Exposé au séminaire *des mathématiques* de l'É.N.S. Paris, 4 Mars 2020

RÉSEAUX UNIMODULAIRES PAIRS

GAËTAN CHENEVIER

1. Un point de départ : formes quadratiques entières

On fixe $n \geq 1$ et on considère

$$\mathrm{S}_n = \{M \in \mathrm{M}_n(\mathbb{Z}) \mid {}^tM = M,\ M \text{ def.pos. et } m_{ii} \equiv 0 \bmod 2,\ 1 \leq i \leq n\}.$$

Pour M dans S_n et $x \in \mathbb{Z}^n$ (vecteur colonne), on a

$$\mathrm{q}_M(x) := \frac{1}{2}\,{}^txMx = \frac{1}{2}\sum_{1\leq i,j\leq n} m_{ij}x_ix_j = \sum_{i=1}^{n}\frac{m_{ii}}{2}\,x_i^2 + \sum_{1\leq i<j\leq n} m_{ij}\,x_ix_i.$$

C'est une forme quadratique *entière*, c'est-à-dire un polynôme $\mathbb{Z}^n \to \mathbb{Z}$ homogène de degré 2. Clairement, $M \mapsto \mathrm{q}_M$ est une bijection entre S_n est l'ensemble des formes quadratiques entières, définies positives sur $\mathbb{R}^n$.

Problème de classification : classifier les formes quadratiques entières à changement de variables inversible – ou *équivalence* – près. Concrètement, le groupe $\mathrm{GL}_n(\mathbb{Z})$ agit sur S_n via $(P, M) \mapsto PM{}^tP$, et on s'intéresse au quotient $\mathrm{GL}_n(\mathbb{Z})\backslash S_n$.

La question a une riche histoire : Lagrange, Gauss, Hermite, Minkowski, Hasse, Siegel... Motivation initiale principale : déterminer les valeurs prises ("représentées") par une forme. Il serait pédagogique de commencer par exposer leurs résultats, mais je souhaite partir dans une autre direction alors je ne vais rappeler qu'un résultat essentiel : la finitude du nombre de classes. Pour $d \geq 1$ entier on pose $\mathrm{S}_n(d) = \{M \in \mathrm{S}_n,\ \det M = d\}$, il est stable sous l'action de $\mathrm{GL}_n(\mathbb{Z})$ (justifier !).

Théorème : $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{S}_n(d)$ est fini pour tout $n, d \geq 1$.

Exemple : $(n = 2)$ On a $\det\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = 4ac - b^2$, donc $d = 0, -1 \bmod 4$. Gauss a montré que $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{S}_2(d)$ est le défaut de principalité de l'anneau $\mathbb{Z}[\sqrt{-d/4}]$ ou $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$, pour $d > 0$. Par exemple, $\mathbb{Z}[i]$ principal $\Leftrightarrow$ $x^2 + y^2$ seule forme de déterminant 4 à équivalence près.

But de l'exposé : au lieu de fixer n petit comme chez Lagrange ou Gauss, et de faire varier d, on prend $d = 1$ (le plus petit possible) et on fait varier n. On pose

$$\mathrm{X}_n = \mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{S}_n(1).$$

Une motivation : pour M dans S_n, la forme bilinéaire symétrique $\mathrm{b}_M(x, y) = {}^txMy$ sur $\mathbb{Z}^n$ définit par réduction mod p premier une forme bil. sym. sur $(\mathbb{Z}/p\mathbb{Z})^n$, de déterminant (ou "discriminant") $\det M \bmod p$. Ainsi, $\det M = 1$ ssi b_M est non dégénérée mod p pour tout premier p. *Ce sont donc les formes quadratiques entières les moins dégénérées qui soient : on parle aussi de formes quadratiques "sur $\mathbb{Z}$".* Mon but est d'expliquer quelques résultats connus sur X_n.

Fait : X_n est non vide ssi $n \equiv 0 \bmod 8$ (explication de $\Rightarrow$?).

Nous expliquerons $\mathrm{X}_{8k} \neq \emptyset$ plus loin. Pour construire des éléments intéressants de S_n, il est beaucoup plus agréable d'utiliser un troisième point de vue : celui des réseaux euclidiens. On part de l'espace euclidien $E = \mathbb{R}^n$ standard, de produit scalaire $(x_i) \cdot (y_i) = \sum_i x_i y_i$. Un réseau de E est un sous-groupe $L \subset E$ engendré par une base $e_1, \ldots, e_n$ de l'espace E :

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n.$$

L'exemple typique est $L = \mathbb{Z}^n$. Tout réseau est de la forme $L = g(\mathbb{Z}^n)$ avec $g \in \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$. Le covolume de L est le réel $|\det g|$ (bien défini !) : c'est le volume d'un domaine fondamental de L. Quand $\operatorname{covol} L = 1$ on dit que L est unimodulaire.

