Le réseau E_8

Francisco J. Vial Prado
2011

Résumé

On étudie le réseau $E_8 \subset \mathbb{R}^8$ au moyen de la théorie des formes modulaires et fonctions thêta. En exhibant sa fonction thêta on montre le résultat suivant : tout nombre entier pair positif peut s'écrire sous la forme $2(x_1^2 + x_7x_8 - x_1x_2) + \sum_{i=1}^{8}(x_i - x_{i+1})^2$ (où la somme est cyclique), $x \in \mathbb{Z}^8$.

Table des matières

1 Préliminaires

On commence par rappeler quelques concepts et théorèmes de base dans la théorie des formes modulaires et la géométrie des nombres, pour arriver à la construction du réseau E_8 et la fonction thêta associée.

1.1 Réseaux

Soit V un espace vectoriel de dimension finie, muni d'une mesure invariante μ.

Définition 1. *Un **réseau de V** est un sous-groupe discret de V qui engendre V comme $\mathbb{R}$-espace vectoriel.*

Proposition 1. *(i) Tout réseau admet une famille $\mathbb{Z}$-génératrice qui est une $\mathbb{R}$-base de V.*

(ii) Si Γ est un réseau, le ***covolume*** *de Γ, noté* $\mathrm{covol}(\Gamma)$ *est la quantité*[1] $\mu\left(\frac{V}{\Gamma}\right)$. *Si $\Gamma' \subset \Gamma$ est un sous-groupe d'indice fini, Γ' est un réseau de $\mathbb{R}^n$ et* $\mathrm{covol}(L') = |\Gamma/\Gamma'|\,\mathrm{covol}(\Gamma)$.

Définition 2. *Soit $e = \{e_1, \cdots, e_n\}$ une base de V. Alors le sous-groupe $L(e) = \oplus_i \mathbb{Z}e_i$ est un réseau de V que nous appelons* ***réseau engendré par e****.*

Proposition 2. *Si e, f sont deux bases de V et P est la matrice de e dans la base f, alors $L(e) = L(f)$ si et seulement si $P \in GL_n(\mathbb{Z})$, ou ce qui revient au même $P \in \{M \in M_n(\mathbb{Z}), \det(M) = \pm 1\}$.*

Pour voir les preuves nous renvoyons au lecteur à [Ch], Chapitre 2 : "Géométrie des nombres" Théorème 2.3 et Proposition 2.1.

1.2 Groupe modulaire et domaine fondamental

On note $H = \mathbb{R} \oplus i\mathbb{R}_*^+$ le demi-plan de Poincaré et $SL_2(\mathbb{Z})$ le sous-groupe de $M_n(\mathbb{R})$ des matrices de déterminant 1. On fait agir $SL_2(\mathbb{R})$ sur $\widetilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ par l'application de Möbius $GL_2(\mathbb{R}) \to \widetilde{\mathbb{C}}$, $\quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \dfrac{az+b}{cz+d}$ et on vérifie aisément que H est stable par $SL_2(\mathbb{R})$.

Définition 3. *Le groupe $G = SL_2(\mathbb{Z})/\{\pm 1\}$ est appelé le* ***groupe modulaire****. L'ensemble $D = \{z \in H, -1/2 \leq \Re z < 1/2, |z| \geq 1$ si $\Re z \leq 0$ et $|z| > 1$ sinon$\}$ est la fermeture domaine fondamental de G : en particulier on a $H = GD$.*

Pour voir ceci, on constate que deux générateurs de G sont $S : z \mapsto -1/z$ et $T : z \mapsto z+1$. Pour visualiser cette construction, consulter [Se], chap. VII.

1.3 Formes modulaires

Définition 4. *Une fonction $f : H \to \mathbb{C}$ est dite* ***faiblement modulaire de poids 2k*** *si elle est méromorphe dans H vérifiant*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z),\ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Proposition 3 (*Caractérisation des formes faiblement modulaires*)**.** *Une fonction méromorphe f est faiblement modulaire de poids $2k$ si et seulement si elle est invariante par S et T, c'est à dire*

$$f(z+1) = f(z), \qquad f(-1/z) = z^{2k} f(z).$$

La relation $f(z+1) = f(z)$ implique que l'on peut exprimer f comme fonction de $q = e^{2i\pi z}$. On note cette fonction $\tilde{f}$, elle est méromorphe dans le disque $|q| < 1$ privé de l'origine. On dira que "f est méromorphe à l'infini" si $\tilde{f}$ est méromorphe en $q = 0$, dans ce cas elle admet un développement dans un voisinage de l'origine de la forme $\tilde{f} = \sum_{k=-N}^{\infty} a_k q^k$ pour un certain $N \in \mathbb{Z}$.

Définition 5. *Une fonction faiblement modulaire qui est méromorphe à l'infini est appelée* ***fonction modulaire****. La "valeur" de f à l'infini est $\tilde{f}(0)$.*

1. Dans le cas $V = \mathbb{R}^n$ avec la mesure $dx = dx_1 \cdots dx_n$, c'est le volume de l'ensemble $\Pi_\Gamma = \{v = \sum_i v_i e_i, 0 \leq |v_i| < 1\}$, où (e_i) est une base de Γ, nommé "pavé fondamental".

