Gaëtan CHENEVIER. – Formes quadratiques sur $\mathbb{Z}$ et formes automorphes

1. Réseaux

$\mathbb{R}^n \quad (x_i)\cdot(y_i) = \sum_{i=1}^{n} x_i y_i$

$L \subset \mathbb{R}^n$ réseau pair $\forall x \in L,\ x\cdot x \in 2\mathbb{Z}$

$(x\cdot y \in \mathbb{Z}\ \forall x, y \in L$ formule de polarisation$)$

$$q_L : L \longrightarrow \mathbb{Z}$$
$$x \longmapsto \frac{x\cdot x}{2}$$

$$\{L \subset \mathbb{R}^n \text{ pair}\}/O(n,\mathbb{R}) \xrightarrow{\sim} \{\text{formes quadratiques } \mathbb{Z}^n \to \mathbb{Z} \text{ déf} > 0\}/\text{isom}$$

$q_L(x+y) - q_L(x) - q_L(y) = x\cdot y$ forme bilinéaire associée

$\underset{\underset{\text{covol}(L)^2}{\parallel}}{\text{dét}(q_L)} \in \mathbb{Z}$ déterminant $\sim$ discriminant $(-1)^{\frac{n(n-1)}{2}}\,\text{dét}(q_L)$

$\boxed{n=2}$ $\quad \{\text{réseau} \subset \mathbb{R}^2 \text{ pair dét} = D\}/SO(2,\mathbb{R})$

$$\Big\downarrow s \quad \text{(Gauss)}$$

classes d'idéaux d'un anneau d'entiers de $\mathbb{Q}(\sqrt{-D})$

Problème : classifier les réseaux de dét $= 1$

(i.e. $\mathrm{covol}(L) = 1$) réseaux unimodulaires pairs

Théorie de la réduction : nombre fini de classes d'isométrie de déterminant donnée [Borel : Introduction aux groupes arithmétiques]

$X_n = \{$ classes d'isom de réseaux unimodulaires pairs $\subset \mathbb{R}^n \}$

Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$ covol $= 1$ pas pair

$D_n = \{ (x_i) \in \mathbb{Z}^n \mid \sum_{i=1}^{n} x_i \equiv 0 \ [2] \}$ pair

mais covol $= 2$

$e = \frac{1}{2}(1, 1, \ldots 1)$ $\qquad e \cdot e = \frac{n}{4}$

$\boxed{E_n = D_n + \mathbb{Z} e}$ $\qquad e \cdot D_n \subset \mathbb{Z}$

convient $\Leftrightarrow n \equiv 0 \ (8)$

formes quadratiques qui restent non-dég mod p pour tout p

E_8

Thm (i) $X_n \neq \emptyset \Leftrightarrow n \equiv 0 \ (8)$

(ii) $X_8 = \{ E_8 \}$ (Mordell)

$X_{16} = \{ E_{16}, E_8 \oplus E_8 \}$ (Witt)

$\# X_{24} = 24$ (Niemeier)

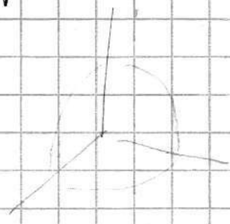
$\# X_{32} > 10^9$ $(80 \cdot 10^6)$

∃ formule explicite pour $\sum_{L \in X_n} \frac{1}{|O(L)|}$

minoration : $|O(L)| \geq 2$ (Siegel-Minkowski) - Smith

↑ formule de masse

$L \subset \mathbb{R}^n$ pair



$R(L) = \{x \in L : x \cdot x = 2\}$ racines

<u>Ex</u> : $R(D_n) = \{\pm e_i \pm e_j : i < j\}$ eng. $\mathbb{Z}$-lin. D_n

$$R(E_n) = R(D_n) \cup \{e + (x_i),\ (x_i) \in D_n,\ \sum (2x_i + 1)^2 = 8\}$$

$$= \begin{cases} R(D_n) & n > 8 \\ R(D_n) \cup \{\frac{1}{2} \underbrace{\sum \pm e_i}_{\text{nombre pair de } -}\} \end{cases}$$

