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.

Nous avons négligé deux points techniques : d'abord les stabilisateurs

$$\Gamma_x := \{\gamma \in \Gamma, \gamma x = x\}$$

ont pour cardinaux 1, 2, 4, ou 6. Comme dans toute formule de masse, il serait plus habile de compter une classe x avec poids $1/|\Gamma_x|$ plutôt que d'exclure arbitrairement certains points du bord du domaine fondamental. Ici ces derniers sont peu nombreux et absorbés dans le terme d'erreur. Ensuite, nous n'avons pas à séparer le bon grain de l'ivraie : il n'y a pas de points de discriminant nul dans l'intérieur de C_X et, dans le cas de discriminants négatifs, il n'y a pas non plus lieu d'isoler les anneaux isomorphes à $\mathbb{Z}^2$, dont le discriminant est un carré parfait.

2.3. Densités locales et crible

Si on se restreint aux classes primitives, la formule d'inversion de Moebius donne :

Corollaire 2.4. — *Quand $X \to +\infty$, on a*

$$\sum_{0<-D<X} \left|\mathrm{Cl}^+(D)\right| \sim \frac{\pi}{9\zeta(3)} X^{3/2}, \quad \textit{soit} \quad \sum_{0<-D<X} |\mathrm{Cl}(D)| \sim \frac{\pi}{18\zeta(3)} X^{3/2}.$$

La condition imposée est de nature locale (une condition p-adique pour chaque premier p), se traduisant par l'apparition du facteur eulérien $\prod(1-p^{-3}) = 1/\zeta(3)$, et admet un grand nombre de variantes naturelles. On peut par exemple se limiter aux D qui sont discriminants d'un *corps* quadratique, ou *discriminants fondamentaux*, ce qui permet d'obtenir une somme sur les corps quadratiques, en fait une somme sur leurs ordres maximaux. Ceci se traduit par l'élimination des points (a, b, c) satisfaisant l'une des congruences

$$(*_p) \qquad \begin{cases} \mathrm{Disc}(a,b,c) \equiv 0 \pmod{p^2} & \text{pour } p \text{ premier impair,} \\ \mathrm{Disc}(a,b,c) \equiv 0, 4 \pmod{2^4} & \text{pour } p = 2. \end{cases}$$

(Cette condition ne dépend que de (a, b, c) modulo p^2, y compris quand $p = 2$.) La formule de Moebius prend alors la forme du crible d'inclusion-exclusion et on retrouve un cas particulier d'un résultat de Goldfeld-Hoffstein [26], qu'ils obtenaient en utilisant des séries d'Eisenstein de poids demi-entier.

Théorème 2.5. — *Si k parcourt les corps quadratiques, on a*

$$\sum_{0<-\mathrm{Disc}\, k<X} |\mathrm{Cl}(\mathrm{Disc}\, k)| \sim \prod_p (1 - p^{-2} - p^{-3} + p^{-4}) \cdot \frac{\pi}{18} X^{3/2}.$$

Démonstration. — Indiquons les deux ingrédients nécessaires pour résoudre l'exercice : pour un entier sans facteur carré q, soit $N_q(C_X)$ le nombre des points de C_X vérifiant $(*_p)$ pour tout $p \mid q$. Alors

$$N_q(C_X) = \nu(q) N(C_X) + R_q(C_X) \tag{3}$$

pour un reste R_q effectif venant du principe de Lipschitz et une fonction (de densité) multiplicative

$$\begin{aligned}\nu(q) &= \frac{1}{(q^2)^3}\#\left\{(a,b,c)\in(\mathbb{Z}/q^2\mathbb{Z})^3 \text{ satisfait } (*_p) \text{ pour tout } p\mid q\right\}\\ &= \prod_{p\mid q}(p^{-2}+p^{-3}-p^{-4}) = O\Big(q^{-2}\prod_{p\mid q}(1+1/p)\Big)\end{aligned}$$

obtenue par un dénombrement élémentaire (voir par exemple [1, § 4]). Si q est grand, le reste $R_q(X)$ domine le terme principal et on remplace (3) par une majoration uniforme

$$N_q(C_X) = O\Big(N(C_X)q^{-2}\prod_{p\mid q}(1+1/p)\Big), \tag{4}$$

obtenue en majorant

$$\big|\mathrm{Cl}(q^2D)\big| \,/\, |\mathrm{Cl}(D)| = O\Big(q\prod_{p\mid q}(1+1/p)\Big),$$

voir par exemple [16, § 7.D], avec une complication technique pour gérer les formes non primitives. Pour tout paramètre $Q>0$, la somme restreinte aux D fondamentaux vaut

$$\begin{aligned}\sum_{q\geqslant 1}\mu(q)N_q(C_X) &= \sum_{q<Q}\mu(q)\big(\nu(q)N(C_X)+R_q\big)+\sum_{q\geqslant Q}O(N_q(C_X))\\ &= N(C_X)\prod_p(1-\nu(p)) + O\Big(\sum_{q<Q}R_q(C)+\sum_{q\geqslant Q}\nu(q)N(C_X)+N_q(C_X)\Big),\end{aligned}$$

où μ est la fonction de Moebius. Il ne reste plus qu'à optimiser Q en fonction de X pour minimiser les termes d'erreur. Les conditions locales $(*_p)$ ne raréfient pas trop l'ensemble des points, ce qui se traduit par la convergence de $\sum_q N_q(C_X)$, $\sum_q \nu(q)$ et $\prod_p(1-\nu(p))$. □

Remarque 2.6. — Par cette méthode du « domaine fondamental », on obtient naturellement des termes d'erreur, que nous avons omis ci-dessus. Sous la forme générale du principe de Lipschitz, ils sont en effet loin d'être optimaux. Pour s'en convaincre, considérons le problème des points entiers du disque : on obtient comme Gauss

$$\#\left\{(a,b)\in\mathbb{Z}^2, a^2+b^2\leqslant X\right\} = \pi X^2 + O(X).$$

L'argument revient à considérer la formule de Poisson

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

avec $f(n)=\sqrt{X^2-n^2}\times\mathbf{1}_{|n|\leqslant X}$, pour ne retenir du membre de droite que le terme $\widehat{f}(0)$. Il est naturel qu'un lissage convenable et une analyse harmonique plus fine faisant

intervenir des majorations de sommes d'exponentielles permettent des progrès (reste en $O(X^{131/208})$ actuellement pour le problème du cercle, voir le survol de Huxley [28]).

Remarque 2.7. — Cet exemple est pédagogique. Tous ces résultats s'obtiennent en quelques lignes avec de meilleurs termes d'erreur par un argument de Siegel [51] fondé sur la formule du nombre de classes de Dirichlet.

$$L(1,\chi_D)=\sum_{n\geqslant 1}\frac{\chi_D(n)}{n}=\frac{|\mathrm{Cl}(D)|}{w(D)\sqrt{|D|}}\times\begin{cases}2\pi & \text{si } D<0\\ 4\log\varepsilon(D) & \text{si } D>0 \text{ non carré,}\end{cases}\tag{5}$$

où χ_D est le caractère de Kronecker modulo $D\equiv 0,1 \pmod 4$, où $\varepsilon(D)>1$ est l'unité fondamentale de l'ordre quadratique de discriminant D et $w(D)$ le nombre de racines de l'unité, soit $w(D)=2$ pour $D\neq -4,-6$. En sommant les $L(1,\chi_D)$ au lieu des $|\mathrm{Cl}(D)|$, on introduit essentiellement un poids $|D|^{-1/2}$, que l'on supprime par intégration par partie. Il suffit d'intervertir les sommations et de majorer non trivialement $\sum_{D<X}\chi_D(n)$ pour n non carré, par réciprocité quadratique et Pólya-Vinogradov par exemple. Comme au Corollaire 2.4, mais à l'envers, la formule de Moebius donne les formes non primitives.

Avantage supplémentaire, on obtient des estimations analogues pour les discriminants D positifs, non carrés parfaits. Suite à la modification de (5), on remplace $|\mathrm{Cl}(D)|$ par $|\mathrm{Cl}(D)|\log\varepsilon(D)$ dans la somme, et l'équivalent est multiplié par $\pi/2$ (on élimine les carrés dans le terme d'erreur). Siegel [51] en donne une interprétation en termes de domaine fondamental mais, suite à la présence d'un nombre infini d'unités, les stabilisateurs ne sont plus finis : il faut introduire une densité analogue aux $\mu(x)$ du § 3.2, formule (9).

3. ESPACES VECTORIELS PRÉHOMOGÈNES

3.1. Motivation

Le Théorème 2.2 estime une formule de masse asymptotique de type

$$\sum_{\substack{x\in L/\Gamma\\ 0<|P(x)|<X}}\mu(x)\tag{6}$$

où L est un réseau sur lequel agit un groupe linéaire discret Γ, dont les stabilisateurs Γ_x sont supposés finis, $\mu(x)=|\Gamma_x|^{-1}$, et P est un polynôme Γ-invariant. Nous avons évoqué la « méthode du domaine fondamental ». Une autre méthode classique étudie les propriétés analytiques (prolongement analytique, pôles et résidus, croissance dans les bandes verticales) de la série de Dirichlet associée

$$\sum_{x\in L'/\Gamma}\mu(x)\,|P(x)|^{-s},\quad \text{où } L'=\{x\in L\colon P(x)\neq 0\}.\tag{7}$$

Les espaces vectoriels préhomogènes introduits par Sato [45, 44] systématisent cette étude.

DÉFINITION 3.1. — *Soit k un corps. Un espace vectoriel préhomogène sur k est une représentation (G,V) d'un groupe linéaire algébrique connexe G défini sur k sur un espace affine de dimension finie $V=\mathbb{A}^n_k$, possédant une G-orbite Zariski-dense.*

On notera S le fermé complémentaire de cette orbite dense. Un espace préhomogène est donc un espace « presque homogène », clôture de l'espace homogène Gx pour $x\notin S$.

DÉFINITION 3.2. — *On dit que (G,V) préhomogène est réductif* régulier *si G est réductif et S est une hypersurface irréductible de V. Un polynôme irréductible définissant S sera appelé invariant relatif de (G,V).*

PROPOSITION 3.3 (Sato). — *Si (G,V) est préhomogène réductif régulier, un invariant relatif P est un polynôme homogène, unique modulo k^*. Il existe un caractère rationnel χ de G tel que $P(g\cdot x)=\chi(g)P(x)$ pour tout $g\in G$ et*

$$(\det\rho(g))^2=\chi(g)^{2\kappa},\quad \text{où}\quad \kappa:=\frac{\dim V}{\deg P}\in\tfrac{1}{2}\mathbb{Z}, \tag{8}$$

et $\rho: G\to \mathrm{GL}(V)$ est la représentation de G sur V.

On verra au paragraphe suivant le lien entre ces définitions et la série (en fait, les séries) de Dirichlet associée à (6). Pour les applications, il est crucial que (G,V) soit défini sur $\mathbb{R}$, et utile qu'il soit régulier (sinon les fonctions obtenues ont une variable par composante irréductible de S, ce qui complique les choses).

On dispose d'une construction abstraite assez générale d'espaces préhomogènes : si G est un groupe réductif, $P=LU$ un sous-groupe parabolique maximal, la composante de Levi L agit par conjugaison sur le radical unipotent U, donc sur l'abélianisé $V=U/[U,U]$. Vinberg [52] démontre que (L,V) est préhomogène.