Définition 6. *On appelle* ***forme modulaire*** *toute fonction modulaire f qui est holomorphe partout. Si de plus sa valeur à l'infini est 0, on dit que f est* ***parabolique****.*

Si Γ est un réseau et $\lambda \in \mathbb{C}^*$, on note $\lambda\Gamma$ le réseau $\{\lambda v, v \in \Gamma\}$. On identifie $\mathbb{R}^2$ à $\mathbb{C}$, de sorte que à chaque réseau de $\mathbb{R}^2$ lui correspond un réseau de $\mathbb{C}$ engendré par deux éléments $\omega_1, \omega_2 \in \mathbb{C}$ (i.e., le réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$). Enfin, on note $\mathscr{R}$ l'ensemble des réseaux de $\mathbb{C}$.

Définition 7. *Soit $F : \mathscr{R} \to \mathbb{C}$, et soit $k \in \mathbb{Z}$. On dit que F est (une fonction de réseaux) de poids $2k$ si l'on a $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$ pour tout $\Gamma \in \mathscr{R}, \lambda \in \mathbb{C}^*$.*

On a que, si Γ est le réseau engendré par (ω_1, ω_2), en posant $z = \omega_1/\omega_2$ on déduit qu'il existe une fonction f sur H telle que $F(\omega_1, \omega_2) = \omega_2^{-2k} f(\omega_1/\omega_2)$. Mieux, cette fonction est une fonction modulaire de poids $2k$ (cf. [Se], chapitre VII, proposition 3). Ainsi on fait correspondre à chaque fonction de réseaux de poids $2k$ telle que $F(z, 1)$ est méromorphe, une fonction modulaire de poids $2k$.

Définition 8 (*Séries d'Eisenstein*)**.** *Soit Γ un réseau de $\mathbb{C}$ et $k > 1$ un entier. La série*

$$G_k(\Gamma) = \sum_{\gamma \in \Gamma}{}' \gamma^{-2k}, \tag{1}$$

dite ***série d'Eisenstein****, est absolument convergente (le symbole Σ' indique que la somme ne porte que sur les éléments non nuls de Γ). Elle est évidemment une fonction de réseaux de poids $2k$, et définit une fonction faiblement modulaire, notée encore G_k, par $G_k(z) = \sum_{m,n}{}' \frac{1}{(mz+n)^{2k}}$ qui vérifie $G_k(\infty) = 2\zeta(2k)$, où ζ désigne la fonction zêta de Riemann.*

En montrant que G_k est holomorphe dans $\widetilde{\mathbb{C}}$, on conclut qu'elle est en fait une forme modulaire non parabolique de poids $2k$. Pour exhiber une forme parabolique, on pose $g_2 = 60G_2, g_3 = 140G_3$, de sorte que $g_2(\infty) = \frac{4}{3}\pi^4$ et $g_3(\infty) = \frac{8}{27}\pi^6$ et on définit

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

elle est donc une forme parabolique de poids 12.

1.4 Algèbre des formes modulaires

Ainsi définies, les formes modulaires de poids $2k$ forment un $\mathbb{C}$-espace vectoriel pour l'addition de fonctions que l'on note M_k. On note M_k^0 l'espace des formes paraboliques de poids $2k$. Comme M_k^0 est le noyau de l'application linéaire $M_k \to \mathbb{C}, g \mapsto g(\infty)$, on a $\dim(M_k)/\dim(M_k^0) \leq 1$, d'où on déduit que M_k est la somme directe de M_k^0 et $\mathbb{C}f$, où f est n'importe quel forme modulaire de poids $2k$ non parabolique, par exemple $M_k = M_k^0 \oplus \mathbb{C}G_k$,

Théorème 1. *(i) $M_k = 0$ pour $k < 0$ et $k = 1$,*

(ii) Pour $k = 0, 2, 3, 4, 5$, M_k est un espace de dimension 1 admettant pour base $1, G_2, G_3, G_4, G_5$; on a $M_k^0 = 0$.

(iii) La multiplication par Δ définit un isomorphisme de M_{k-6} sur M_k^0.

Corollaire 1. *Pour $k \geq 0$,*

$$\dim M_k = \begin{cases} \lfloor k/6 \rfloor & \text{si } k \equiv 1 \mod 6, \\ \lfloor k/6 \rfloor + 1 & \text{si } k \not\equiv 1 \mod 6. \end{cases}$$

Corollaire 2. *L'espace M_k admet pour base la famille des monômes $G_2^\alpha G_3^\beta$ avec α, β entiers ≥ 0 et $2\alpha + 3\beta = k$.*

Note : Soit f une fonction modulaire de poids $2k$, non identiquement nulle. Ce théorème ainsi que les corollaires sont conséquence directe de la formule

$$v_\infty(f) + \sum_{y \in H/G} \frac{1}{e_y} v_y(f) = \frac{k}{6},$$

où $v_y(f)$ est l'ordre de f en y (l'entier n tel que $f(z)/(z-y)$ soit holomorphe et non nul en y), et e_y est l'ordre du stabilisateur du point y [2]. Pour démontrer cette formule on intègre $\frac{1}{2i\pi} f$ sur le contour du domaine fondamental D du groupe modulaire.

