Séminaire BOURBAKI Juin 2004
56e année, 2003-2004, nO 935, p. 267 à 299

PARAMÉTRISATION DE STRUCTURES ALGÉBRIQUES ET DENSITÉ DE DISCRIMINANTS
[d'après Bhargava]

par **Karim BELABAS**

Gauss publie ses *Disquisitiones Arithmeticae* en 1801. La moitié du traité est consacrée aux formes quadratiques binaires $f(x,y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, notées (a,b,c), de discriminant $D = b^2 - 4ac$ [(1)]. Intéressé par les valeurs représentées par ces formes, c'est-à-dire par $\{f(x,y)\colon x, y \in \mathbb{Z}\}$, Gauss constate que l'action du groupe linéaire $\mathrm{SL}_2(\mathbb{Z})$ par changement de variables

$$(\gamma \cdot f)(x,y) = f((x,y)\gamma), \tag{1}$$

permet de ranger les formes en classes, les formes d'une orbite représentant les mêmes entiers. Le discriminant est constant sur une orbite et le nombre d'orbites de discriminant fixé est fini. Enfin,

« *sujet très important et dont personne ne s'est encore occupé* » [§ 234],

il munit les orbites primitives, telles que $\mathrm{pgcd}(a,b,c) = 1$, d'une structure de groupe, compatible avec les valeurs représentées. L'idée est de généraliser l'identité de Brahmagupta

$$(x^2 + Dy^2)(z^2 + Dt^2) = X^2 + DY^2, \quad \text{pour } X = xz + Dyt,\ Y = xt - yz,$$

qu'on n'expliquait pas encore par la multiplicativité de la norme dans $\mathbb{Z}[\sqrt{D}]$. Gauss écrit en complète généralité

$$(a_1x^2 + b_1xy + c_1y^2)(a_2z^2 + b_2zt + c_2t^2) = AX^2 + BXY + CY^2$$

dans $\mathbb{Z}[x,y,z,t]$, où X et Y sont des fonctions linéaires de (xz, xt, yz, yt) données par une transformation primitive (les mineurs maximaux de la matrice 2×4 associée sont premiers entre eux) et où tous les coefficients sont indéterminés et entiers. Puis il résout tranquillement le système. Il découvre ainsi toutes les lois de composition possibles :

(1) Gauss considère les formes dont la forme polaire bilinéaire est à *valeurs* entières, et le coefficient de xy est toujours pair. Il utilise donc le symbole (a,b,c) là où nous écrivons $(a,2b,c)$ et définit son discriminant par $b^2 - ac$. Nous traduisons dans les notations modernes.

il n'y en a essentiellement qu'une[(2)], qui s'exprime plus agréablement pour les formes primitives de même discriminant. Voici la formulation qu'en donne Dirichlet[(3)] : pour deux formes primitives de discriminant $D \neq 0$, vérifiant $a_1 a_2 \neq 0$, on pose

$$(a_1, b_1, *) \times (a_2, b_2, *) = (A, B, *), \tag{2}$$

où $n = \operatorname{pgcd}(a_1, a_2, (b_1 + b_2)/2)$, $A = a_1 a_2 / n^2$, B est solution du système de congruences

$$\begin{aligned} B &\equiv b_1 \pmod{2a_1/n} \\ B &\equiv b_2 \pmod{2a_2/n} \\ B^2 &\equiv D \pmod{4a_1 a_2/n}, \end{aligned}$$

et le troisième coefficient, déterminé par les deux premiers et le discriminant, est omis. Consciencieux, Gauss vérifie que l'opération passe au quotient et qu'elle est associative. En langage moderne, il définit la multiplication des idéaux dans un anneau quadratique S et identifie le groupe des classes de S-idéaux projectifs (*i.e.* inversibles). Cette caractérisation est toujours algorithmiquement utile et permet d'autre part d'estimer de nombreuses densités liées à ces groupes de classes quand le discriminant varie.