DÉFINITION 3.4. — *Un tel espace préhomogène est dit* de type parabolique.

Sur $\mathbb{C}$, les espaces préhomogènes irréductibles, modulo une relation d'équivalence naturelle (*roques* ou *castling transforms*), sont classifiés par Kimura et Sato [45] : il y a 29 types réguliers, dont 5 séries infinies : matrices $m\times n$, formes quadratiques en n variables, etc. Les formes réelles de ces espaces qui sont paraboliques sont classifiées par Rubenthaler [41] : presque tous les types de Kimura-Sato sont paraboliques, il y a 6 exceptions ne comportant aucune série infinie. Il existe aussi une classification sur un corps local ou un corps de nombres, due à Saito [42].

Inspiré par Wright et Yukie [56] (qui s'intéressent aux orbites rationnelles, *cf.* § 3.3), Bhargava [3, 4, 5, 6, 7] a recherché systématiquement comment paramétrer des situations liées aux anneaux de nombres par les orbites *entières* d'espaces préhomogènes. Il se trouve que tous les exemples obtenus sont de type parabolique (réductif) régulier, associés aux groupes de Lie simples $G=B_2, G_2, B_3, D_4, D_5, E_6$ (corps quadratiques),

G_2, F_4, E_6, E_7 (cubiques), F_4 (quartiques), E_8 (quintiques), pour un parabolique LU convenable. Guidé par la classification de Kimura-Sato et des considérations heuristiques sur les diagrammes de Dynkin et leurs symétries, Bhargava construit pour beaucoup d'entre eux des lois de composition que nous décrirons aux §§ 4 et 5. Les structures de groupe obtenues ont peu d'intérêt intrinsèque puisqu'on les obtient aussi via les groupes des classes des anneaux sous-jacents, du moins pour l'instant. Mais elles en donnent des descriptions explicites, et sont justiciables du même type de traitement qu'au § 2.

3.2. La théorie de Sato-Shintani

Soit (G, V) réductif régulier associé à P, χ comme ci-dessus. On note H le noyau de χ. Soit $G_{\mathbb{R}}^+$ la composante connexe du neutre dans le groupe de Lie $G_{\mathbb{R}}$, $H_{\mathbb{R}}^+ = H_{\mathbb{R}} \cap G_{\mathbb{R}}^+$. On fixe des mesures de Haar dg sur $G_{\mathbb{R}}^+$, d^1h sur $H_{\mathbb{R}}^+$, $d\nu_x$ sur $(H_{\mathbb{R}}^+)_x$ pour $x \in (V - S)$ avec

$$\begin{aligned}\int_{G_{\mathbb{R}}^+} \phi(g)dg &= \int_{G_{\mathbb{R}}^+/H_{\mathbb{R}}^+} \frac{d\chi(g)}{|\chi(g)|} \int_{H_{\mathbb{R}}^+} \phi(gh)d^1h \\ &= \int_{G_{\mathbb{R}}^+/(H_{\mathbb{R}}^+)_x} |P(g\cdot x)|^{-\kappa}\, d(g\cdot x) \int_{(H_{\mathbb{R}}^+)_x} \phi(gh)d\nu_x(h), \quad \forall\, \phi \in L^1(G_{\mathbb{R}}^+).\end{aligned}$$

(D'après (8), $|P(y)|^{-\kappa}\, dy$ est une mesure $G_{\mathbb{R}}^+$-invariante sur $V - S$.) Soit $\Gamma = G_{\mathbb{Z}} \cap H_{\mathbb{R}}^+$. On fixe un réseau Γ-stable L, et on pose $L' = L - (L \cap S)$. On fait les hypothèses simplificatrices suivantes :

(H1) (G, V) est *réductif régulier* défini sur $\mathbb{Q}$, tel que $G_{\mathbb{Z}} \cdot V_{\mathbb{Z}} \subset V_{\mathbb{Z}}$,

(H2) $S \cap V_{\mathbb{R}}$ se décompose en un nombre fini de $H_{\mathbb{R}}^+$-orbites,

(H3) une hypothèse technique destinée à justifier la convergence des identités formelles, en particulier (11) : pour toute fonction ϕ dans la classe de Schwartz sur $V_{\mathbb{R}}$, l'intégrale

$$I(\phi) = \int_{H_{\mathbb{R}}/H_{\mathbb{Z}}} \sum_{x \in L} \phi(h \cdot x)d^1h$$

converge absolument et définit une distribution tempérée sur $V_{\mathbb{R}}$.

La dernière hypothèse est restrictive, elle ne couvre pas le cas des formes quadratiques $\mathrm{Sym}^2 \mathbb{A}^n$ si $n \leqslant 4$ ou des formes cubiques $\mathrm{Sym}^3 \mathbb{A}^2$ par exemple. Shintani [49, 50] règle le problème pour ces deux exemples en renormalisant les fonctions zêta.

Soient $V_1, \ldots, V_l$ les composantes connexes de $(V - S)_{\mathbb{R}}$, qui sont des $G_{\mathbb{R}}^+$-orbites. Pour tout $x \in (V - S)_{\mathbb{Q}}$, on définit la fonction Γ-invariante

$$\mu(x) = \int_{(H_{\mathbb{R}}^+)_x/\Gamma_x} d\nu_x < \infty. \tag{9}$$

L'hypothèse (H3) implique la finitude de $\mu(x)$, en fait une majoration polynomiale en X de la somme des $\mu(x)$ sur $\{x \in L'/\Gamma, |P(x)| < X\}$. On définit les séries de Dirichlet

$$\xi_i(s,L) = \sum_{x\in(L\cap V_i)/\Gamma} \mu(x)\,|P(x)|^{-s}, \text{ associées à } \sum_{\substack{x\in(L\cap V_i)/\Gamma\\ 0<|P(x)|<X}} \mu(x) \qquad (1\leqslant i\leqslant l), \tag{10}$$

qui convergent donc pour $\Re(s) \gg 1$. (Ceci est démontré par Saito [43] sous des hypothèses bien moins restrictives que (H3).) Si Γ_x est fini pour tout $x \in V_i$, on obtient $\mu(x) = c_i\,|\Gamma_x|^{-1}$ pour une constante c_i indépendante de $x \in V_i$. Il s'agit donc bien d'un raffinement de (7), qu'on retrouve par sommation sur les composantes connexes.

On obtient des notions analogues pour la représentation contragrédiente sur le dual (G, V^*) qui est aussi préhomogène : S^*, P^* de même degré que P, $\chi^* = \chi^{-1}$, $V_1^* \cup \cdots \cup V_l^*$ (pour le même l), $d\nu^*(x)$, $\xi_i^*(s, L^*)$, etc. Sous nos hypothèses, en considérant

$$Z(\phi,s) := \int_{G_{\mathbb{R}}^+/\Gamma} |\chi(g)|^s \sum_{x\in L'} \phi(g\cdot x)dg = \sum_{i=1}^{l} \xi_i(s) \int_{V_i} \phi(y)\,|P(y)|^{s-\kappa}\,dy \tag{11}$$

et la distribution duale Z^*, Sato et Shintani [46] démontrent que les séries $\xi_i(s, L)$, $\xi_i^*(s, L^*)$ admettent un prolongement analytique méromorphe sur $\mathbb{C}$ et satisfont une équation fonctionnelle matricielle $l \times l$ reliant

$$(\xi_i(s,L)\colon 1\leqslant i\leqslant l) \quad \text{et} \quad (\xi_i^*(\kappa - s, L^*)\colon 1\leqslant i\leqslant l).$$

Le prolongement vient d'une intégration par parties qui fait intervenir des polynômes de Bernstein-Sato ou « fonctions b », définis par

$$P^*(\nabla_x)P(x)^s = b(s)P(x)^{s-1},$$

où $P^*(\nabla_x)$ est l'opérateur différentiel à coefficients constants sur $V_{\mathbb{R}}$ satisfaisant

$$P^*(\nabla_x)\exp(\langle x,y\rangle) = P^*(y)\exp(\langle x,y\rangle), \qquad \forall\, y \in V_{\mathbb{R}}^*.$$

On a $\deg b = \deg P$ et, sous nos hypothèses, les zéros de $b(s-\kappa)$ sont les pôles (simples) des ξ_i et ξ_i^*. Les fonctions b sont connues explicitement pour les 29 types réguliers de Kimura-Sato, ainsi que leur comportement par roque (*cf.* Kimura [32]) et leurs zéros sont rationnels (voir aussi Kashiwara [31]). Dans les autres cas où les ξ_i, ξ_i^* sont connus, la multiplicité d'un zéro de $b(s-\kappa)$ borne celle du pôle, mais il arrive qu'on n'ait pas égalité. L'équation fonctionnelle suit de la formule sommatoire de Poisson appliquée à la série théta intervenant dans $Z(\phi, s)$, en isolant la partie polaire ($x \in L - L'$, $x^* \in L^* - L'^*$). Par transformée de Mellin et déplacement de contour, on en tire un développement asymptotique des sommes partielles (10) quand $X \to +\infty$.

Exemple 3.5. — Pour $(G, V) = (\mathrm{GL}_1, \mathbb{A}^1)$, le plus simple des espaces préhomogènes, on trouve $P(x) = x$, $\kappa = 1$, $b(s) = s$, $(V-S)_{\mathbb{R}} = V_1 \cup V_2 = \mathbb{R}_+^* \cup \mathbb{R}_-^*$ et $G_x = \{1\}$ pour $x \in (V-S)_{\mathbb{R}}$, soit $\mu(x) = 1$ avec la normalisation naturelle. Ainsi $\xi_i(s) = \xi_i^*(s) = \zeta(s)$

pour $i = 1, 2$ et on retrouve les résultats de Riemann, essentiellement par la même méthode.

3.3. Adélisation et G_k-orbites

Si $\mathbb{A}$ désigne les adèles du corps global k, on remplace le sous-groupe discret $G_{\mathbb{Z}} \subset G_{\mathbb{R}}$ par $G_k \subset G_{\mathbb{A}}$. Pour $\phi = \otimes_v \phi_v$ une fonction de Schwartz-Bruhat sur $V_{\mathbb{A}}$, on pose

$$Z(\phi, s) = \int_{G_{\mathbb{A}}/G_k} |\chi(g)|_{\mathbb{A}}^s \sum_{x \in L'} \phi(g \cdot x) dg, \tag{12}$$

et le formalisme est proche de celui du paragraphe précédent, en distinguant une place infinie de k. Les séries de Dirichlet associées se décomposent en somme sur les orbites L'/G_k de termes faisant apparaître des produits eulériens sur v de fonctions zêta locales

$$\int_{G_{k_v} \cdot x} \phi_v(y) \, |P(y)|_v^{s-\kappa} \, dy, \tag{13}$$

pondérés par $\mu(x)/o(x)$, où $o(x) = [(H_x)_k : (H_x^0)_k]$ et $\mu(x)$ est le volume de $(H_x^0)_{\mathbb{A}}/(H_x^0)_k$ pour une mesure convenable (voir [57]). Pour v infinie, les b-fonctions permettent comme précédemment le prolongement méromorphe de (13). Si v est finie et ϕ_v est la fonction caractéristique du disque unité $\mathcal{O}_{k_v}$, on obtient une fonction locale d'Igusa, d'expression élémentaire connue pour presque tous les types de Kimura-Sato (voir [29]). Hors d'un ensemble fini de places T, ϕ_v est de cette forme, et la fonction zêta pour T fixée est contrôlée. Par contre, pour énumérer les G_k-orbites, il faut un passage à la limite sur T, axiomatisé par Wright (cf [57, § 0.5]), d'esprit analogue à celui du § 2.3, mais bien plus contraignant. Ceci étant dit, que représentent les G_k-orbites ?