1.5 Fonctions thêta

Soit V un espace vectoriel de dimension finie n muni d'une mesure invariante μ, et soit V' le dual de V. Nous supposons désormais que V est muni d'une forme bilinéaire symétrique $x \cdot y$ positive et non dégénérée (i.e. si $x \neq 0$, $x \cdot x > 0$).

Définition 9. *Si $f : V \to \mathbb{C}$ est une fonction indéfiniment différentiable à décroissance rapide sur V, on définit la* **transformée de Fourier de f**, *ce que l'on note $\mathcal{F}(f)$ est définie par la formule $\mathcal{F}(f) = \int_V e^{-2i\pi\langle x,y\rangle} f(x)\mu(x)$. Elle est indéfiniment différentiable à décroissance rapide sur V'.*

Définition 10. *Soit Γ un réseau de V. Le* ***réseau dual de Γ*** *est l'ensemble $\Gamma' = \{y \in V', \langle x, y\rangle \in \mathbb{Z}, \forall x \in \Gamma\}$.*

Dans le cas où $V = V'$ (ou même dans le cas général de dimension finie car on peut identifier V à V' au moyen de la forme bilinéaire de V), on a que si Γ est un réseau de V, alors Γ' l'est aussi : $y \in \Gamma' \Leftrightarrow x \cdot y \in \mathbb{Z} \forall x \in \Gamma$.

Proposition 4 (*Formule de Poisson*)**.** *Soit $v = \mu(V/\Gamma)$. On a* $\sum_{x\in\Gamma} f(x) = v^{-1} \sum_{y\in\Gamma'} \mathcal{F}f(y)$.

Cette formule est analogue à la formule de Poisson classique [3].

On associe à chaque réseau et chaque forme bilinéaire $x \cdot x$ une fonction définie sur $\mathbb{R}_+^*$ à valeurs dans $\mathbb{C}$:

Définition 11. *Soit Γ un réseau de V. On définit la* ***fonction thêta associée à Γ*** *par $\Theta_\Gamma : \mathbb{R}_+^* \to \mathbb{C}$, $\Theta_\Gamma(t) = \sum_{x\in\Gamma} e^{-\pi t x\cdot x}$.*

C'est facile de voir que cette somme est convergente, par exemple en la comparant avec un multiple d'une puissance de la somme $\sum_{x\in\mathbb{Z}} e^{-\pi t x^2}$. On fait correspondre à la forme $x \cdot x$ une matrice symétrique positive et non dégénérée comme suit : soit $e = \{e_1, \cdots, e_n\}$ une base de Γ. Soit $a_{ij} = e_i \cdot e_j$, alors $A = (a_{ij})$ est une telle matrice.

2. On montre que cet ordre est 1 sauf si $y \in \{i, e^{2\pi i/3}\}$, et on réécrit cette formule sous la forme $v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_{e^{2\pi i/3}}(f) + \sum^*_{y\in H/G} v_y(f) = \frac{k}{6}$, où le symbole Σ^* indique que la somme porte sur les points y n'appartenant pas aux classes de $i, e^{2i\pi/3}$.

3. Détaillons : on suppose que $\mu(V/\Gamma) = 1$ (sinon on remplace μ par $v^{-1}\mu$), on identifie $V \simeq \mathbb{R}^n$, $\Gamma \simeq \mathbb{Z}^n$, auquel cas la formule est $\sum_{\mathbb{Z}^n} f(x) = \sum_{\mathbb{Z}^n} \mathcal{F}f(y)$, c'est à dire la formule de Poisson classique.

L'intérêt de cette représentation matricielle est le suivant : si $x \in V, x = \sum_{i=1}^{n} x_i e_i$, on a $x \cdot x = \sum_{i,j} a_{ij} x_i x_j$ de sorte que

$$\Theta_\Gamma(t) = \sum_{x \in \mathbb{Z}^n} e^{-\pi t \sum a_{ij} x_i x_j}, \quad \mu(V/\Gamma) = \det(A)^{1/2}.$$

Proposition 5. *On a* $\Theta_\Gamma(t) = t^{-n/2} v^{-1} \Theta_{\Gamma'}(t^{-1})$.

Ceci est un résultat facile de la proposition 4 et du fait bien connu que $\mathcal{F}(g) = g$ pour $g = e^{-\pi(x_1^2 + \cdots + x_n^2)}$.

2 Le réseau E_8

On a introduit la plupart des outils qui seront fondamentaux pour la suite. Dorénavant on donnera preuves complètes pour les résultats.

2.1 Construction

On s'intéresse au cas $V = \mathbb{R}^8$ muni de la mesure $dx = dx_1 \cdots dx_8$. Soit $D_8 = \{(x_1, \cdots, x_8) \in \mathbb{Z}^8, \sum_i x_i \equiv 0 \mod 2\}$.