<u>Cor</u> : $E_8 \oplus E_8 \not\simeq E_{16}$

réseau eng. par les racines $\quad E_8 \oplus E_8 \qquad D_{16}$

$R(L)$ <u>système de racines</u> dans $\mathrm{Vect}_{\mathbb{R}} R(L)$

2. <u>Séries thêta</u>

$L \subset \mathbb{R}^n$ pair $\quad \vartheta_L = \sum_{v \in L} q^{\frac{v \cdot v}{2}} = \sum_{n \geq 0} r_L(n) q^n$

où $r_L(n) = \#\{v \mid v\cdot v = 2n\}$

$$\vartheta_L = 1 + \#R(L)\, q + \cdots$$

<u>Thm</u> : L unimodulaire paire. Alors :

$$\vartheta_L \in M_{\frac{n}{2}}(SL(2,\mathbb{Z}))$$

$q = e^{2i\pi z}$ $\quad \mathrm{Im}(z) > 0 \Leftrightarrow |q| < 1$ $\quad$ La série converge car $r_L(n)$ pol en n

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

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

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

<u>preuve</u> : $f : \mathbb{R}^n \to \mathbb{C}$

$$x \longmapsto e^{i\pi z x\cdot x}$$

$$\vartheta_L(z) = \sum_{v \in L} f(v) \underset{\text{Poisson}}{=} \sum_{v \in L} \hat{f}(v)$$

On utilise l'hypothèse ici $L \simeq$ réseau dual

$$\hat{f}(y) = (-iz)^{-\frac{n}{4}} e^{-i\pi x\cdot x/z}$$

$$\vartheta_L(-1/z) = (-iz)^{n/2}\, \vartheta_L(z)$$

Cette astuce permet de montrer que $n \equiv 0\ [8]$

□

$M_k(SL(2,\mathbb{Z}))$ a dimension finie

$$\xi_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \Big(\sum_{d \mid n} d^{k-1} \Big) q^n \in M_k(SL(2,\mathbb{Z}))$$

$k \geq 4$

Si $k < 12$, $M_k(SL(2,\mathbb{Z})) = \mathbb{C}.\xi_k$

<u>$n=8$</u> $\quad L \subset \mathbb{R}^8$ $\quad \vartheta_L = \mathcal{E}_4 = \vartheta_{E_8}$

unim. paire

$\# R(L) = \# R(E_8) = 240$

$\xRightarrow{\text{liste de syst. de racines}}$ le seul système de racines $\subset \mathbb{R}^m$, $m \leq 8$, ayant 240 racines et pour $m = 8$, c'est E_8

$\Rightarrow$ on peut supposer $R(E_8) \subset L$

$\Rightarrow E_8 \subset L \Rightarrow E_8 = L$

$\uparrow$

$\mathrm{covol}(E_8) = \mathrm{covol}(L) = 1.$

<u>$n = 16$</u>

$\vartheta_L = \xi_8 = 1 + 480 \sum \cdots$

systèmes de racines D_{16} et $E_8 \cup E_8$

<u>$n=24$</u> $\quad M_{12}(SL(2,\mathbb{Z})) = \mathbb{C}\xi_{12} \oplus \mathbb{C}\Delta$

E_8^3, E_{24}

(cf. Boris Venkov)

réseau de Leech : 0 racines

3. Voisins de Kneser

$L, M \subset \mathbb{R}^n$ réseaux unimodulaires pairs,

p premier

L et M sont p-voisins si $L \cap M \subset L$ est

d'indice p ($\Leftarrow$ covolume p) $\Rightarrow L \cap M \subset M$ indice p

Construction de p-voisins d'un L donné

les p-voisins de $L \underset{\text{can.}}{\overset{\sim}{\rightarrow}} C_L(\mathbb{F}_p)$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$

$\qquad\qquad\qquad\qquad\qquad \{$droites isotropes de la quadrique $x \mapsto \frac{x \cdot x}{2}$ (p) sur $L/pL\}$

en effet, si $x \in L$

$\frac{x \cdot x}{2} \equiv 0 \ (p)$, on le modifie tq. $\frac{x \cdot x}{2} \equiv 0 \ (p^2)$ (Hensel)

on regarde :

