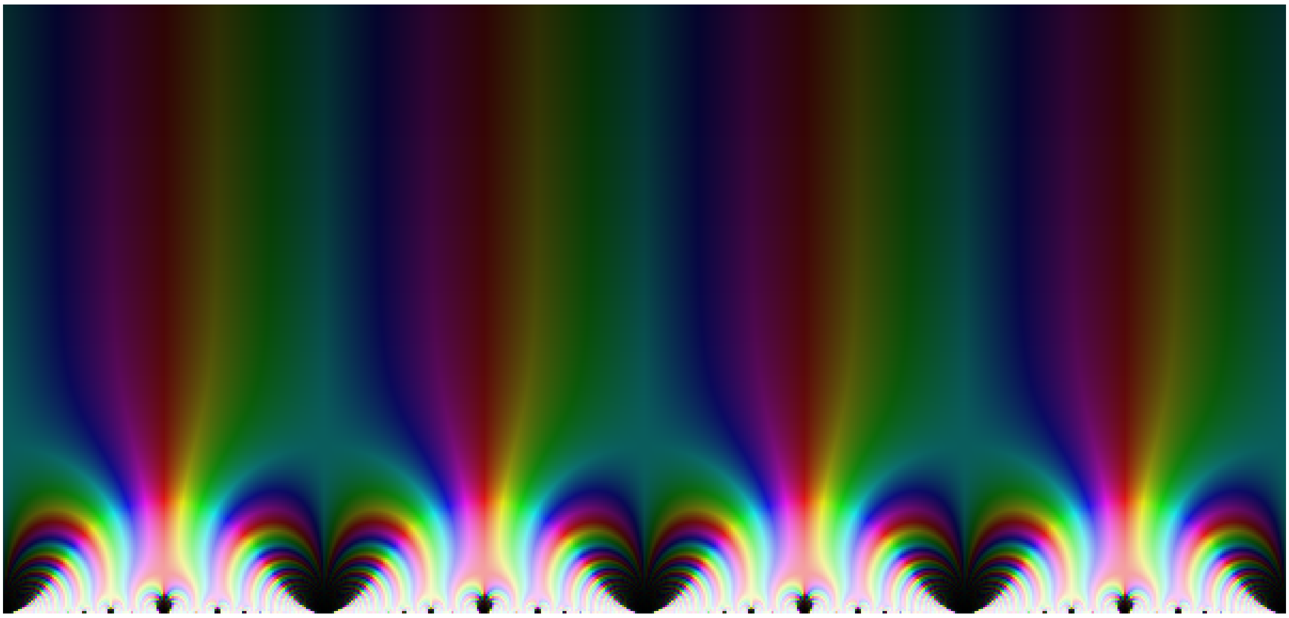
$$\sum_i \mu_i = \sum_i \left(\lambda_1 - \frac{1}{2}\right) = \sum_i \lambda_i - 4k \in 2\mathbb{Z}$$

donc $\mu \in \Lambda_d \cap \mathbb{Z}^d$. Par le point précédent, $\|\mu\|^2 \in 2\mathbb{Z}$. Finalement,