Proposition 6. *D_8 est un réseau de $\mathbb{R}^8$ de covolume 2 (c'est à dire, $\mu\left(\frac{\mathbb{R}^8}{D_8}\right) = 2$).*

Preuve : $D_8 \subset \mathbb{Z}^8$ et donc il est discret dans $\mathbb{R}^8$. Il a évidemment une structure de groupe : $0 \in D_8$ et si $x, y \in D_8$, alors $x+y \in D_8$, $-x \in D_8$. Soit $e = \{e_1, \cdots, e_8\} \subset \mathbb{Z}^8$ une base de $\mathbb{R}^8$. Alors $2e = \{2e_1, \cdots, 2e_8\} \subset D_8$ et engendre $\mathbb{R}^8$ comme $\mathbb{R}-$espace vectoriel, ce qui preuve la première assertion. Pour la deuxième, notons que D_8 est un sous-groupe d'indice 2 dans le groupe $\mathbb{Z}^8$: il est le noyau de l'application linéaire $\phi : \mathbb{Z}^8 \to \mathbb{Z}/2\mathbb{Z}, x \mapsto \sum_i x_i \mod 2$ ce qui entraîne $|\mathbb{Z}^8/D^8| = 2$. Comme $\mathrm{covol}(\mathbb{Z}^8) = \mu(\mathbb{R}^8/\mathbb{Z}^8) = 1$ est le volume du cube unitaire, on conclut d'après la proposition 1 : $\mathrm{covol}(D_8) = |\mathbb{Z}^8/D^8| \,\mathrm{covol}(\mathbb{Z}^8) = 2$. □

Ainsi, on définit le réseau E_8 comme suit : soit $e = \frac{1}{2}(1,1,1,1,1,1,1,1)$. Alors

Définition 12. *l'ensemble $\boldsymbol{E_8 = \mathbb{Z}e + D_8}$ est un réseau de $\mathbb{R}^8$ de covolume 1.*

Preuve : E_8 est discret car $2\mathbb{Z}^8 \subset 2E_8 \subset \mathbb{Z}^8$. Puisque D_8 est un réseau, il contient une base engendrant $\mathbb{R}^8$ comme $\mathbb{R}$–espace vectoriel, d'où on déduit que E_8 aussi. Une vérification simple montre que E_8 a une structure de sous-groupe, il est alors un réseau. Comme $2e \in D_8$ et $e \notin D_8$ on a que D_8 est d'indice 2 dans E_8, ce qui entraîne la deuxième assertion. □

On munit $\mathbb{R}^n$ du produit scalaire usuel.

Proposition 7. *Si $u, v \in E_8$, alors $u \cdot v \in \mathbb{Z}$ et $u \cdot u \equiv 0 \mod 2$.*

Preuve : Notons que $e \cdot e = 2$ et que si $d \in D_8$, alors $e \cdot d = \frac{1}{2}\sum_i d_i \in \mathbb{Z}$ car $\sum d_i \equiv 0 \mod 2$. En écrivant u, v comme somme des éléments en $D_8, e\mathbb{Z}$, on obtient par bilinéarité que $u \cdot v \in \mathbb{Z}$. Pour la deuxième assertion, écrivons $u = xe + d$ avec $x \in \mathbb{Z}, d \in D_8$: on a $u \cdot u = 2x^2 + 2xe \cdot d + d \cdot d \equiv 0 \mod 2$ (on a $\sum d_i^2 \equiv 0 \mod 2$ car $d_i^2 \equiv d_i \mod 2$). □

Les deux propriétés que l'on vient de vérifier sont en fait clés pour les résultats suivants. En particulier la contrainte $u \cdot u \in 2\mathbb{Z}$ fait de E_8 un *réseau pair* : les termes diagonaux de la matrice définie par une base de E_8 sont paires. Une des raisons pour lesquelles on travaille dans $\mathbb{R}^8$ est justement cette propriété.

Proposition 8. *Soit Γ un réseau **unimodulaire pair** de V (c'est à dire, Γ admet une $\mathbb{Z}$-base b avec $\det(b) = \pm 1$, et $x \cdot x \equiv 0 \mod 2$ pour tout $x \in \Gamma$). Alors la dimension de V est divisible par 8.*

Deux preuves simples se trouvent dans [Se] : chap. V, théoreme 2 et chap. VII, théorème 8. La choix de $n = 8$ est donc la plus simple.

Proposition 9. *Il y a 240 éléments de E_8 de norme 2, qui est la plus petite norme dans E_8.*

Preuve : D'abord constatons que $E_8 = \{x \in \mathbb{Z}^8 \cup (\mathbb{Z}+1/2)^8, \sum x_i \equiv 0 \mod 2\} = D_8 \cup \{x \in (\mathbb{Z}+1/2)^8, \sum x_i \equiv 0 \mod 2\}$. Soit $x \in E_8$, alors selon cette écriture il a soit tous ses coordonnées entières (il appartient à D_8) soit tous ses coordonnées demi-entières. Supposons d'abord que $x \in D_8$, et écrivons cet élément dans la base canonique de $\mathbb{R}^8$: $x = (x_1, \cdots, x_8)$. Alors $x \cdot x = \sum_{i=1}^8 x_i^2 = 2$ si et seulement si $x_i, x_j = \pm 1$ pour $i \neq j$ et 0 pour le reste. Il y a $4 \times \binom{8}{2} = 112$ choix. Si $x \notin D_8$, i.e. les coordonnées sont demi-entières, alors pour avoir une norme 2 il faut $|x_i| = 1/2$. Pour avoir $\sum_i x_i \equiv 0 \mod 2$, on ne peut choisir qu'une quantité pair de signes négatifs. On a alors $\binom{8}{0} + \binom{8}{2} + \binom{8}{4} + \binom{8}{6} + \binom{8}{8} = 2^{8-1} = 128$ choix. En résumant, si (e_i) est la base canonique de $\mathbb{R}^n$, les 240 éléments de plus petit norme sont

$$\pm e_i \pm e_j \quad (i \neq j), \qquad \sum_{i=1}^8 \varepsilon_i e_i \quad \left(\varepsilon_i \in \{\pm 1\}, \prod_{i=1}^8 \varepsilon_i = 1\right). \quad \square$$