Exemple 3.6. — Reconsidérons les formes quadratiques binaires du § 2 ; la $\mathrm{SL}_2(k)$-orbite d'une forme quadratique irréductible x de $\mathrm{Sym}^2 k^2$ définit un *corps* quadratique K_x/k : l'orbite des racines de x. Les formes réductibles forment deux orbites, suivant qu'elles ont ou non une racine multiple. En étudiant la fonction zêta adélique associée, Datskovsky [19] obtient une version relative du Théorème 2.5 sur un corps de nombres k : dans ce cas, $\mu(x)$ est essentiellement $|\mathrm{Disc}\, K_x|^{1/2} \, \mathrm{Res}(\zeta_{K_x}, s = 1)$.

Exemple 3.7. — Shintani [50, 49], dans les premières études sur les séries de Dirichlet provenant de la théorie du § 3.2, obtient d'excellents termes d'erreur pour le nombre de classes de formes quadratiques ou cubiques binaires avec les méthodes du § 3.2. À nouveau, l'ensemble naturel des orbites de formes cubiques est stratifié suivant le type de décomposition de l'équation associée. En traitant les formes quadratiques et cubiques générales, Shintani peut isoler les $G_{\mathbb{Z}}$-orbites de formes cubiques irréductibles. Nous verrons au § 5.1 que ce dernier exemple paramètre les anneaux cubiques. Datskovsky et Wright [54, 17, 18] adélisent le travail de Shintani sur un corps global k

de caractéristique différente de 2 ou 3. Comptant les G_k-orbites de formes cubiques irréductibles, ils obtiennent la densité des discriminants des corps cubiques sur k.

Remarque 3.8. — Dans ces deux cas, la fonction zêta pour T fixé admet un autre pôle réel à gauche de 1, mais le passage à la limite sur T empêche de tenir compte de ce pôle secondaire, et même d'obtenir un terme d'erreur. On conjecture que le passage à la limite formel donne le développement asymptotique correct (voir Roberts [40] pour le cas cubique).

Plus généralement, soit $n \geqslant 1$ et k un corps infini de caractéristique nulle ou strictement supérieure à n. On note $E(k,n)$ l'ensemble des classes d'isomorphismes d'extensions galoisiennes de k qui sont corps de décomposition d'un polynôme séparable de degré inférieur à n. Wright et Yukie [56] (voir aussi [30]) construisent pour six nouveaux types d'espaces préhomogènes paraboliques (G,V) une bijection naturelle entre G_k-orbites de $(V-S)_k$ et classes de conjugaison d'homomorphismes de $\mathrm{Gal}(\overline{k}/k)$ dans le groupe symétrique à n éléments où $n = 2,3,4,5$ suivant les cas. Ceci définit une application

$$\alpha_V : (V-S)_k/G_k \longrightarrow E(k,n),$$

où une orbite a pour image le noyau d'un des homomorphismes associés. En inspectant les classes de conjugaison de S_n, on voit que α_V est bijective pour les six exemples associés à $n = 2,3$. Dans les deux cas restants, $n = 4,5$ et les fibres sont réduites à un point, sauf dans des cas dégénérés (2 ou 4 points) correspondant à des extensions de petit degré, inférieur à 12. Quand k est un corps global, en supposant résolus les problèmes de convergence et la détermination des pôles et résidus, on espère pouvoir compter les extensions x de k de degré n munies du poids $\mu(x)/o(x)$, mais ce programme n'est pas achevé. La partie globale du cas quartique est traitée par Yukie [57].

3.4. Comparaison

Pour conclure cette présentation des méthodes en présence[(4)], les calculs de densités de discriminants d'extensions de type Wright-Yukie reposent sur l'existence d'une représentation (G,V) préhomogène, telle que V_k/G_k paramètre les extensions du corps k. Ces constructions sont actuellement restreintes aux extensions de degré $n \leqslant 5$.

Bhargava démontre que dans ces mêmes cas, $V_{\mathbb{Z}}/G_{\mathbb{Z}}$ paramètre essentiellement des anneaux de nombres de degré n sur $\mathbb{Z}$ (et non des corps). En principe, les méthodes élémentaires du § 2 permettent de les énumérer, puis de les cribler pour ne retenir que les ordres maximaux, ce qui revient à compter leurs corps de fractions, *i.e.* les

[(4)] Pour être complet, il eût fallu inclure les séries génératrices issues de la théorie du corps de classes ou directement de la théorie de Kummer, pour les extensions abéliennes d'une base raisonnable. Elles sont disjointes des travaux de Bhargava que nous présentons et nous renvoyons au survol de Cohen [11].

$G_{\mathbb{Q}}$-orbites de $V_{\mathbb{Q}}$. Ces méthodes fournissent des termes d'erreur qui survivent aux cribles, mais restent loin des valeurs conjecturées à la lecture des pôles des séries de Sato-Shintani.

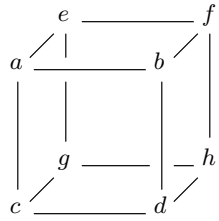
À l'inverse, ces dernières fournissent les termes d'erreur attendus sur les problèmes de comptage de $G_{\mathbb{Z}}$-orbites et leur adélisation permet le passage aux G_k-orbites sur V_k, et donc aux extensions du corps global k par la théorie de Wright-Yukie, pour $n = 2, 3$. Par contre, elle ne fournit pour l'instant qu'un équivalent pour ces décomptes d'extensions de k, y compris quand $k = \mathbb{Q}$, et se heurte à de redoutables problèmes de convergence d'identités formelles (voir [57, Part IV]).

Ce sont les problèmes de comptage associés aux deux cas $n = 4, 5$ ci-dessus que Bhargava vient, semble-t-il, de résoudre sur $\mathbb{Q}$, en étudiant directement les domaines fondamentaux associés aux $G_{\mathbb{Z}}$-orbites des espaces préhomogènes de Wright et Yukie. Nous décrirons une partie de ces travaux à partir du § 5.3, mais nous commençons par sa ré-interprétation des cas $n = 2, 3$.

4. PARAMÉTRISATIONS ET COMPOSITIONS QUADRATIQUES

4.1. Cubes

Soit $\mathcal{C}_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, dont on peut représenter les éléments par des octuplets $(a, b, c, d, e, f, g, h) \in \mathbb{Z}^8$ ou plus naturellement par un cube de sommets étiquetés par des entiers :



En notant (α, β) la base canonique de $\mathbb{Z}^2$, ce cube remplace avantageusement l'élément

$$\begin{aligned} & a(\alpha\otimes\alpha\otimes\alpha) + b\,(\alpha\otimes\beta\otimes\alpha) + c(\beta\otimes\alpha\otimes\alpha) + d(\beta\otimes\beta\otimes\alpha) \\ + \quad & e(\alpha\otimes\alpha\otimes\beta) + f(\alpha\otimes\beta\otimes\beta) + g(\beta\otimes\alpha\otimes\beta) + h(\beta\otimes\beta\otimes\beta). \end{aligned}$$

On peut partitionner un tel cube $A \in \mathcal{C}_2$ en deux matrices 2×2 de trois façons différentes : $M_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), N_1 = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$, ou $M_2 = \left(\begin{smallmatrix} a & c \\ e & g \end{smallmatrix}\right), N_2 = \left(\begin{smallmatrix} b & d \\ f & h \end{smallmatrix}\right)$, ou encore $M_3 = \left(\begin{smallmatrix} a & e \\ b & f \end{smallmatrix}\right), N_3 = \left(\begin{smallmatrix} c & g \\ d & h \end{smallmatrix}\right)$. Soit $\gamma = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ un élément générique de $\mathrm{SL}_2(\mathbb{Z})$. On définit une action de $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{C}_2$, en spécifiant que $(\gamma \times \mathrm{Id} \times \mathrm{Id})$ agit sur le cube A en remplaçant (M_1, N_1) par $(rM_1 + sN_1, tM_1 + uN_1)$, $(\mathrm{Id} \times \gamma \times \mathrm{Id})$ et $(\mathrm{Id} \times \mathrm{Id} \times \gamma)$ agissant de même sur (M_2, N_2) et (M_3, N_3) respectivement. Il s'agit bien d'une action (à gauche !), on vérifie que les actions des trois facteurs $\mathrm{SL}_2(\mathbb{Z})$ dans Γ

commutent. C'est l'analogue de l'associativité de la multiplication matricielle : les opérations sur les lignes et colonnes d'une matrice rectangulaire commutent. Par exemple, la transformation de (M_1, N_1) indiquée se traduit par $(M_2, N_2) \to (\gamma M_2, \gamma N_2)$ et $(M_3, N_3) \to (M_3{}^t\gamma, N_3{}^t\gamma)$.

Alternativement, cette action est donnée par

$$(\gamma_1, \gamma_2, \gamma_3) \cdot (x_1 \otimes x_2 \otimes x_3) = \gamma_3 x_1 \otimes \gamma_2 x_2 \otimes \gamma_1 x_3.$$

(Nous conservons les normalisations de Bhargava.)

Étant donné un cube $A \in \mathcal{C}_2$, on construit pour $1 \leqslant i \leqslant 3$ une forme quadratique binaire $Q_i = Q_i^A$ par la règle

$$Q_i(x, y) = -\det(xM_i - yN_i).$$

La forme Q_1 est invariante sous l'action de $\{\mathrm{Id}\} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \subset \Gamma$, puisque les deux autres facteurs agissent par multiplication à gauche ou à droite sur (M_1, N_1). Le premier facteur agit de la façon habituelle $(\gamma \cdot Q_1)(x, y) = Q_1((x, y)\gamma)$, et cette action a un unique invariant, à savoir $\mathrm{Disc}\, Q_1$. Il en est donc de même pour l'action de Γ sur $\mathcal{C}_2$. Par symétrie, $\mathrm{Disc}\, Q_2$ et $\mathrm{Disc}\, Q_3$ sont aussi des invariants, et on vérifie que $\mathrm{Disc}\, Q_1 = \mathrm{Disc}\, Q_2 = \mathrm{Disc}\, Q_3$. On baptise cette valeur commune $\mathrm{Disc}\, A$. Explicitement,

$$\begin{aligned}
Q_1 &= (bc - ad,\ -ah + bg + cf - de,\ fg - eh),\\
Q_2 &= (ce - ag,\ -ah - bg + cf + de,\ df - bh),\\
Q_3 &= (be - af,\ -ah + bg - cf + de,\ dg - ch),\\
\mathrm{Disc}\, A &= a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2\\
&\quad - 2(abgh + acfh + adeh + bcfg + bdeg + cdef) + 4(adfg + bceh).
\end{aligned}$$

Toute forme quadratique $(d, h, g) \in (\mathrm{Sym}^2\, \mathbb{Z}^2)^*$ provient d'un cube : prendre $a = -1$, $b = c = e = 0$, $f = 1$ par exemple.