Dans sa thèse, Bhargava entreprend une vaste recherche de « lois de composition » arithmétiques, guidé par une série d'heuristiques et la classification des espaces vectoriels préhomogènes (voir § 3). Il considère un groupe algébrique G, une représentation naturelle V, choisis tels que l'action de $G_{\mathbb{Z}}$ sur $V_{\mathbb{Z}}$ n'ait qu'un seul invariant, baptisé discriminant, puis montre que les orbites $V_{\mathbb{Z}}/G_{\mathbb{Z}}$ paramètrent les paires $(R, *)$, où R est une classe d'isomorphisme d'anneaux de nombres de petit degré (voir § 1.1) et $*$ désigne des structures supplémentaires, en général des R-modules. Ce sont les structures algébriques du titre de l'exposé. Le discriminant usuel de R coïncide avec celui de l'orbite de $V_{\mathbb{Z}}/G_{\mathbb{Z}}$ associée. Bhargava obtient une dizaine de tels exemples, très explicites, et d'autres encore conjecturaux.

D'une part, il munit un sous-ensemble « projectif » de $V_{\mathbb{Z}}/G_{\mathbb{Z}}$ d'une loi de groupe intrinsèque et élégante, qui se réinterprète en termes du groupe des classes $\mathrm{Cl}(R)$. D'autre part, il peut énumérer les orbites par discriminant croissant, algorithmiquement ou asymptotiquement quand le discriminant tend vers l'infini. En particulier, en oubliant les structures $*$ et en se restreignant aux anneaux R intègres maximaux, Bhargava obtient de nouveaux résultats sur les densités de discriminants de corps de nombres quartiques et quintiques. Il convient toutefois de rester prudent pour cette dernière application : seul le cas des corps quartiques totalement réels est complètement rédigé à ce jour. Ces résultats restent mystérieux : la vision est unifiée et

(2) Gauss exclut les formes de discriminant nul et impose une transformation primitive, ainsi qu'un choix de signe (distinguant ainsi composition directe et indirecte).
(3) Pour l'essentiel. Dirichlet-Dedekind se restreint au cas $n = 1$ des formes « unifiées » [35, Supp. X].

élégante, mais chaque démonstration est unique quoique suivant un motif commun dans l'esprit de la théorie des invariants classique, et laisse une part décisive au calcul formel explicite. Tout comme la démonstration de Gauss.

Après quelques définitions, nous détaillons sur l'exemple de Gauss la technique de comptage employée par Bhargava en dimension supérieure. Nous décrivons ensuite les techniques alternatives utilisant les fonctions zêta de Sato-Shintani, plus générales mais aussi plus sophistiquées, qui fournissent de nombreux résultats de densités, en particulier pour les discriminants des corps quadratiques et cubiques sur une base arbitraire, et proposent un vaste programme susceptible d'aboutir à d'autres résultats de ce type, mais sans être pour l'instant en mesure de fournir les résultats annoncés par Bhargava sur $\mathbb{Q}$. Elles inspirent néanmoins ses paramétrisations et lois de composition que nous présentons ensuite. Nous énonçons finalement les résultats de densité obtenus ainsi que les conjectures qu'ils corroborent.

Je voudrais remercier A. Chambert-Loir, H. Cohen, O. Gabber, H. Gangl, J. Klüners, B. Perrin-Riou et J.-P. Serre pour leurs suggestions.

1. DÉFINITIONS

1.1. Anneaux de nombres

On appelle *anneau de nombres de degré* n un anneau R (commutatif, associatif, unitaire) qui est un $\mathbb{Z}$-module libre de rang n. On dit que R est un *ordre* s'il est intègre, auquel cas son corps des fractions est un corps de nombres. Dans cet exposé, $2 \leqslant n \leqslant 5$; conformément à une respectable tradition, nous parlerons d'anneaux quadratiques, cubiques, quartiques et quintiques pour $n = 2, 3, 4, 5$ respectivement. La trace $\mathrm{Tr} : R \to \mathbb{Z}$ assigne à $\alpha \in R$ la trace de la multiplication par α. Elle permet de définir le *discriminant* $\mathrm{Disc}(R)$ comme $\det(\mathrm{Tr}(\alpha_i\alpha_j))$, où $(\alpha_i)_{1\leqslant i\leqslant n}$ est une $\mathbb{Z}$-base arbitraire de R. C'est un entier relatif congru à 0 ou 1 modulo 4.