Donnons une $\mathbb{Z}-$base de E_8. Motivés par la définition de $E_8 = \mathbb{Z}e + D_8$, il est judicieux de prendre par exemple $e_1 = e = \frac{1}{2}(1,1,1,1,1,1,1,1)$. Pour le reste des vecteurs on peut tout simplement prendre $(0,1,1,0,0,0,0,0)$, $(0,0,1,1,0,0,0,0)$, $\cdots$, $(0,0,0,0,0,0,1,1)$, $(0,0,0,0,0,0,0,2)$, formant ainsi une famille libre de 8 éléments de norme 2 de E_8. On peut changer des signes et permuter les éléments pour avoir des relations d'orthogonalité entre les éléments et une matrice triangulaire supérieure. Une vérification facile montre que en effet ceci est bien une base de E_8.

Proposition 10. *Une $\mathbb{Z}$-base pour E_8 est donnée par les colonnes de la matrice*

$$E_8 = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} \end{pmatrix}.$$

En particulier, E_8 est unimodulaire. Si $x_i \in \mathbb{Z}$, l'élément $x = (x_1, \cdots, x_8) \in E_8$ dans cette base a norme

$$x \cdot x = 2(x_1^2 + x_7 x_8 - x_1 x_2) + \sum_{\text{cyclique}} (x_i - x_{i+1})^2.$$

Note : Cette forme est bien définie positive : sa matrice associée est la matrice définie positive ${}^t E_8 E_8$ par définition.

Corollaire 3. $E_8' = E_8$.

Le corollaire s'en déduit en regardant l'action de cette base sur un élément $\in E_8' = \{y \in \mathbb{R}^8, y \cdot x \in \mathbb{Z} \forall x \in E_8\}$. [4]

Preuve de la proposition : Le fait que les colonnes forment une base pour E_8 a été déjà justifié plus haut. Ainsi, la matrice correspondante $(e_i \cdot e_j)$ est donné par

$$A = {}^t E_8 E_8 = \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 & 0 & -1 \\ -2 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

et, si $x = {}^t(x_1, \cdots, x_8)$ dans cette base on a $x \cdot x = {}^t x A x = 2(x_1^2 + \cdots + x_8^2) - 2(x_1 x_2 + x_2 x_3 + \cdots + x_7 x_8 + x_8 x_1) + 2x_1^2 + 2x_7 x_8 - 2x_1 x_2$. Alors

$$\begin{aligned} x \cdot x - 2(x_1^2 + x_7 x_8 - x_1 x_2) &= 2\sum_{i=1}^{8} x_i^2 - 2 \sum_{\text{cyclique}} x_i x_{i+1} \\ &= \sum_{\text{cyclique}} (x_i^2 + x_{i+1}^2) - \sum_{\text{cyclique}} 2x_i x_{i+1} \\ &= \sum_{\text{cyclique}} (x_i - x_{i+1})^2. \qquad \square \end{aligned}$$

On a ainsi montré que l'équation en 8 variables $2(x_1^2 + x_7 x_8 - x_1 x_2) + \sum (x_i - x_{i+1})^2 = 2$ où la somme est cyclique a 240 solutions que l'on a exhibées dans la proposition 9.

2.2 Fonction $\theta_{E_8}(z)$

Suivant le §1.5, on définit la fonction thêta associée au réseau E_8 comme $\Theta_{E_8}(t) = \sum_{x \in \Gamma} e^{-\pi t x \cdot x}$ pour $t \in \mathbb{R}_+^*$. Si on note $r_{E_8}(k) = \#\{x \in \Gamma, x \cdot x = 2k\}$ pour $k \in \mathbb{N}$, alors on voit que

$$\Theta_{E_8}(t) = \sum_{k=0}^{\infty} r_{E_8}(k) e^{-2\pi k t}.$$

4. Précisons : si $y \in \Gamma'$, alors $y \cdot e_i \in \mathbb{Z}$ pour tous les éléments de la base, donnés par la matrice E_8. En faisant le produit par la dernière colonne on voit que $e_8 \cdot y = \sum_i \frac{y_i}{2} \in \mathbb{Z} \Rightarrow \sum_i y_i \equiv 0 \mod 2$. En regardant $e_1 \cdot y = 2y_i \in \mathbb{Z}$, on voit que $y_1 \in \frac{1}{2}\mathbb{Z}$. En regardant $e_2 \cdot y = y_2 - y_1 \in \mathbb{Z}$, on trouve $(y_1, y_2) \in \mathbb{Z}^2 \cup (\mathbb{Z} + 1/2)^2$. On continue ainsi pour conclure $(y_1, \cdots, y_8) \in \mathbb{Z}^8 \cup (\mathbb{Z} + 1/2)^8$, ce qui entraîne $\Gamma' \subset \Gamma$. D'après la proposition 7 on a l'inclusion inverse.