4.2. Loi du cube et loi de Gauss

Définition 4.1. — *Un cube $A \in \mathcal{C}_2$ est dit* projectif *si les trois formes quadratiques associées (Q_1^A, Q_2^A, Q_3^A) sont primitives. On note $\mathrm{Cl}(\mathcal{C}_2; D)$ l'ensemble des classes de cubes projectifs modulo Γ de discriminant D.*

Motivé par la loi de groupe sur une courbe elliptique, Bhargava considère le groupe libre engendré par les formes quadratiques *primitives* de discriminant D, modulo les relations

$$Q_1^A \oplus Q_2^A \oplus Q_3^A = 0, \tag{14}$$

où $A \in \mathcal{C}_2$. En particulier, deux formes $\mathrm{SL}_2(\mathbb{Z})$-équivalentes sont identifiées puisque, si Q_1 est donnée, alors il existe un cube A comportant Q_1 parmi ses formes associées (Q_1, Q_2, Q_3). En considérant $(\gamma \times \mathrm{Id} \times \mathrm{Id}) \cdot A$, on en déduit que

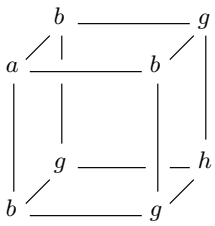
$$Q_1 \oplus Q_2 \oplus Q_3 = \gamma Q_1 \oplus Q_2 \oplus Q_3 = 0,$$

soit $Q_1 = \gamma Q_1$ dans le quotient de Bhargava, pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. De même, on voit facilement que $(a,b,c) \oplus (c,b,a) = 0$.

THÉORÈME 4.2. — *Soit $D \equiv 0,1 \pmod 4$ un entier. Fixons un cube projectif A_0 de discriminant D, dont les formes quadratiques associées sont* égales *; soit Q^0 cette forme primitive. Il existe une unique loi de groupe additif sur l'ensemble des classes de formes quadratiques binaires $[Q]$* primitives *modulo $\mathrm{SL}_2(\mathbb{Z})$, de discriminant D, telle que $[Q^0] = 0$, et $[Q_1^A] + [Q_2^A] + [Q_3^A] = 0$ pour tout cube projectif $A \in \mathcal{C}_2$. Réciproquement, pour tout triplet de classes de formes primitives de somme nulle dans ce groupe, il existe un cube projectif $A \in \mathcal{C}_2$, unique à Γ-équivalence près, dont ce sont les formes associées.*

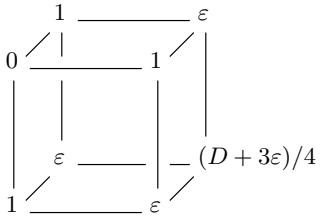
On démontrera ce résultat en même temps que le Théorème 4.6. Les cubes A_0 satisfaisant la condition du théorème avec $Q^0 \neq (0,0,0)$ présentent une triple symétrie :

(15)



Le choix le plus naturel est $Q^0 = (1, \varepsilon, (\varepsilon - D)/4)$ pour $D \equiv \varepsilon \pmod 4$, $\varepsilon \in \{0,1\}$, associée au cube A_0 de discriminant D donné par

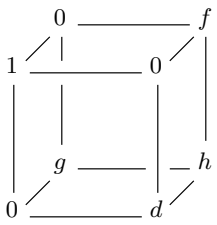
(16)



THÉORÈME 4.3. — *Pour le choix de A_0 donné par* (16)*, la loi de groupe du Théorème 4.2 est la composition de Gauss du Théorème 2.1.*

Démonstration. — $[Q^0]$ est bien la classe principale de Gauss. Si A est un cube projectif, le pgcd de ses coefficients est 1. À Γ-équivalence près, on peut donc supposer qu'un sommet est 1. Toujours à Γ-équivalence près, on utilise ce 1 pour annuler les trois sommets adjacents (pivot de Gauss tridimensionnel !). On suppose donc que A

est de la forme



soit

$$Q_1 = (-d, h, fg), \quad Q_2 = (-g, h, df), \quad Q_3 = (-f, h, dg).$$

De $[Q_1] + [Q_2] = -[Q_3] = (dg, h, -f)$, on tire la composition de Dirichlet (2). □

COROLLAIRE 4.4. — *Soit $D \equiv 0, 1 \pmod 4$ un entier, et soit A_0 le cube* (16)*. Il existe une unique loi de groupe sur $\mathrm{Cl}(\mathcal{C}_2; D)$, de neutre $\Gamma \cdot A_0$, telle que les projections*

$$\begin{aligned} \phi_i : \mathrm{Cl}(\mathcal{C}_2; D) &\longrightarrow \mathrm{Cl}^+(D) \\ A &\longmapsto [Q_i^A] \end{aligned}$$

soient des homomorphismes de groupe pour $1 \leqslant i \leqslant 3$.

Démonstration. — Si A et A' sont deux cubes projectifs, alors

$$\sum_{i=1}^{3} ([Q_i^A] + [Q_i^{A'}]) = \sum_{i=1}^{3} [Q_i^A] + \sum_{i=1}^{3} [Q_i^{A'}] = 0 + 0 = 0.$$

D'après le dernier point du Théorème 4.2, il existe $A'' \in \mathcal{C}_2$ tel que $[Q_i^{A''}] = [Q_i^A] + [Q_i^{A'}]$ pour $i = 1, 2, 3$. Les $Q_i^{A''}$ étant primitives par définition de la loi de groupe, A'' est projectif. On pose $A'' = A' + A$. □

4.3. Paramétrisations

Identifions maintenant ces lois de composition.

DÉFINITION 4.5. — *Soit S l'anneau quadratique de discriminant D et $K = S \otimes_{\mathbb{Z}} \mathbb{Q}$ l'algèbre quadratique associée. Un triplet (I_1, I_2, I_3) d'idéaux orientés de S est* équilibré *si $I_1 I_2 I_3 \subset S$ et $\mathrm{N}(I_1)\,\mathrm{N}(I_2)\,\mathrm{N}(I_3) = 1$. Deux tels triplets (I_1, I_2, I_3) et (I_1', I_2', I_3') sont équivalents s'il existe $\kappa_1, \kappa_2, \kappa_3 \in K$ tel que $I_i = \kappa_i I_i'$ pour $1 \leqslant i \leqslant 3$.*

Si S est un anneau de Dedekind, une classe d'équivalence de triplets équilibrés n'est rien d'autre qu'un triplet de classes d'idéaux restreintes de produit 1.

THÉORÈME 4.6. — *Il existe une bijection canonique entre*

– *l'ensemble des Γ-orbites de discriminant $D \neq 0$ sur l'espace $\mathcal{C}_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$,*

– *l'ensemble des classes d'isomorphismes de paires $(S, (I_1, I_2, I_3))$, où S est un anneau quadratique orienté de discriminant D, et (I_1, I_2, I_3) est une classe d'équivalence de triplets équilibrés d'idéaux orientés de S.*

Sa restriction aux cubes projectifs induit un isomorphisme de groupes

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \simeq \mathrm{Cl}^+(D) \times \mathrm{Cl}^+(D).$$

Démonstration. — Soit $D \equiv \varepsilon \pmod 4$, $\varepsilon \in \{0,1\}$ et soit $\langle 1, \tau\rangle$ une base positive de S, pour une orientation $\pi : S/\mathbb{Z} \to \mathbb{Z}$, où $\tau^2 - \varepsilon\tau + (\varepsilon - D)/4 = 0$. Soient $\langle \alpha_1, \alpha_2\rangle$, $\langle \beta_1, \beta_2\rangle$, $\langle \gamma_1, \gamma_2\rangle$ des bases de I_1, I_2, I_3, de même orientation que I_1, I_2, I_3 respectivement. Comme $I_1 I_2 I_3 \subset S$, on a

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk}\tau, \tag{17}$$

pour des entiers a_{ijk} et c_{ijk}, $1 \leqslant i, j, k \leqslant 2$. Le cube associé est $A = (a_{ijk})$. De façon plus intrinsèque, $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ représente l'application trilinéaire $I_1 \times I_2 \times I_3 \to \mathbb{Z}$ donnée par la formule $(x, y, z) \mapsto \pi(xyz)$. On vérifie que A est bien défini à Γ-équivalence près.

Réciproquement, pour un cube $A = (a_{ijk})$ fixé, on considère le système (17), qui comporte essentiellement des indéterminées pour l'instant. On cherche τ, (α_i), (β_j), (γ_k) le satisfaisant tels que les S, I_1, I_2, I_3 associés vérifient $I_1 I_2 I_3 \subset S$ et $N(I_1)N(I_2)N(I_3) = 1$. Ceci implique

$$\operatorname{Disc} A = \mathrm{N}(I_1)^2\, \mathrm{N}(I_2)^2\, \mathrm{N}(I_3)^2 \operatorname{Disc} S,$$

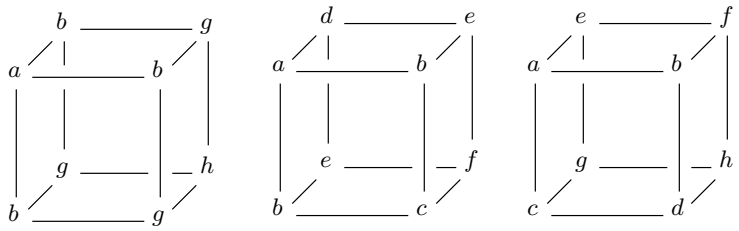
ainsi $\operatorname{Disc} S = \operatorname{Disc} A$ et donc S sont déterminés. Comme dans la preuve du Théorème 4.3, on peut supposer que les trois sommets adjacents à un sommet fixé (qui porte le pgcd des coefficients) sont nuls. Par associativité et commutativité de la multiplication dans S, un calcul explicite montre que les c_{ijk} sont déterminés, et entiers ! Grâce à la nullité de trois des a_{ijk}, on déduit de (17) que les $\alpha_i, \beta_j, \gamma_k$ sont inversibles dans K, puis que les quotients α_1/α_2, β_1/β_2 et γ_1/γ_2 sont fixés. Un calcul explicite montre que les $\mathbb{Z}$-modules obtenus sont bien des idéaux.

Un triplet équilibré (I_1, I_2, I_3) est dit projectif si les I_i sont projectifs (c'est-à-dire inversibles) comme S-modules. Les formes normes associées aux I_i sont exactement les Q_i^A, donc les I_i sont projectifs si et seulement si A l'est. L'ensemble des classes d'équivalence de triplets équilibrés projectifs est muni de la loi de groupe naturelle $(I_1, I_2, I_3) \cdot (I_1', I_2', I_3') = (I_1 I_1', I_2 I_2', I_3 I_3')$, qui le rend isomorphe à $\mathrm{Cl}^+(D) \times \mathrm{Cl}^+(D)$ par la projection $(I_1, I_2, I_3) \mapsto (I_1, I_2)$. On conclut grâce aux Théorèmes 4.3 et 2.1. □

Bhargava définit de même des flèches naturelles préservant le discriminant entre espaces de formes

$$\begin{array}{ccccc}
\mathrm{Sym}^3 \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \\
 & & \downarrow & & \downarrow \\
 & & (\mathrm{Sym}^2 \mathbb{Z}^2)^* & \longleftarrow & \mathbb{Z}^2 \otimes \Lambda^2 \mathbb{Z}^4 \\
 & & & & \downarrow \\
 & & & & \Lambda^3 \mathbb{Z}^2
\end{array}$$

munies d'actions de groupes linéaires. Par exemple, la première rangée correspond à l'inclusion des ensembles de cubes présentant une triple symétrie, une double symétrie ou pas de symétrie *a priori* :



À partir de la loi du cube, on obtient des lois de groupe sur les ensembles d'orbites projectives de discriminant D non nul :

$$\begin{array}{ccccc}
\mathrm{Cl}(\mathrm{Sym}^3\,\mathbb{Z}^2;D) & \longrightarrow & \mathrm{Cl}(\mathbb{Z}^2\otimes\mathrm{Sym}^2\,\mathbb{Z}^2;D) & \longrightarrow & \mathrm{Cl}(\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2;D)\\
 & & \downarrow\wr & & \downarrow\\
 & & \mathrm{Cl}^+(D)\simeq\mathrm{Cl}((\mathrm{Sym}^2\,\mathbb{Z}^2)^*;D) & \xleftarrow{\sim} & \mathrm{Cl}(\mathbb{Z}^2\otimes\Lambda^2\mathbb{Z}^4;D)\\
 & & & & \downarrow\\
 & & & & \mathrm{Cl}(\Lambda^3\mathbb{Z}^2;D)=\{0\}
\end{array}$$

Bhargava identifie ensuite les structures dont ils paramètrent les classes d'équivalence. Dans l'énumération suivante, toutes les formes et les anneaux sont de discriminant non nul, S désigne un anneau quadratique orienté, I (avec ou sans indice) un S-idéal orienté, et un « S-idéal de rang n » est un sous-S-module de $(S\otimes\mathbb{Q})^n$, de rang maximal $2n$ sur $\mathbb{Z}$. Voir [5] pour les définitions manquantes et les démonstrations.