Le réseau $L \subset E$ est dit *pair* si on a $x.x \in 2\mathbb{Z}$ pour tout $x \in L$. En particulier, on a $x.y \in \mathbb{Z}$ pour tout $x, y \in L$, i.e. L est *entier*. On note $\mathcal{P}_n$ l'ensemble des réseaux pairs de $\mathbb{R}^n$. Si L est pair, alors on construit une forme quadratique sur $L \simeq \mathbb{Z}^n$ en posant $\mathrm{q}_L(x) = \frac{x.x}{2}$. Concrètement, si $L = g(\mathbb{Z}^n)$ alors $\mathrm{q}_L \circ g = \mathrm{q}_M$ avec $M = {}^t g\, g$. La classe de q_L dans $\mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{S}_n$ est bien définie, et $L \mapsto \mathrm{q}_L$ induit une bijection

$$\mathrm{O}(\mathbb{R}^n)\backslash \mathcal{P}_n \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{S}_n.$$

(Explications !) Dans cette bijection, on a donc $\det \mathrm{q}_L = (\operatorname{covol} L)^2$.

Corollaire : X_n est aussi l'ensemble des classes d'isométrie de r. u. p. de $\mathbb{R}^n$.

2. Un exemple : le réseau E_n

On part du réseau euclidien $\mathrm{D}_n = \{(x_i) \in \mathbb{Z}^n, \sum_i x_i \equiv 0 \bmod 2\}$. C'est un sous-réseau d'indice 2 de $\mathbb{Z}^n$, donc de covolume 2. Il est manifestement entier, et même pair : c'est le plus grand sous-réseau pair de $\mathbb{Z}^n$. On pose $e = \frac{1}{2}\sum_i \epsilon_i$ et

$$\mathrm{E}_n = \mathrm{D}_n + \mathbb{Z}e.$$

Fait : E_n est unimodulaire pair $\Leftrightarrow$ $n \equiv 0 \bmod 8$.

Preuve : On a $e.\mathrm{D}_n \subset \mathbb{Z}$ et $e.e = n/4$. Donc E_n est pair ssi $n \equiv 0 \bmod 8$. Enfin, pour n pair D_n est d'indice 2 dans E_n, donc $\operatorname{covol} \mathrm{E}_n = 1$.

Remarque : Pour n pair, $\mathrm{E}_n \setminus \mathrm{D}_n$ est l'ens. des $\frac{1}{2}(x_1, \ldots, x_n)$ avec les x_i impairs, un nombre pair étant $\equiv -1 \bmod 4$.

E_8 est un réseau exceptionnellement symétrique. Son nom vient du lien avec la théorie des systèmes de racines. Qu'est-ce qu'une racine ?

Racines : Pour $L \in \mathcal{P}_n$, on pose $\mathrm{R}(L) = \{\alpha \in L \,|\, \alpha \cdot \alpha = 2\}$. Exemples : $\mathrm{R}(\mathrm{D}_n) = \{\pm\epsilon_i \pm \epsilon_j, i \neq j\}$, $\mathrm{R}(\mathrm{E}_n) = \mathrm{R}(\mathrm{D}_n)$ pour $n > 8$, et pour $n = 8$ il faut rajouter les 2^7 éléments $\frac{1}{2}(\sum_i \pm\epsilon_i)$. En particulier, E_8 a $4\binom{8}{2} + 2^7 = 112 + 128 = 240$ racines. Pour chaque racine $\alpha \in \mathrm{R}(L)$, la symétrie orthogonale

$$\mathrm{s}_\alpha(x) = x - (\alpha.x)\,\alpha$$

est un élément du groupe d'isométries $\mathrm{O}(L)$ de L. C'est une explication du fait que E_8 est exceptionnellement symétrique : cela permet de montrer

$$|\mathrm{O}(\mathrm{E}_8)| = 8! \cdot 2^7 \cdot 135 = 696\,729\,600$$

c'est la taille maximale d'un sous-groupe fini de $\mathrm{GL}_8(\mathbb{Z})$ (c'est 135/2 fois le $2^n n!$ évident : un record). À quoi ressemble la forme quadratique E_8 ? On constate que

$$\epsilon_2-\epsilon_3, \epsilon_3-\epsilon_4, \epsilon_4-\epsilon_5, \epsilon_5-\epsilon_6, \epsilon_6-\epsilon_7, \epsilon_7-\epsilon_8, \epsilon_7+\epsilon_8, \frac{1}{2}(\epsilon_1-\epsilon_2-\epsilon_3-\epsilon_4-\epsilon_5-\epsilon_6-\epsilon_7+\epsilon_8)$$

est une $\mathbb{Z}$-base de E_8 constituée de racines (dictée par la théorie des systèmes de racines !). On retrouve le diagramme de Dynkin de type $\mathbf{E}_8$. Enfin, si on note $e_1, \dots, e_8$ cette base et si on pose $x = \sum_i x_i e_i$, on a

$$\mathrm{q}_{\mathrm{E}_8}(x) = \frac{x.x}{2} = \sum_{i=1}^{8} x_i^2 - x_1x_2 - x_2x_3 - x_3x_4 - x_4x_5 - x_5x_6 - x_5x_7 - x_7x_8,$$

c'est le premier exemple de forme quadratique sur $\mathbb{Z}$! En fait, c'est la seule en dimension 8, à équivalence près.