Nous avons envie de définir une extension holomorphe de cette fonction à H pour appliquer la théorie des formes modulaires. Notons d'abord que

Proposition 11. $r_{E_8}(m) = O(m^4)$.

Preuve : Si $B(x,r)$ est la boule centré en x de rayon r pour la norme euclidienne, on a $r_{E_8}(m) \leq r_{(\frac{1}{2}\mathbb{Z})^8}(m) < |\left(\frac{1}{2}\mathbb{Z}\right)^8 \cap B(0,(2m)^{1/2})| \leq \text{covol}\left(\left(\frac{1}{2}\mathbb{Z}\right)^8\right) \cdot \mu(B(0,(2m)^{1/2})) = \frac{1}{2^8}\frac{(4\pi m)^4}{2\cdot 4\cdot 6\cdot 8} = O(m^4)$. $\square$.

On en déduit que la série entière $\sum_{k=0}^{\infty} r_{E_8}(k)q^k$ converge pour $|q| < 1$, ce qui nous amène à définir

Définition 13. $\theta_{E_8}(z) : H \to \mathbb{C},\ z \mapsto \sum_{k=0}^{\infty} r_{E_8}(k)q^k$, *(où* $q = e^{2\pi i z}$*). C'est une fonction holomorphe sur* H*. On a* $\theta_{E_8}(z) = \sum_{x\in\Gamma} e^{i\pi z x\cdot x}$ *et* $\theta_{E_8}(it) = \Theta_{E_8}(t)$.

La proposition suivante constitue un lien explicite et fondamental entre réseaux et formes modulaires. Elle est en fait un théorème pour tous les espaces vectoriels admettant un réseau unimodulaire pair, voir [Se] (chap. 5, Théorème 8).

Proposition 12. *La fonction* θ_{E_8} *est une forme modulaire de poids* 4.

Preuve : D'après la proposition 3 (caractérisation des formes faiblement modulaires), il suffit de montrer que θ_{E_8} vérifie

$$\theta_{E_8}(-1/z) = z^4\theta_{E_8}(z).$$

La formule est vraie pour $z = it \in i\mathbb{R}_+^*$: comme $\theta_{E_8}(it) = \Theta_{E_8}(t)$ c'est l'énoncé de la proposition 5 (vu que $v = 1, E_8' = E_8$). Or comme $\theta_{E_8}(-1/z), \theta_{E_8}(z)$ sont analytiques, la formule est vraie pour H tout entier, d'où on conclut. $\square$

Proposition 13. $\theta_{E_8}(z) = \frac{1}{2\zeta(4)}G_2(z)$.

Preuve : En effet, l'espace M_2 de formes modulaires de poids 4 est de dimension 1, engendré par la fonction d'Eisenstein G_2. Comme $\theta_{E_8}(\infty) = 1$ (il n'y a qu'un élément de Γ de norme 0), on conclut. $\square$

3 Une équation diophantienne

On a montré déjà que l'équation diophantienne en 8 variables

$$2(x_1^2 + x_7x_8 - x_1x_2) + \sum_{\text{cyclique}} (x_i - x_{i+1})^2 = 2$$

a 240 solutions, ce sont les éléments de norme 2 dans E_8. Soit $d \in \mathbb{N}$, considérons l'équation

$$2(x_1^2 + x_7x_8 - x_1x_2) + \sum_{\text{cyclique}} (x_i - x_{i+1})^2 = 2d. \tag{2}$$

Comme le membre de gauche est la norme associée à E_8, les solutions à cette équation sont exactement les éléments de E_8 de norme $2d$: il y en a par définition $r_{E_8}(d)$. Le nombre de solutions c'est donc le coefficient de q^d dans le développement de $\theta_{E_8}(z)$. Pour obtenir ce coefficient, il faut développer la fonction d'Eisenstein $G_2(z)$ et on a fini, en vertu de la proposition 13. On donne même un développement de $G_k(z)$ pour tout $k \geq 2$.

Proposition 14. $G_k(z) = 2\zeta(2k) + 2\dfrac{(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n, \quad$ *où* $\sigma_l(n) = \sum_{i|n} i^l$.

On aura besoin du calcul suivant

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

Preuve : En effet, on a l'identité bien connue

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

et d'une autre part,

$$\pi\operatorname{cotg}(\pi z) = i\pi\frac{q+1}{q-1} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi\sum_{k=0}^{\infty} q^k.$$

Ainsi

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

et on déduit en dérivant k fois cette formule. □

Preuve de la proposition :

$$\begin{aligned} G_k(z) &= \sum_{(n,m)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(zm+n)^{2k}} = 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}}\frac{1}{(nz+m)^{2k}} \\ &= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{j=1}^{\infty} j^{2k-1}q^{jn} = 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{i|n}^{\infty} i^{2k-1}q^n \\ &= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n. \quad \square \end{aligned}$$

Ainsi, $\dfrac{1}{2\zeta(4)}G_2(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$, d'où on voit que le nombre de solutions entières de (2) est $240\sum_{j|d} d^3$, par exemple il y a $240(1^3+2^3) = 2160$ solutions pour $d = 2$. D'ailleurs on retrouve le fait qu'il y a 240 éléments de norme 2 dans E_8. Comme le nombre de solutions est non nul pour tout d, on a en particulier que

Tout nombre positif pair est de la forme
$2(x_1^2 + x_7x_8 - x_1x_2) + \sum_{\text{cyclique}}(x_i - x_{i+1})^2$ avec $(x_1, \cdots x_8) \in \mathbb{Z}^8$.