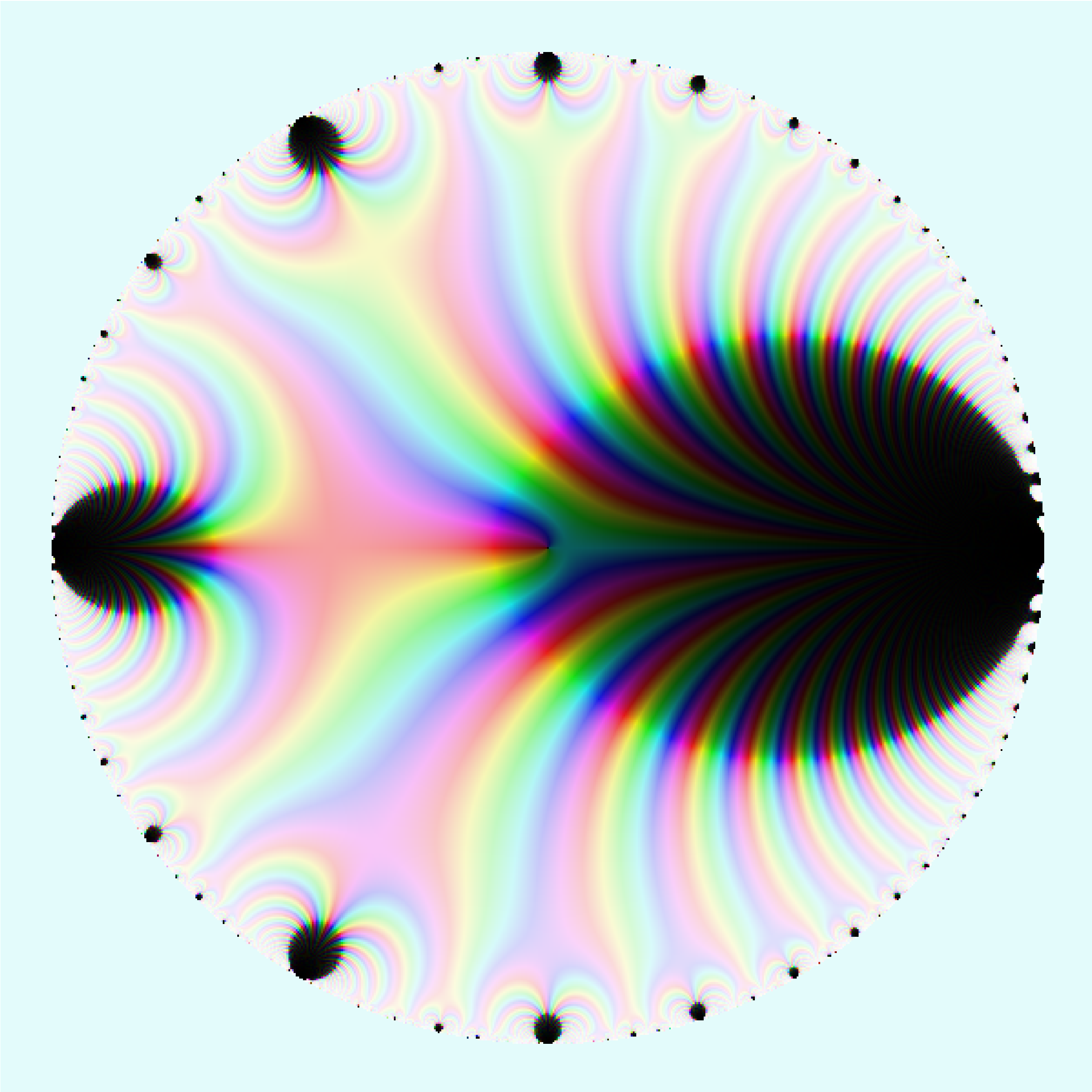
$$\|\lambda\|^2 = \sum_i \left(\mu_i + \frac{1}{2}\right)^2 = \|\mu\|^2 + \sum_i \mu_i + 2k \in 2\mathbb{Z}$$

ce qui conclut.

On a donc deux réseaux unimodulaires pairs de $\mathbb{R}^{16}$: $\Lambda_8 \times \Lambda_8$ et Λ_{16}. Leurs fonctions thêta sont des formes modulaires de poids 8 sur $SL_2(\mathbb{Z})$ de même coefficient constant ; elles sont donc égales. La fonction thêta ne détermine donc pas le réseau. Il reste à voir que $\Lambda_8 \times \Lambda_8$ et Λ_{16} ne sont pas isomorphes...



Représentation de Δ sur $[-2, 2] + i[0, 2]$



Représentation de Δ sur le disque unité