– $\mathrm{Sym}^3\,\mathbb{Z}^2$, $\mathrm{SL}_2(\mathbb{Z})$: formes cubiques binaires et triplets (S,I,δ), où $\delta\in S\otimes\mathbb{Q}$ tel que $I^3\subset\delta S$ et $\mathrm{N}(I)^3=\mathrm{N}(\delta)$. Si on se restreint aux formes projectives, I est inversible et $\mathrm{N}(I^3)=\mathrm{N}(I)^3$, d'où $I^3=(\delta)$. L'application $\mathrm{Cl}(\mathrm{Sym}^3\,\mathbb{Z}^2;D)\to\mathrm{Cl}_3(D)$ donnée par $(S,I,\delta)\to I$ est un morphisme surjectif dont le noyau est de cardinal $\#(S^*/S^{*3})$. En particulier si S est un anneau de Dedekind, ce morphisme est un isomorphisme si $D<-3$, et a un noyau d'ordre 3 sinon (cette construction remonte à Eisenstein [23], voir aussi Hoffman-Morales [27]).

– $\mathbb{Z}^2\otimes\mathrm{Sym}^2\,\mathbb{Z}^2$, $\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_2(\mathbb{Z})$: paires de formes quadratiques binaires et triplets $(S,I_1,I_2,I_3=I_2)$ où (I_1,I_2,I_2) est un triplet équilibré. L'application naturelle $\mathbb{Z}^2\otimes\mathrm{Sym}^2\,\mathbb{Z}^2\to(\mathrm{Sym}^2\,\mathbb{Z}^2)^*$ donnée par $A\mapsto Q_3^A$ devient un isomorphisme par passage aux quotients, si on la restreint aux classes projectives ($I_1I_2I_3$ étant principal, si $I_2=I_3$ l'est, I_1 aussi).

– $(\mathrm{Sym}^2\,\mathbb{Z}^2)^*$, $\mathrm{SL}_2(\mathbb{Z})$: formes quadratiques binaires, c'est le cas considéré par Gauss.

– $\mathbb{Z}^2 \otimes \Lambda^2\mathbb{Z}^4$, $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$: paires de 2-formes alternées de rang 4. Elles paramètrent les paires $(S, (I, M))$, où M est un « S-idéal de rang 2 » et (I, M) est équilibré.

– $\Lambda^3\mathbb{Z}^6$, $\mathrm{SL}_6(\mathbb{Z})$: 3-formes alternées de rang 6. Elles paramètrent les paires (S, M) où M est un « S-idéal de rang 3 » équilibré.

5. PARAMÉTRISATIONS EN DEGRÉ SUPÉRIEUR

5.1. Anneaux cubiques

THÉORÈME 5.1 (Delone-Faddeev [22], Gan-Gross-Savin [25])

Il existe une bijection canonique entre les deux ensembles suivants :

– *les classes d'isomorphismes d'anneaux cubiques,*

– *les formes cubiques binaires entières, soit* $(\mathrm{Sym}^3 \mathbb{Z}^2)^*$*, modulo l'action de* $\mathrm{GL}_2(\mathbb{Z})$.

Cette bijection préserve le discriminant. La classe contenant la forme de coefficients (a, b, c, d) *est associée au* $\mathbb{Z}$*-module libre* $R = \langle 1, \omega, \theta \rangle_{\mathbb{Z}}$*, muni de la multiplication*

$$\begin{aligned} \omega\theta &= -ad, \\ \omega^2 &= -ac + b\omega - a\theta, \\ \theta^2 &= -bd + d\omega - c\theta. \end{aligned}$$

Démonstration. — Vérification explicite, facilitée par le choix d'une base de R telle que $\omega\theta \in \mathbb{Z}$, toujours possible par translation de ω et θ. Une autre démonstration pour R intègre consiste à comparer deux applications classiques : la forme indice (qui, à un ordre de rang n, associe une forme de $(\mathrm{Sym}^{n(n-1)/2} \mathbb{Z}^{n-1})^*$, modulo $\mathrm{GL}_{n-1}(\mathbb{Z})$) et l'ordre de Dedekind (qui, à une forme irréductible de $(\mathrm{Sym}^n \mathbb{Z}^2)^*$, associe un ordre de degré n). Elles sont compatibles si et seulement si $n = 3$, et inverses l'une de l'autre dans ce cas. □

Par exemple

$$(0, 0, 0, 0) \longleftrightarrow \mathbb{Z}[\omega, \theta]/(\omega^2, \theta^2, \omega\theta), \tag{18}$$

$$(a, b, c, d) \longleftrightarrow \mathbb{Z}[a\omega, a\omega^2 + b\omega]/(a\omega^3 + b\omega^2 + c\omega + d) \quad \text{si } a \neq 0. \tag{19}$$

Zagier [58] a donné une jolie interprétation de l'application réciproque, en associant à R l'application

$$\begin{aligned} \Phi_{3,2} : R/\mathbb{Z} &\longrightarrow \Lambda^3 R \cong \mathbb{Z} \\ \xi &\longmapsto 1 \wedge \xi \wedge \xi^2, \end{aligned}$$

que l'on identifie à une forme cubique en choisissant une base $\langle \alpha, \beta \rangle$ du $\mathbb{Z}$-module $R/\mathbb{Z}$ de rang 2 et en posant $\xi = x\alpha + y\beta$. La construction est bien définie modulo $\mathrm{GL}_2(\mathbb{Z})$.

5.2. Paramétrisations cubiques

L'espace $V_{\mathbb{Z}} = \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ peut se représenter comme l'ensemble des boîtes $2 \times 3 \times 3$ à sommets entiers, ou encore les paires (A, B) de matrices 3×3. De façon analogue au § 4.1, on le munit d'une action de $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$. On se restreint à $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ puisque $(-\mathrm{Id}_2, \mathrm{Id}_3, -\mathrm{Id}_3)$ et $(-\mathrm{Id}_2, -\mathrm{Id}_3, \mathrm{Id}_3)$ agissent trivialement (cette action est fidèle). Soit $f(x, y)$ la forme cubique binaire $\det(xA - yB)$, on note

$$\mathrm{Disc}((A, B)) = \mathrm{Disc}(\det(xA - yB)) = \mathrm{Disc}(f),$$

qui est l'unique $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-invariant sur $V_{\mathbb{Z}}$. D'après le Théorème 5.1, on associe un ordre cubique R de discriminant $\mathrm{Disc}(f)$ à f.

THÉORÈME 5.2. — *Il y a une bijection canonique entre*

– *l'ensemble des* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$*-orbites de discriminant* $D \neq 0$ *sur* $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$*,*

– *l'ensemble des classes d'isomorphismes de paires* $(R, (I, I'))$*, où* R *est un anneau cubique de discriminant* $D \neq 0$*, et* (I, I') *est une classe d'équivalence de paires équilibrées de* R*-idéaux fractionnaires de* $R \otimes \mathbb{Q}$*.*

THÉORÈME 5.3. — *Il y a une bijection canonique entre*

– *l'ensemble des* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$*-orbites de discriminant* $D \neq 0$ *sur* $\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3$*,*

– *l'ensemble des classes d'isomorphismes de triplets* (R, I, δ)*, où* R *est un anneau cubique de discriminant* $D \neq 0$*,* I *est un* R*-idéal et* δ *est un élément inversible de* $R \otimes \mathbb{Q}$*, tels que* $I^2 \subset (\delta)$*,* $\mathrm{N}(\delta) = \mathrm{N}(I)^2$*.*

Tout comme au § 4, on obtient des applications naturelles

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3 \longrightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \longrightarrow \mathbb{Z}^2 \otimes \Lambda^2 \mathbb{Z}^6,$$

munies d'actions de $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$, $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ et $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$, respectivement. Restreintes à des sous-espaces convenables et modulo ces actions, elles deviennent des morphismes de groupes. Par exemple, pour R fixé et I, I' projectifs comme R-modules (*i.e.* inversibles), la restriction de la bijection du Théorème 5.2 associe à $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ la classe d'idéaux de I. C'est un isomorphisme sur le groupe des classes des R-idéaux inversibles $\mathrm{Cl}(R)$.

5.3. Les cas quartiques et quintiques

La paramétrisation des anneaux quartiques requiert de nouveaux préliminaires.

DÉFINITION 5.4. — *Pour un anneau* R *de degré* n*, soit* I_R *l'idéal de* $R^{\otimes n}$ *engendré par les éléments de la forme*

$$(x \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes x \otimes \cdots \otimes 1) + \cdots + (1 \otimes 1 \otimes \cdots \otimes x) - \mathrm{Tr}(x) \times (1 \otimes \cdots \otimes 1).$$

La S_n-clôture $\widehat{R}$ de R est l'anneau de degré $n!$ donné par $\widehat{R} = M/M_{tor}$, où $M := R^{\otimes n}/I_R$ et M_{tor} est le sous-groupe de torsion de M.

Si R est intègre de corps des fractions K, $\widehat{R}$ est la $\mathbb{Z}$-algèbre engendrée par les conjugués des éléments de R et son corps des fractions $\mathrm{Frac}(\widehat{R})$ est une clôture galoisienne de $K/\mathbb{Q}$. On fixe un plongement $x \mapsto (x \otimes 1 \otimes \cdots \otimes 1)$ de R dans $\widehat{R}$. Les *n conjugués* de x sont les $(x \otimes 1 \otimes \cdots \otimes 1), \ldots, (1 \otimes 1 \otimes \cdots \otimes x)$. Il y a une action naturelle du groupe symétrique S_n sur $\widehat{R}$ et $\widehat{R}^{S_n} = \mathbb{Z} \otimes \cdots \otimes \mathbb{Z} = \mathbb{Z}$.