4 Généralisations

À des rotations près, il n'y a pas d'autres réseaux dans $\mathbb{R}^8$ avec les propriétés de E_8, comme le précise le théorème suivant. Ainsi, pour généraliser ces idées à d'autres réseaux on ne peux qu'aller dans des espaces plus grands.

Théorème 2 (Mordell 1938)**.** *Soit* Γ *un réseau pair unimodulaire de* $\mathbb{R}^8$*. Alors* $L \simeq E_8$.

Il existe des nombreux démonstrations, voir [Elk] pour une démonstration originale, [Gr] pour une démonstration élémentaire ou encore [Se], Chapitre V, §2.3.

4.1 $E_8 \oplus E_8$.

Il est facile de voir que si Γ, Γ' sont des réseaux de $\mathbb{R}^m, \mathbb{R}^n$ alors $\Gamma \oplus \Gamma'$ est un réseau de $\mathbb{R}^{n+m}$. On a donc que $E_8 \oplus E_8$ est un réseau unimodulaire pair de $\mathbb{R}^{16}$, et on peut déjà avoir un énoncé similaire à celui de la section précédente. Détaillons :

1. La fonction thêta associé à $\Gamma = E_8 \oplus E_8$ est $(\theta_{E_8}(z))^2$.
2. Il s'agit d'une forme modulaire de poids 8, et comme l'espace M_4 est encore de dimension 1, on a $G_2(z)^2 = \lambda G_4(z)$ où λ est un nombre réel qui se détermine en prenant $z = \infty$.
3. On développe la fonction $G_4(z)$ selon la proposition 14.
4. On trouve ainsi $\theta_\Gamma(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n$, où $\sigma_7(n) = \sum_{k|n} k^7$.
5. Alors tout nombre pair $n = 2d$ est représenté par une certaine forme quadratique en 16 variables [5], de $480 \times \sum_{k|d} k^7$ manières.

Il y a un autre réseau dans $\mathbb{R}^{16}$, il s'agit de E_{16} (construit de façon analogue à E_8) : on vérifie ainsi que le théorème de Mordell n'est pas vrai dans $\mathbb{R}^{16}$ (en tout rigueur il faut vérifier que ces réseaux ne sont pas isomorphes...) Or, ces deux réseaux ont la même fonction thêta.

4.2 Construction de E_{8k}

La construction de E_{8k} est tout-à-fait analogue à celle de E_8.

- On prend $V = \mathbb{R}^{8k}$ avec la mesure $dx = dx_1 \cdot dx_{8k}$.
- Soit $D_{8k} = \{x_1, \cdots, x_{8k} \in \mathbb{Z}^{8k}, \sum_i x_i \equiv 0 \mod 2\}$.
- On constate que D_{8k} est un réseau de covolume 2 (même preuve que la proposition 6).
- Soit $e = \frac{1}{2}(1, 1, \cdots, 1)$, de sorte que $2e \in D_8$.
- Alors on définit $E_{8k} = D_{8k} + \mathbb{Z}e$, un réseau de $\mathbb{R}^{8k}$
- On vérifie que E_{8k} est pair : la proposition 7 est aussi vraie pour E_{8k} (avec même preuve).
- En imitant le raisonnement de la proposition 10, on a que une base pour E_{8k} est donnée par les colonnes de la matrice

$$E_{8k} = \begin{pmatrix} 2 & -1 & 0 & \cdots & 0 & -\frac{1}{2} \\ 0 & 1 & -1 & \cdots & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & \ddots & 0 & -\frac{1}{2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & \cdots & 0 & -\frac{1}{2} \end{pmatrix}.$$

En particulier, E_{8k} est unimodulaire. En regardant la matrice $(e_i, e_j) = {}^t E_8 E_8$ on voit que la norme euclidienne d'un élément $x \in E_{8k}$ écrit sur cette base $x = \sum_{i=1}^{8k} x_i e_i$ est

$$x \cdot x = 2(x_1^2 + x_{8k-1}x_{8k} - x_1 x_2) + \sum_{\text{cyclique}} (x_i - x_{i+1})^2.$$

5. D'après la proposition 10 il est facile de voir que pour le réseau $\Gamma = E_8 \oplus E_8$, la norme associée est $2(x_7x_8 - x_1x_2 + x_{15}x_{16} - x_9x_{10}) - (x_8 - x_9)^2 + \sum_{i=1}^{16}(x_i - x_{i+1})^2$ (où la somme est cyclique)

Proposition 15. *La fonction thêta de E_{8k} est une forme modulaire de poids $4k$.*

(Même preuve que pour la proposition 12).

Mentionnons enfin que la fonction thêta de E_{16} est la même que du réseau $E_8 \oplus E_8$, car l'espace de M_4 est encore de dimension 1.