Un anneau de nombres est dit maximal s'il n'est pas strictement inclus dans un anneau de même degré. En particulier un ordre maximal est l'anneau des entiers de son corps des fractions, *i.e.* il est intégralement clos. La maximalité est une propriété locale qui se voit sur les $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

1.2. Anneaux quadratiques

Soit $D \equiv 0, 1 \pmod 4$ un entier relatif. À isomorphisme près, il existe un unique anneau quadratique de discriminant D, à savoir $S(D) := \mathbb{Z}[X]/(X^2 - DX + (D^2 - D)/4)$. Une *orientation* sur $S = S(D)$ est un choix d'isomorphisme $\pi : S/\mathbb{Z} \to \mathbb{Z}$, ce qui revient à choisir une racine carrée de D, ou encore une $\mathbb{Z}$-base $\alpha \wedge \beta$ de $\Lambda^2 S \simeq \mathbb{Z}$. Une base $\langle x, y\rangle$ d'un sous-module de rang 2 de l'algèbre $K = S \otimes_{\mathbb{Z}} \mathbb{Q}$ est *orientée positivement* si et seulement si $x \wedge y = c \cdot \alpha \wedge \beta$, avec $c > 0$.

Un anneau quadratique orienté n'ayant pas d'automorphismes non triviaux, deux tels anneaux de même discriminant sont canoniquement isomorphes. Ainsi, l'ensemble des entiers $D \equiv 0, 1 \pmod 4$ paramètre les classes d'isomorphismes d'anneaux quadratiques orientés. Un *idéal orienté* de S est un couple (I, ε), où $I \subset K$ est un idéal fractionnaire de S et $\varepsilon \in \{\pm 1\}$. (Alternativement, on peut définir (I, ε) par une $\mathbb{Z}$-base de I d'orientation donnée par le signe de ε.) La norme d'un idéal orienté (I, ε) est $\varepsilon\,|L/S|\,/\,|L/I| \in \mathbb{Z}$, où L est un sous-$\mathbb{Z}$-module de rang 2 de K arbitraire contenant S et I.

Les idéaux orientés forment un monoïde pour la multiplication composante par composante et tout $\kappa \in K^*$ définit un idéal orienté principal $((\kappa), \operatorname{sgn}(N_{K/\mathbb{Q}}\kappa))$. Les idéaux orientés inversibles forment un groupe, dont les idéaux principaux inversibles forment un sous-groupe. Le quotient, noté $\mathrm{Cl}(D)^+$, est le *groupe des classes orientées*, de discriminant D. Si $D > 0$, c'est le groupe des classes au sens restreint. Si $D < 0$, $\mathrm{Cl}^+(D) = \{\pm 1\} \times \mathrm{Cl}(D)$, où $\mathrm{Cl}(D)$ est le groupe des classes usuel.

1.3. Formes

Une forme k-ique n-aire est un polynôme homogène de degré k en n variables ou, par abus de langage, le polynôme nul. Par exemple, une forme quadratique binaire est un polynôme $f(x, y) = ax^2 + bxy + cy^2$, pour certains coefficients a, b, c, éventuellement tous nuls. On notera $(a_0, a_1, \ldots, a_n)$ la forme binaire $\sum_i a_i x^{n-i} y^i$ de degré n, quand le contexte ne portera pas à confusion. On note $\mathrm{Sym}^k \mathbb{Z}^n$ l'ensemble des formes $f : \mathbb{Z}^n \to \mathbb{Z}$ satisfaisant $f(x) = F(x, \ldots, x)$ pour une forme polaire F k-linéaire symétrique de $(\mathbb{Z}^n)^k \to \mathbb{Z}$, et $(\mathrm{Sym}^k \mathbb{Z}^n)^*$ l'ensemble des formes k-iques n-aires. Par exemple $(\mathrm{Sym}^2 \mathbb{Z}^2)^*$ est l'ensemble des f comme ci-dessus, avec $(a, b, c) \in \mathbb{Z}^3$. On a $f \in \mathrm{Sym}^2 \mathbb{Z}^2$ si et seulement si b est pair ; plus généralement, les monômes de $\mathrm{Sym}^n \mathbb{Z}^k$ sont pondérés de coefficients multinomiaux. Finalement, soit $\Lambda^k \mathbb{Z}^n$ l'espace des fonctions multilinéaires $(\mathbb{Z}^n)^k \to \mathbb{Z}$ alternées.