Dimension 16 : La construction précédente fournit au moins deux exemples, à savoir $\mathrm{E}_8 \oplus \mathrm{E}_8$ (somme orthogonale) et E_{16}. Sont-ils isométriques ? Non : les systèmes de racines ne sont pas isométriques, car l'un est "connexe" (on dit irréductible) et pas l'autre ! Explications. En revanche, on peut montrer qu'ils représentent chaque entier exactement le même nombre de fois ! (par exemple, elles ont toutes les deux 480 racines). C'est la clé des tores plats isospectraux de dimension 16 construits par Milnor.

Dimension 24 : Au moins trois exemples non isomorphes : E_{24}, $\mathrm{E}_{16} \oplus \mathrm{E}_8$ et E_8^3. On est en fait loin du compte ! L'état de l'art :

Théorème : On a $\mathrm{X}_8 = \{\mathrm{E}_8\}$ (Mordell), $\mathrm{X}_{16} = \{\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8\}$ (Witt), $|\mathrm{X}_{24}| = 24$ et ... $|\mathrm{X}_{32}| \geq 10^9$! (King)

Dans la dernière partie, je vais donner une indication pour la preuve de ce théorème pour $n \leq 24$ qui utilise des idées dues à Kneser.

3. La méthode des voisinages, suivant Kneser

On fixe L un r.u.p. dans $\mathbb{R}^n$ et p un nombre premier. On regarde L/pL : c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel muni d'une forme quadratique non dégénérée par réduction de $x \mapsto \frac{x.x}{2} \bmod p$. Cette forme est équivalente à $x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$. Elle a toujours des droites isotropes : un petit exercice montre qu'elle en a exactement

$$\mathrm{c}_n(p) = 1 + p + p^2 + \dots + p^{n-2} + p^{n/2-1}.$$

Kneser fait la construction suivante. Soit $\ell \subset L/pL$ une droite isotrope. On choisit $x \in L$ engendrant ℓ et tel que $\frac{x.x}{2} \equiv 0 \bmod p^2$. On pose

$$M = \{v \in L,\ v \cdot x \equiv 0 \bmod p\},$$

un sous-réseau d'indice p de L contenant x, et on pose

$$\mathrm{vois}_p(L, \ell) \ = \ M \ + \ \mathbb{Z}\,\frac{x}{p}.$$

Fait : $\mathrm{vois}_p(L, \ell)$ est encore un réseau unimodulaire pair, qui ne dépend que de ℓ, i.e. pas du choix de x engendrant $\ell \bmod p$.

On a donc un procédé pour fabriquer des quantités de réseaux unimodulaires pairs à partir d'un seul, et du choix d'un nombre premier. Cette construction a des applications frappantes.

Exemple : le réseau de Leech. On part de E_{24} et on regarde l'élément $\rho = (0, 1, 2, 3, \ldots, 23)$. Il est dans D_{24}, donc dans E_{24}. On a $\frac{1}{2}\rho\cdot\rho = 46\cdot 47$. On peut donc fabriquer un 47-voisin à l'aide de la droite isotrope engendrée par ρ dans $\mathrm{E}_{24}\otimes\mathbb{Z}/47$. C'est le réseau de Leech !

$$\text{Leech} = \mathrm{vois}_{47}(\mathrm{E}_{24}, \rho).$$

Je n'écrirai pas la forme quadratique associée... Il n'est pas difficile de voir qu'il n'a pas de racines : par exemple, aucune des racines $\pm\epsilon_i \pm \epsilon_j$ de E_{24} n'est dans Leech, car elle serait dans $M = \mathrm{E}_{24} \cap \text{Leech}$ et toutes les coordonnées x_i de ρ vérifient $x_i \neq \pm x_j \bmod 47$ pour $i \neq j$ par définition. Le groupe "de Conway" $\mathrm{O}(\text{Leech})/\{\pm 1\}$ est l'un des plus gros groupes simples sporadiques finis.

Le théorème d'approximation forte de Kneser admet la conséquence suivante.

Théorème : (Kneser) Fixons $n \equiv 0 \bmod 8$ et p premier. Soit $\mathrm{X}_n(p)$ le graphe ayant pour ensemble de sommets X_n, et où $[L]$ et $[L']$ sont reliés ssi L admet un p-voisin isométrique à L'. Alors $\mathrm{X}_n(p)$ est connexe.

Ainsi, on peut théoriquement construire tout X_n à partir de E_n et de ... $p = 2$. Cela conduit très vite à une preuve du théorème de classification pour $n = 8$ et 16 (on profite des symmétries). C'est aussi comme cela que Niemeier a déterminé X_{24}. Très calculatoire ! Pourtant le résultat final est un des joyaux des mathématiques. Le réseau de Leech et l'unique sans racine, et il se trouve que les 23 autres réseaux de Niemeier ont, à l'inverse, beaucoup de racines : elles engendrent $\mathbb{R}^{24}$ comme $\mathbb{R}$-ev. Leur construction est encore mal comprise, est très délicate : basée sur une quantité impressionnantes de coincidences en géométrie finie.