Définition 5.5. — *Soit Q un anneau quartique de S_4-clôture $\widehat{Q}$. Pour $x \in Q$, on note x, x', x'', x''' ses S_4-conjugués et on définit $\Phi_{4,3} : Q \to \widehat{Q}$ par $\Phi_{4,3}(x) = xx' + x''x'''$. On note*

$$R^{\mathrm{inv}}(Q) = \mathbb{Z}[\,\{\Phi_{4,3}(x) \colon x \in Q\}\,] \subset \widehat{Q}.$$

On démontre que $R^{\mathrm{inv}}(Q)$ est inclus dans un anneau cubique, le sous-anneau de $\widehat{R}$ fixe par un sous-groupe $D_4 \subset S_4$ diédral d'ordre 8.

Définition 5.6. — *Soit Q un anneau quartique. Une résolvante cubique de Q est un anneau cubique R tel que $\mathrm{Disc}(R) = \mathrm{Disc}(Q)$ et $R^{\mathrm{inv}}(Q) \subset R$.*

Bhargava a aussi donné une description plus fonctorielle des résolvantes cubiques qui n'utilise pas la notion de S_n-clôture. L'idée est de voir une résolvante cubique R d'un anneau quartique Q comme un anneau cubique muni d'une application quadratique $\Phi_{4,3} : Q \to R$ satisfaisant des propriétés formelles convenables.

Théorème 5.7. — *Tout anneau quartique admet au moins une résolvante cubique R, qui est unique si et seulement si Q est « de contenu 1 », c'est-à-dire si $Q/\mathbb{Z}$ n'est pas de la forme $n(Q'/\mathbb{Z})$ pour un $n > 1$ et un anneau quartique Q'. Dans ce cas, $R = R^{\mathrm{inv}}(Q)$.*

Si R est une résolvante cubique de Q, $\Phi_{4,3}$ induit une application quadratique de $Q/\mathbb{Z}$ dans $R/\mathbb{Z}$, c'est-à-dire de $\mathbb{Z}^3$ dans $\mathbb{Z}^2$ aux changements de base près. C'est donc une paire de formes quadratiques ternaires modulo $\Gamma = \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$. Explicitement $(g_3, g_2) \in \Gamma$ opère sur $(A, B) \in \mathbb{Z}^2 \otimes (\mathrm{Sym}^3 \mathbb{Z}^2)^*$, où A, B sont vues comme matrices symétriques 3×3 à coefficients demi-entiers en dehors de la diagonale, par

$$(g_3, g_2) \cdot (A, B) = (r \cdot g_3 A g_3^t + s \cdot g_3 B g_3^t,\ t \cdot g_3 A g_3^t + u \cdot g_3 B g_3^t),$$

avec $g_2 = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. Soit f la forme cubique binaire $4 \det(xA - yB)$ — le facteur 4 assure l'intégralité. La forme f est invariante sous l'action du facteur $\mathrm{GL}_3(\mathbb{Z})$ de Γ, et le facteur $\mathrm{GL}_2(\mathbb{Z})$ agit via $\left(\begin{smallmatrix} r & -s \\ -t & u \end{smallmatrix}\right) \cdot f$. L'action de Γ a un unique invariant $\mathrm{Disc}((A, B)) := \mathrm{Disc}(f)$.

Théorème 5.8. — *Il existe une bijection entre les ensembles suivants :*

– *les paires de formes quadratiques ternaires (A, B) de discriminant $\mathrm{Disc}((A, B)) = D$, soit $\mathbb{Z}^2 \otimes (\mathrm{Sym}^2 \mathbb{Z}^3)^*$, modulo l'action de $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$,*

– *les classes d'isomorphismes de triplets* (Q, R, Φ)*, où* Q*,* R *sont des anneaux respectivement quartique et cubique,* $\Phi : Q/\mathbb{Z} \to R/\mathbb{Z}$ *est une application quadratique,* R *est une résolvante cubique de* Q *et* $\operatorname{Disc} Q = \operatorname{Disc} R = D$*. La classe d'isomorphisme de* R *est donnée par la* $\mathrm{GL}_2(\mathbb{Z})$*-orbite de la forme cubique binaire* $f(x, y) = 4\det(xA - yB)$*.*

On notera $Q(A, B)$ l'anneau quartique associé à la paire (A, B). Ce théorème est un analogue du cas cubique, qui associe à un anneau cubique R de discriminant D, une résolvante quadratique $S(D)$ et une application cubique $\Phi_{3,2} : R/\mathbb{Z} \to S/\mathbb{Z}$. Ces deux données étant entièrement déterminées par R, elles n'apparaissaient pas explicitement. Dans la paramétrisation ci-dessus, Φ est en fait déterminée par Q et R si leur discriminant commun est non-nul. De surcroît, comme nous l'avons vu au Théorème 5.7, Q de contenu 1 détermine R.

Ce théorème se démontre « explicitement » comme le Théorème 4.6, la grande difficulté venant du fait qu'il n'y a pas de choix naturel pour la résolvante cubique R. Pour un choix particulier d'un représentant (A, B) dans la classe modulo $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$, Bhargava montre que la structure multiplicative de Q et R est fixée, en écrivant explicitement des lois de multiplication génériques analogues à (17), et en résolvant les conditions de compatibilité, associativité, commutativité, au terme d'un processus où le mot « miracle » apparaît plusieurs fois [2]. On vérifie que R est bien une résolvante cubique de Q, et que (Q, R) a bien pour image (A, B).

Bhargava [3, 4] annonce d'autres paramétrisations, dont le résultat suivant :

THÉORÈME 5.9. — *Il existe une bijection entre les ensembles suivants :*

– *les quadruplets de* 2*-formes alternées de rang* 5*, soit* $\mathbb{Z}^4 \otimes \Lambda^2\mathbb{Z}^5$*, modulo l'action de* $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$*,*

– *les paires* $(P, \mathcal{S})$*, où* P *est une classe d'isomorphisme d'anneaux quintiques, et* $\mathcal{S}$ *est une résolvante sextique de* P*.*

Cette bijection préserve le discriminant.

6. COMPTAGES PAR DISCRIMINANT ET DENSITÉS

6.1. La conjecture de Malle

Soit k un corps de nombres dont on fixe une clôture algébrique $\overline{k}$, $G \subset S_n$ un groupe de permutations sur n lettres et K/k une extension finie de degré $[K : k] = n$. Par abus de notation, on écrit « $\mathrm{Gal}(K/k) = G$ » si le groupe de Galois de la clôture galoisienne de K/k, vu comme groupe de permutation sur les n k-plongements de K dans $\overline{k}$, est isomorphe à G. Soit

$$\mathcal{F}_{n,k}(X, G) = \left\{K/k \colon K \subset \overline{k}, \mathrm{Gal}(K/k) = G, \mathrm{N}_{k/\mathbb{Q}}(d_{K/k}) \leqslant X\right\} \big/ \mathrm{Gal}(\overline{k}/k),$$

l'ensemble des classes d'isomorphismes d'extensions de k de groupe de Galois G, au sens précédent, dont la norme du discriminant relatif $d_{K/k}$ est bornée par X. On note

$$N_{n,k}(X,G) := \sum_{K\in\mathcal{F}_{n,k}(X,G)} \frac{1}{\#\operatorname{Aut}_k K}.$$

La pondération par le nombre d'automorphismes, qui ne dépend que de k et G, nous permettra de formuler plus naturellement certaines densités.

DÉFINITION 6.1. — *Pour $\sigma \in S_n$, on définit l'*indice *de σ par*

$$\operatorname{ind}(\sigma) := n - \#\{\textit{cycles de } \sigma\}$$

(*il ne dépend que de la classe de conjugaison de σ*). *Si $G \neq \{\mathrm{Id}\}$ est un sous-groupe de S_n, on note*

$$\operatorname{ind}(G) := \min_{\sigma\in G-\{\mathrm{Id}\}} \operatorname{ind}(\sigma), \quad a(G) = 1/\operatorname{ind}(G) \in]0,1].$$

On note $b(G,k) \geqslant 1$ le nombre de k-classes de conjugaison de G, c'est-à-dire de classes modulo l'action naturelle de $\mathrm{Gal}(\overline{k}/k)$, *dont l'indice est* $\operatorname{ind}(G)$.

En particulier, $a(G) = 1$ si et seulement si G contient une transposition ; dans ce cas, $b(G,k) = 1$ pour tout corps de nombres k (Malle [38]). Malle [38, 39] conjecture[(5)] une estimation relativement précise pour $N_{n,k}(X,G)$:

CONJECTURE 6.2. — *Soit G un groupe de permutation transitif et k un corps de nombres. Il existe une constante $c(G,k) > 0$ telle que*

$$N_{n,k}(X,G) \sim c(G,k) X^{a(G)} (\log X)^{b(G,k)-1}.$$

On en déduit que le nombre $N_{n,k}(X) = \sum_{G\subset S_n} N_{n,k}(X,G)$ d'extensions de k de degré n dont on ne fixe plus le groupe de Galois vérifierait

$$N_{n,k}(X) \overset{?}{\sim} X \cdot \sum_{\substack{G\subset S_n \\ a(G)=1}} c(G,k).$$

Bien sûr, cette conjecture implique une solution positive au problème de Galois inverse. Malle conjecture qu'en fixant la structure de k_v-algèbre de $K \otimes k_v$ pour un nombre fini de places v de k, on garde les mêmes exposants (mais la constante change) pour peu qu'au moins une telle extension K existe. Les $c(G,k)$ ne sont pas précisés par la conjecture.

(5) (06/03/2005) : Klüners a depuis trouvé un contre-exemple à la conjecture de Malle (Note aux CRAS, à paraître).

Celle-ci est démontrée si G est abélien[6] (Mäki [37], Wright [55]) ou de petit cardinal : $n = 3$ et $G = S_3$ (Davenport et Heilbronn [21], Datskovsky et Wright [18]), $n = 4$ et $G = D_4$ (Cohen, Diaz y Diaz, Olivier [12] ; malgré le titre, le cas $k \neq \mathbb{Q}$ est traité). Voir [11] pour un survol plus détaillé.

Citons pour finir trois résultats récents. Pour un groupe G nilpotent en représentation régulière, Klüners et Malle [34] obtiennent la forme faible

$$\lim_{X\to+\infty} \frac{\log N_{|G|,k}(X,G)}{\log X} = a(G).$$

Klüners [33] a récemment annoncé que les groupes quaternioniens généralisés

$$Q_{4m} := \langle x, y \mid x^{2m} = 1, y^2 = x^m, y^{-1}xy = x^{-1}\rangle, \quad m = 2^l,\ l \geqslant 1,$$

vérifient la conjecture sur $k = \mathbb{Q}$, fournissant les premiers exemples non abéliens d'ordre arbitrairement élevé ; ici $G = Q_{4m} \subset S_{4m}$ est en représentation régulière, $a(G) = 2m$ et $b(G, \mathbb{Q}) = 1$. Le résultat le plus général à ce jour, dû à Ellenberg et Venkatesh [24] dit que pour tout $\varepsilon > 0$, tout $n \geqslant 1$, et tout corps de nombres k, on a

$$\limsup_{X\to+\infty} \frac{\log N_{n,k}(X)}{\log X} \ll_\varepsilon n^\varepsilon \quad \text{et} \quad \liminf_{X\to+\infty} \frac{\log N_{n,k}(X)}{\log X} \geqslant \frac{1}{2} + \frac{1}{n^2}$$

6.2. La conjecture de Bhargava

Pour v une place de k et $n \geqslant 1$, on définit

$$a_v(n) := \sum_{\substack{A \text{ étale}/k_v \\ [A:k_v]=n}} \frac{\left|d_{A/k_v}\right|_v}{\#\mathrm{Aut}_{k_v} A}$$

où la somme porte sur les classes d'isomorphismes d'algèbres étales de degré n sur le complété k_v. Ici, d_{A/k_v} est le discriminant associé (1 pour v archimédienne), et $|\cdot|_v$ désigne la valeur absolue normalisée habituelle.