2. DOMAINES FONDAMENTAUX : UN EXEMPLE CLASSIQUE

2.1. Paramétrisation

Le prototype des résultats que l'on veut obtenir remonte à Gauss, au langage près.

THÉORÈME 2.1. — *Il existe une bijection canonique entre les deux ensembles suivants* :

– *les classes d'isomorphismes de paires (S, I), où S est un anneau quadratique orienté de discriminant non nul, et I une classe d'idéaux orientés de S,*

– *les classes de formes quadratiques binaires entières, modulo l'action de* $\mathrm{SL}_2(\mathbb{Z})$.

Cette bijection préserve le discriminant et associe une classe de formes quadratiques primitives à une classe de S-idéaux inversibles. Muni de la composition des formes quadratiques, l'ensemble des classes de formes primitives de discriminant $D \neq 0$ est un groupe, isomorphe au groupe des classes orientées $\mathrm{Cl}^+(D)$.

Dans ce théorème, les formes quadratiques entières sont les $(a,b,c) \in (\mathrm{Sym}^2 \mathbb{Z}^2)^* =: V_{\mathbb{Z}}$, une forme est primitive si le pgcd de ses coefficients est 1, et l'action (à droite) de SL_2 est donnée par le changement de variable $(g \cdot F)(x,y) = F((x,y)g)$. Le discriminant $\mathrm{Disc}(F) = b^2 - 4ac$ est un invariant de cette action, et il engendre l'algèbre des invariants sur $\mathbb{C}$. Par abus de langage, on dira que l'action a un unique invariant.

2.2. Domaine fondamental

Les orbites sous $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ ont donc une signification arithmétique et les représentants des classes sont les points entiers $V_{\mathbb{Z}}$ de l'espace affine $V = \mathbb{A}^3$, et non pas un ensemble « mince », comme une sous-variété de codimension $\geqslant 1$ par exemple. Cette représentation s'utilise algorithmiquement pour calculer ou manipuler concrètement le groupe des classes d'idéaux de corps quadratiques, dans les méthodes développées par Shanks [48] après Gauss (voir [8, 10] pour les détails algorithmiques), mais elle permet aussi de démontrer des résultats de densité, par exemple

THÉORÈME 2.2 (Lipschitz [36], conjecturé par Gauss). — *Quand $X \to +\infty$, on a*

$$\sum_{0<-D<X} |V_{\mathbb{Z}}/\Gamma| \sim \frac{\pi}{9} X^{3/2}.$$

(On peut être plus précis, voir [9].) Le principe est simple : on identifie les orbites de discriminant inférieur à X aux points à coordonnées entières du domaine fondamental de Gauss, dont l'adhérence est $C_X \cup (-C_X)$ où

$$C_X = \left\{(a,b,c) \in \mathbb{R}^3 \colon |b| \leqslant a \leqslant c, 4ac - b^2 \leqslant X\right\},$$

et qui s'obtient en imposant qu'une racine de $ax^2 + bx + c = 0$ soit dans le domaine fondamental standard de l'action de Γ sur le demi-plan supérieur. Leur nombre est approché par le volume de C_X.

THÉORÈME 2.3 (« principe de Lipschitz », Davenport [20]). — *Soit $C \subset \mathbb{R}^n$ un ensemble semi-algébrique compact, de volume* $\mathrm{Vol}(C)$, *et soit $N(C) = |C \cap \mathbb{Z}^n|$. On note $R(C)$ le maximum des volumes des projections de C sur les variétés linéaires d'équations $\{x_i = 0, i \in I\}$, où I parcourt les sous-ensembles non-vides de $\{1,\dots,n\}$. Alors*

$$N(C) = \mathrm{Vol}(C) + O(1 + R(C)).$$

La constante implicite est effective et ne dépend que de la dimension n, du nombre et du degré des équations définissant C.