4.3 Dimension $n = 24$

Pour dimension $n = 24$ le problème devient légèrement plus compliqué : si Γ est n'importe quel réseau de $\mathbb{R}^{24}$, θ_Γ est de poids 12 et la dimension de M_6 est 2 : $M_6 = \mathbb{C}\Delta \oplus \mathbb{C}G_6$. On aura donc $\theta_\Gamma(z) = \lambda_\Gamma G_6(z) + \mu_\Gamma \Delta$ pour des facteurs $\mu_\Gamma, \lambda_\Gamma \in \mathbb{C}$. Il en résulte, en prenant $z = \infty$, que $\lambda_\Gamma = 1/G_6(\infty)$ (il n'y a qu'un élément de Γ de norme 0), donc $\theta_\Gamma(z) = \frac{G_6(z)}{G_6(\infty)} + \mu_\Gamma \Delta$. On peut montrer que

$$G_6(z) = G_6(\infty)\left(1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n\right)$$

et on définit la **fonction de Ramanujan** $\tau(n)$ par la formule $\Delta = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)q^n$. Il est facile de voir, dans la définition de Δ et des précédentes expansions pour G_2, G_3 en puissances de q, que $\tau(1) = 1$. Ou mieux, dans le théorème dû à Jacobi suivant :

$$\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}.$$

(Une démonstration élémentaire se trouve dans [Se], chap. VII, §4.4).

On aura donc que les éléments de norme $2d$ pour d un nombre entier ≥ 1 dans Γ sont $\frac{65520}{691}\sigma_{11}(d) + \mu_\Gamma \tau(d)$. En prenant $d = 1$, on détermine $\mu_\Gamma = r_\gamma(1) - \frac{65520}{691}$ ($\neq 0$ car $65520/691 \notin \mathbb{Z}$).

Ceci implique un analyse de la fonction de Ramanujan et des opérateurs de Hecke (voir [Se], chap. VII, §5). Cette fonction a des propriétés de congruence remarquables. Ramanujan avait conjecturé en 1916 que $|\tau(p)| \leq 2p^{11/2}$ pour tout nombre premier p, une preuve a dû attendre jusqu'à 1974 par Deligne. En particulier, comme $\sigma_k(p) = 1 + p^k$, on voit que pour $k > 5$, le terme $\tau(p)$ est négligeable, ce qui nous donne une approximation du problème $\#\{x \in \Gamma, x \cdot x = 2p\}$ [6].

Le remarque de la section précédente sur les sommes directes de réseaux nous permet de trouver des réseaux unimodulaires pairs dans $\mathbb{R}^{24}$ (et en dimensions plus grandes) : quelques exemples sont $E_8 \oplus E_8 \oplus E_8, E_8 \oplus E_{16}, E_{24}$.

En fait, dans $\mathbb{R}^{24}$ il existe 24 réseaux unimodulaires pairs (à isométries près) appelés les "réseaux de Niemeier" (classifiés par Hans-Volker Niemeier en 1973, voir [CS]). Il y a un réseau de Niemeier qui a des certaines particularités : le réseau de Leech, construit par John Leech en 1965. Par exemple, il a la caractérisation de ne pas avoir des éléments de norme 2, c'est à dire $r_L(1) = 0$ et donc $\mu_L = -65520/691$. On peut mentionner aussi que ce réseau résoudre le *"kissing problem"* en dimension 24 :

6. Et même pour le problème $\#\{x \cdot x = 2p^m, x \in \Gamma\}$ si $m \geq 1$, car $\sigma_k(p^m) = 1 + p^{2k} + \cdots + p^{mk} = (p^{km+1} - 1)/(p^k - 1)$.

Problème : *Étant donnée une boule unitaire $B \subset \mathbb{R}^n$, combien de boules unitaires au maximum peuvent être tangentes à B sans se superposer ?*
Il est facile de voir que pour $n = 1$, la réponse est 2, pour $n = 2$ la réponse est 6 (réseau hexagonal), et difficile de prouver que en 3 dimensions [7] la réponse est 12. En fait, en dimension $n = 8$ la réponse est 240 boules arrangées comme le réseau E_8, et en dimension $n = 24$ la réponse est 196560 boules arrangées suivant le réseau de Leech.

5 Bibliographie

[Ch] Chenevier, Gaëtan, Notes du cours "Théorie Algébrique des Nombres" donné à l'École Polytechnique, automne de 2011.

[CS] Conway, J. ; Sloane, N. (1998). "Sphere Packings, Lattices, and Groups" (3rd ed.). Springer-Verlag.

[Elk] Elkies, Noam, "Yet another proof of the uniqueness of the E_8 lattice", Août 2004. `http://www.math.harvard.edu/~elkies/Misc/E8.pdf`

[Gr] Griess, Robert Jr., "Positive definite lattices of rank at most 8", Submitted to Journal of Number Theory, Mars 2003.

[Se] Serre, Jean-Pierre, "Cours d'arithmétique", Ed. Le Mathématicien, 1970.

7. Ceci est l'origine d'une discussion entre Isaac Newton et David Gregory, voir [CS]. Gregory pensait que la réponse était 13, parce que dans l'arrangement avec 12 boules il y a beaucoup de place libre : en fait deux de ces boules peuvent permuter leurs places en faisant un mouvement continue à toutes les boules sans qu'aucune ne perde le contact avec la boule centrale !