Conjecture 6.3 (Bhargava). — *Pour $n \geqslant 2$, on a $N_{n,k}(X, S_n) \sim c(S_n, k)X$ quand $X \to +\infty$, avec*

$$c(S_n, k) = \frac{1}{2}\,\mathrm{Res}(\zeta_k, s = 1) \prod_v a_v(n)(1 - 1/\mathrm{N}\,v) \tag{20}$$

où ζ_k est la fonction zêta de Dedekind de k, et où on omet le facteur $(1-1/\mathrm{N}\,v)$ pour v archimédienne.

(Il s'agit d'une reformulation d'une conjecture équivalente donnée par Bhargava [4].)

[6] Si G est abélien de cardinal n, $G \subset S_n$, p le plus petit diviseur premier de n, n_p le nombre d'éléments d'ordre p dans G, on montre que

$$1/a(G) = |G|(1 - 1/p) \quad \text{et} \quad b(G, k) = n_p/\big[k(e^{2i\pi/p}) : k\big].$$

Comme les algèbres étales sur k_v sont les produits finis de corps sur k_v et que leurs k_v-automorphismes et discriminants sont les produits de ceux de leurs composantes, on obtient l'expression de la série génératrice

$$\sum_n a_v(n)T^n = \exp\left(\sum_{K \text{ corps}/k_v} \frac{\left|d_{K/k_v}\right|_v}{\#\mathrm{Aut}_{k_v} K}\, T^{[K:k_v]}\right). \tag{21}$$

THÉORÈME 6.4. — *On a*

$$\sum_n a_v(n)T^n = \begin{cases} \exp(T) & \text{si } v \text{ est complexe,} \\ \exp\left(T + \frac{1}{2}T^2\right) & \text{si } v \text{ est réelle,} \\ \prod_{k=1}^{+\infty} \dfrac{1}{1-q^{k-1}T^k} & \text{si } v \text{ est finie, } q = (\mathrm{N}\, v)^{-1}. \end{cases}$$

Démonstration. — Les deux premiers cas sont clairs à partir de (21), le troisième résulte de la formule de masse de Serre [47], sous la forme

$$\sum_{\substack{K \text{ corps}/k_v \\ [K:k_v]=n}} \frac{\left|d_{K/k_v}\right|_v}{\#\mathrm{Aut}_{k_v} K} = \sum_{d|n} \frac{q^{n-d}}{d}.$$

La formule donnée dans [47] énonce que la somme sur les extensions totalement ramifiées est q^{n-1}. Pour chaque $d \mid n$, on l'applique à l'unique extension non ramifiée de degré d de k_v, pour compter ses extensions totalement ramifiées de degré n/d. □

COROLLAIRE 6.5. — *Si v est finie, $q = (\mathrm{N}\, v)^{-1}$, alors $a_v(n) = P_n(q)$ où $P_n \in \mathbb{N}[X]$ ne dépend pas de v. On a $P_n(q) = 1 + q + O(q^2)$ quand $q \to 0$ et le produit infini* (20) *converge.*

Exemple 6.6. — Pour v réelle,

$$a_v(2) = 1, \quad a_v(3) = 2/3, \quad a_v(4) = 5/12, \quad a_v(5) = 13/60.$$

Pour v finie, $q = (\mathrm{N}\, v)^{-1}$, on obtient

$$(1-q)a_v(2) = 1 - q^2, \qquad (1-q)a_v(4) = 1 + q^2 - q^3 - q^4,$$
$$(1-q)a_v(3) = 1 - q^3, \qquad (1-q)a_v(5) = 1 + q^2 - q^4 - q^5.$$

Exemple 6.7. — Si $n = 2$, la conjecture prédit

$$N_{\mathbb{Q},2}(X, S_2)/X \longrightarrow \frac{1}{2\zeta(2)},$$

ce qui est un résultat classique. On le démontre par exemple à partir de l'identité $\mu^2(q) = \sum_{d^2|q} \mu(d)$ d'où on déduit la densité des entiers sans facteur carré. (Ne pas oublier que chaque corps est pondéré par $1/\#\,\mathrm{Aut}_{\mathbb{Q}}(K) = 1/2$.)

La conjecture suit du principe heuristique suivant, analogue à celui de Cohen-Lenstra [14] et Cohen-Martinet [15] sur le comportement moyen des groupes de classes. On considère le nombre d'extensions K/k de degré n, avec $\mathrm{Gal}(K/k)=S_n$ et $d_{K/k}=D$. En se demandant quelles collections de $A=K\otimes k_v$ peuvent intervenir et en supposant les comportements indépendants aux différentes places, on s'attend à ce qu'il soit égal à

$$\prod_v \sum_{\substack{A \text{ étale}/k_v \\ [A:k_v]=n \\ |d_{A/k_v}|_v=|D|_v}} \frac{1}{\#\mathrm{Aut}_{k_v} A},$$

en moyenne sur D. La conjecture est vraie pour $n=2$ (Wright [55], Cohen-Diaz y Diaz-Olivier [13]), $n=3$ (Datskovsky-Wright [18]), et correspond aux valeurs annoncées par Bhargava sur $\mathbb{Q}$ pour $n=4,5$. Une variation évidente fixe la structure de k_v-algèbre de $K\otimes k_v$ pour un nombre fini de places, par exemple la signature à l'infini : on remplace les $a_v(n)$ correspondants par la somme sur les algèbres de structure permise. Cette conjecture renforcée est vérifiée dans les mêmes cas que ci-dessus (voir [18, § 4] pour $n=2,3$).

6.3. S_3 sur $\mathbb{Q}$

Ce cas, réinterprété et étendu dans le langage du § 3.3 par Datskovsky et Wright [54, 17, 18], est originellement traité sur $\mathbb{Q}$ par Davenport et Heilbronn [21] avec la méthode du domaine fondamental du § 2. À partir du Théorème 5.1, un équivalent de $N_{\mathbb{Q},3}(X,S_3)$ s'obtient assez simplement : on compte les classes de formes cubiques associées aux ordres maximaux, une condition locale qui prend la forme suivante.

THÉORÈME 6.8 (Davenport-Heilbronn). — *La classe d'une forme cubique irréductible F est associée à un ordre R maximal en p (c'est-à-dire tel que $R\otimes\mathbb{Z}_p$ est maximal) si et seulement si $p\nmid F$ et F n'est pas $\mathrm{GL}_2(\mathbb{Z})$-équivalente à une forme (a,b,pc,p^2d), $a,b,c,d\in\mathbb{Z}$.*

Ce n'est pas la formulation de Davenport et Heilbronn [21], qui ne connaissaient pas le résultat de Delone et Faddeev et faisaient des calculs locaux désagréables, mais elle lui est équivalente.

Démonstration. — Si $p\mid F$, R est inclus dans l'ordre associé à F/p, donc non maximal en p. Si p ne divise pas le discriminant de F, égal à $\mathrm{Disc}\,R$, il n'y a pas de problème. Sinon, en remplaçant au besoin F par une forme $\mathrm{GL}_2(\mathbb{Z})$-équivalente, on peut supposer que la racine double de F modulo p est en 0, et qu'il n'y a pas de racine à l'infini soit $F=(a,b,pc,pd)$, avec $p\nmid a$. Le résultat suit du critère de p-maximalité de Dedekind (*cf.* [10, § 6.1.4]).

Explicitement, si $p\mid d$, l'ordre associé à $(pa,b,c,d/p)$ contient R (voir (19)). □

Posons $G = \mathrm{GL}_2$, $V = \mathrm{Sym}^3 \mathbb{A}^2$; il suffit de compter les points de $V_\mathbb{Z}/G_\mathbb{Z}$ de discriminant borné, satisfaisant les congruences ci-dessus. En effet, les points associés à des anneaux non intègres ou de corps des fractions cubiques cycliques sont absorbés dans un terme d'erreur. On trouve

$$\mathrm{Vol}(V_\mathbb{R}/G_\mathbb{Z} \cap \{F : |\mathrm{Disc}\, F| < X\}) = \left(\frac{1}{2} + \frac{1}{6}\right) \frac{\zeta(2)}{2} X = \frac{\zeta(2)}{3} X,$$

en séparant les deux composantes connexes de $(V - S)_\mathbb{R} = V^+ \cup V^-$ associées aux formes de discriminant respectivement positif ou négatif[(7)]. Le produit des densités p-adiques provenant du Théorème 6.8 est $1/(\zeta(2)\zeta(3))$, et l'on obtient

$$N_{\mathbb{Q},3}(X, S_3)/X \longrightarrow \frac{1}{3\zeta(3)} = \frac{1}{2} \mathrm{Res}(\zeta, s = 1)\, a_\infty(3) \prod_p (1 - 1/p) a_p(3).$$

On peut bien sûr séparer les densités des corps totalement réels et totalement complexes, la première étant trois fois plus faible que la seconde, en se restreignant à V^+ ou V^- au lieu d'additionner leurs contributions.

6.4. S_4 et S_5 sur $\mathbb{Q}$

Pour ce qui concerne S_4 et S_5 sur $\mathbb{Q}$, seul le cas des corps S_4 totalement réels est publié [2] à ce jour. Bhargava [4] annonce une solution complète qui corrobore sa conjecture pour $n = 4, 5$.

Définition 6.9. — *Une paire de formes quadratiques ternaires (A, B) est* totalement réelle*, resp.* mixte*, resp.* totalement complexe *si (A, B) a 4, resp. 2, resp. 0 zéros réels dans $\mathbb{P}^2(\mathbb{R})$. Elle est* irréductible *si A et B n'ont pas de zéro commun dans $\mathbb{P}^2(\mathbb{Q})$ et si la forme cubique binaire $\det(xA - yB)$ est irréductible sur $\mathbb{Q}$. Une paire (A, B) est* maximale *si l'anneau quartique $Q(A, B)$ est maximal.*

Toutes ces définitions ne dépendent que de la classe de (A, B) modulo $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ et on a une description locale, analogue au Théorème 6.8, des paires (A, B) *maximales.*

Théorème 6.10. — *Soit $Q(A, B)$ l'anneau quartique associé à une classe de paires de formes quadratiques (A, B) :*

– *(A, B) est irréductible si et seulement si $Q(A, B)$ est un ordre d'une extension quartique de $\mathbb{Q}$ de clôture galoisienne A_4 ou S_4.*

– *(A, B) est totalement réelle si et seulement si Q est totalement réel ($Q \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{R}^4$).*

– *(A, B) est totalement réelle irréductible maximale si et seulement si $Q(A, B)$ est un ordre quartique maximal, dont le corps des fractions est totalement réel, de clôture galoisienne A_4 ou S_4 sur $\mathbb{Q}$.*

(7) V^+ (resp. V^-) correspond aux formes ayant trois racines réelles (resp. une seule racine réelle), dont le stabilisateur dans $\mathrm{GL}_2(\mathbb{R})$ est isomorphe à S_3 (resp. à S_2). D'où les coefficients 1/6 et 1/2.