$H = \{y \in L : y \cdot x = 0 \ (p)\} \Rightarrow \underbrace{\boxed{\mathbb{Z}\frac{x}{p} + H}}_{\text{unimod. paire}}$

$$|C_L(\mathbb{F}_p)| = 1 + p + p^2 + \dots + p^{n-2} + p^{-\frac{n}{2}-1}$$

<u>Problème</u> : déterminer

$N_p(L, M)$ = nombre de p-voisins de L isométriques à M

<u>Thm</u>

$$N_p(E_8 \oplus E_8, E_{16}) = \frac{405}{691} \frac{p^n - 1}{p-1} (1 + p^{11} - \tau(p))$$

où $\Delta = q \prod_{n \geq 1} (1-q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n$.

[Congruence de Ramanujan : $691 \mid 1 + p^{11} - \tau(p)$]

$\mathbb{Q}[X_n]$ $\quad T_p : \mathbb{Q}[X_n] \longrightarrow \mathbb{Q}[X_n]$

$$[L] \longmapsto \sum_{\substack{M\, p\text{-voisins} \\ \text{de } L}} [M]$$

les T_p commutent 2 à 2

$\mathbb{R}[X_n]$ produit scalaire

$$\langle [L], [M] \rangle = \delta_{L,M} |O(L)|$$

les T_p sont auto-adjoints

$$N_p(L, M) |O(M)| = N_p(M, L) |O(L)|$$

connaître les T_p $\Leftrightarrow$ connaître de vecteurs propres communs et le système des valeurs propres des T_p (λ_p) sur ces vecteurs

$$\sum_{L \in X_n} \frac{1}{|O(L)|} [L] \text{ propre pour } T_p \text{ de valeur}$$

propre $\# C_L(\mathbb{F}_p) = 1 + p + \dots + p^{n-2} + p^{\frac{n}{2}-1}$

<u>Rappel</u>

$M_k(SL(2,\mathbb{Z})) \circlearrowleft T_p$ opérateurs de Hecke

<u>Deligne</u> :

si $f = q + a_2 q^2 + a_3 q^3 + \dots \in M_k(SL(2,\mathbb{Z}))$

propre pour tous les T_p

$T_p f = a_p f$ $\quad \mathbb{Q}(a_n)$ corps de nombres

ℓ fixé $i : \mathbb{Q}(a_n) \longrightarrow \overline{\mathbb{Q}_\ell}$

Il existe $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\overline{\mathbb{Q}_\ell})$

non-ramifiée hors de ℓ,

$$\det(X - \rho_f(\mathrm{Frob}_p)) = X^2 - a_p X + p^{k-1} \quad p \neq \ell$$

système compatible de ℓ-représentations

Thm*. Soit ℓ premier. Soit (λ_p) un système de valeurs propres des T_p sur $\overline{\mathbb{Q}}_\ell[X_n]$.

$\exists\ \rho_\pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(n, \overline{\mathbb{Q}}_\ell)$

non-ramifiée hors de ℓ

$$\mathrm{tr}\,(\rho_\pi(\mathrm{Frob}_p)) = \lambda_p \quad p \neq \ell$$

Cette propriété caractérise (à semi-simplicité près) la représentation par le théorème de Chebotarev.

Retour à $n = 16$

$\mathbb{Q}_\ell[X_{16}]$ dim 2

vecteur propre trivial e

soit f l'autre vecteur propre des T_p

Thm 1 $\iff$ $\rho_e = 1 + \omega + \omega^2 + \dots + \omega^{14} + \omega^7$

$$\rho_f = \rho_{\Delta,\ell} \otimes (1 + \omega + \omega^2 + \omega^3) \otimes \omega^4 \otimes (1 + \dots + \omega^6 + \omega^3)$$

$\rho_\pi(\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell))$ nombres de Hodge

$$0, 1, 2, 3, \dots n-2, \frac{n}{2} - 1$$

lim ave $H^i_{cusp}(SL(n, \mathbb{Z}), \mathbb{Q})$