– *Le produit des densités locales associées aux* (A, B) *maximales est*

$$\frac{1}{\zeta(2)^2\zeta(3)}\prod_p(1+p^{-2}-p^{-3}-p^{-4}).$$

On trouve cette fois-ci

$$\mathrm{Vol}(V_{\mathbb{R}}/G_{\mathbb{Z}}\cap\{(A,B):|\mathrm{Disc}(A,B)|<X\})=\left(\frac{1}{24}+\frac{1}{4}+\frac{1}{8}\right)\frac{\zeta(2)^2\zeta(3)}{2}X,$$

où $V_{\mathbb{R}}=\mathbb{R}^2\otimes\mathrm{Sym}^2\,\mathbb{R}^3$, $G_{\mathbb{Z}}=\mathrm{GL}_2(\mathbb{Z})\times\mathrm{GL}_3(\mathbb{Z})$, et les coefficients 1/24, 1/4, 1/8 proviennent respectivement des cas réels, mixtes et complexes (stabilisateurs S_4, S_2^2 et S_2^3) qui sont les trois composantes connexes de $(V-S)_{\mathbb{R}}$.

THÉORÈME 6.11. — *Conformément à la conjecture de Bhargava, le nombre de classes d'isomorphismes de corps quartiques* totalement réels *de discriminant inférieur à* X *est équivalent à* CX*, où*

$$C=\frac{1}{2}\times\frac{1}{24}\times\prod_p a_4(p)(1-1/p).$$

Démonstration. — Ce théorème suit formellement de ce qui précède, en montrant que sont négligeables

– le nombre d'extensions A_4 de discriminant inférieur à X,

– les points associés aux (A, B) réductibles,

– le terme reste algébrique lié au passage à la limite dans le produit des facteurs locaux (analogue de (4)),

– le terme géométrique provenant du principe de Lipschitz (Théorème 2.2), lié aux volumes des projections d'un domaine fondamental.

Wong [53, Remark 9] démontre que $N_{\mathbb{Q},4}(X, A_4) = O(X^{7/8+\varepsilon})$ pour tout $\varepsilon > 0$, et les trois autres points sont démontrés par Bhargava. Le deuxième est de loin le plus délicat, faisant hélas appel à un domaine fondamental explicite et à de lourdes estimations directes (en dimension 12). Parmi les points entiers du domaine fondamental, les paires réductibles sont en fait largement majoritaires ; elles sont heureusement concentrées sur quelques sections hyperplanes qui peuvent être éliminées avant le décompte par principe de Lipschitz. □

L'hypothèse « totalement réel » et le domaine fondamental explicite qu'elle permet sont utilisés pour traiter un cas dégénéré mais crucial. Je ne sais pas si Bhargava les supprime pour traiter les deux autres signatures possibles ou bien s'il doit refaire tous les calculs.

Si K est un corps de nombres et p un nombre premier, soit

$$r_p(K)=\dim_{\mathbb{F}_p}\left(\mathrm{Cl}(K)\otimes_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z})\right)$$

le p-rang du groupe des classes de K ; ainsi, $p^{r_p(K)}$ est le nombre d'éléments de p-torsion du groupe des classes, et $(p^{r_p(K)}-1)/(p-1)$ le nombre de sous-groupes

d'indice p. La méthode de Davenport et Heilbronn du § 6.3 permet la détermination de l'ordre moyen de $3^{r_3(K)}$ quand K parcourt les corps quadratiques, et la vérification de l'heuristique de Cohen-Lenstra dans ce cadre. Bhargava obtient l'analogue suivant :

THÉORÈME 6.12. — *Conformément aux heuristiques de Cohen-Martinet, on a*

$$\sum_K \left(2^{r_2(K)} - 1\right) \sim \frac{1}{4} \sum_K 1, \quad \textit{quand } X \longrightarrow \infty,$$

où K parcourt les corps cubiques totalement réels *de discriminant inférieur à X.*

Démonstration. — Soit K_4 un corps quartique de type A_4 ou S_4, de clôture galoisienne L, $K_3 \subset L$ un corps cubique, et K_6 l'unique extension quadratique de K_3 dont la clôture galoisienne soit L. Alors K_6/K_3 est ramifiée en une place divisant p si et seulement si le type de ramification de p dans K_4 est (1^4), (2^2), ou $(1^2 2^2)$. Le corps K_4 est totalement réel si et seulement si L l'est, ce qui implique que K_3 et K_6 le sont aussi.

Réciproquement si K_3 est un corps cubique totalement réel et si K_6/K_3 est une extension quadratique non ramifiée, alors la clôture galoisienne L de K_6 est de type A_4 ou S_4 et contient un unique corps quartique K_4 à conjugaison près, et K_4 est totalement réel puisque K_6 et donc L le sont. Par théorie du corps de classes, $2^{r_2(K)} - 1$ est le nombre d'extensions quadratiques non ramifiées K_6 de K_3. On vérifie par ailleurs que $\operatorname{Disc} K_3 = \operatorname{Disc} K_4$. Le membre de gauche compte donc les extensions K_4 totalement réelles de type A_4 ou S_4 et de ramification restreinte comme ci-dessus.

Bhargava démontre que, pour $Q(A, B)$ maximal, la structure de l'anneau quotient $Q(A, B)/(p)$ est donnée par les degrés résiduels aux points d'intersections des deux coniques définies par A et B sur $\mathbb{F}_p$. (Le résultat reste vrai pour $Q(A, B)$ non-maximal, s'il n'y a pas de point d'intersection quadruple.) En particulier le type de décomposition d'un premier p dans le corps des fractions K_4 de $Q(A, B)$ se voit par des congruences modulo p sur (A, B). En renforçant la condition locale de p-maximalité de la démonstration précédente pour imposer l'absence de ramification de type (1^4), (2^2) ou $(1^2 2^2)$, on obtient un équivalent du membre de gauche. Le théorème de Davenport-Heilbronn démontré au § 6.3 donne un équivalent du membre de droite. □

RÉFÉRENCES

[1] K. BELABAS – « Crible et 3-rang des corps quadratiques », *Ann. Inst. Fourier (Grenoble)* **46** (1996), p. 909–949.

[2] M. BHARGAVA – « Higher composition laws », Thèse, Princeton University, 2001.

[3] ———, « Gauss composition and generalizations », in *Ants V, Sydney*, Lecture Notes in Comput. Sci., no. 2369, Springer-Verlag, 2002, p. 1–9.

[4] ———, « The parametrization of algebraic structures », *Explicit Methods in Number Theory* (Oberwolfach). Exposé, 2003.

[5] ———, « Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations », *Ann. of Math. (2)* **159** (2004), no. 1, p. 217–250.
[6] ———, « Higher composition laws. II. On cubic analogues of Gauss composition », *Ann. of Math. (2)* **159** (2004), no. 2, p. 865–886.
[7] ———, « Higher composition laws. III. The parametrization of quartic rings », *Ann. of Math. (2)* **159** (2004), no. 3, p. 1329–1360.
[8] D.A. Buell – *Binary quadratic forms*, Springer-Verlag, 1989.
[9] F. Chamizo & H. Iwaniec – « On the Gauss mean-value formula for class number », *Nagoya Math. J.* **151** (1998), p. 199–208.
[10] H. Cohen – *A course in computational algebraic number theory*, 3e éd., Springer-Verlag, 1996.
[11] ———, « Constructing and counting number fields », in *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)* (Beijing), Higher Ed. Press, 2002, p. 129–138.
[12] H. Cohen, F. Diaz y Diaz & M. Olivier – « Enumerating quartic dihedral extensions of $\mathbb{Q}$ », *Compositio Math.* **133** (2002), no. 1, p. 65–93.
[13] ———, « On the density of discriminants of cyclic extensions of prime degree », *J. reine angew. Math.* **550** (2002), p. 169–209.
[14] H. Cohen & H.W. Lenstra, Jr. – « Heuristics on class groups of number fields », in *Number theory, Noordwijkerhout 1983*, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, p. 33–62.
[15] H. Cohen & J. Martinet – « Études heuristiques des groupes de classes des corps de nombres », *J. reine angew. Math.* **404** (1990), p. 39–76.
[16] D. Cox – *Primes of the form $x^2 + ny^2$*, Wiley-Interscience, 1989.
[17] B. Datskovsky & D.J. Wright – « The adelic zeta function associated to the space of binary cubic forms. II. Local theory », *J. reine angew. Math.* **367** (1986), p. 27–75.
[18] ———, « Density of discriminants of cubic extensions », *J. reine angew. Math.* **386** (1988), p. 116–138.
[19] B.A. Datskovsky – « On Dirichlet series whose coefficients are class numbers of binary quadratic forms », *Nagoya Math. J.* **142** (1996), p. 95–132.
[20] H. Davenport – « On a principle of Lipschitz », *J. London Math. Soc.* **26** (1951), p. 179–183, corrigendum *ibid* **39** (1964), p. 580.
[21] H. Davenport & H. Heilbronn – « On the density of discriminants of cubic fields (ii) », *Proc. Roy. Soc. London Ser. A* **322** (1971), p. 405–420.
[22] B.N. Delone & D.K. Faddeev – *The theory of irrationalities of the third degree*, Translations of Math. Monographs, vol. 10, American Mathematical Society, 1964.
[23] G. Eisenstein – « Untersuchungen über die cubischen Formen mit zwei Variabeln », *J. reine angew. Math.* **27** (1844), p. 89–104.
[24] J. Ellenberg & A. Venkatesh – « The number of extensions of a number field with fixed degree and bounded discriminant », *Ann. of Math.*, à paraître.
[25] W.T. Gan, B. Gross & G. Savin – « Fourier coefficients of modular forms on G_2 », *Duke Math. J.* **115** (2002), no. 1, p. 105–169.

[26] D. Goldfeld & J. Hoffstein – « Eisenstein series of $\frac{1}{2}$-integral weight and the mean value of real Dirichlet L-series », *Invent. Math.* **80** (1985), no. 2, p. 185–208.

[27] J.W. Hoffman & J. Morales – « Arithmetic of binary cubic forms », *Enseign. Math. (2)* **46** (2000), no. 1-2, p. 61–94.

[28] M.N. Huxley – « Integer points, exponential sums and the Riemann zeta function », in *Number theory for the millennium, II (Urbana, IL, 2000)*, AK Peters, Natick, MA, 2002, p. 275–290.

[29] J.-i. Igusa – *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, American Mathematical Society, Providence, RI, 2000.

[30] A.C. Kable & A. Yukie – « Prehomogeneous vector spaces and field extensions. II », *Invent. Math.* **130** (1997), no. 2, p. 315–344.

[31] M. Kashiwara – « B-functions and holonomic systems. Rationality of roots of B-functions », *Invent. Math.* **38** (1976/77), no. 1, p. 33–53.

[32] T. Kimura – « The b-functions and holonomy diagrams of irreducible regular prehomogeneous vector spaces », *Nagoya Math. J.* **85** (1982), p. 1–80.

[33] J. Klüners – « On the asymptotics of number fields with given Galois group », 2003, *Explicit Methods in Number Theory* (Oberwolfach). Exposé.

[34] J. Klüners & G. Malle – « Counting nilpotent Galois extensions », *J. reine angew. Math.*, à paraître.

[35] P.G. Lejeune Dirichlet – *Vorlesungen über Zahlentheorie*, Herausgegeben und mit Zusätzen versehen von R. Dedekind. Vierte, umgearbeitete und vermehrte Auflage, Chelsea Publishing Co., New York, 1968.

[36] R. Lipschitz – « Über die asymptotischen Gesetze von gewissen Gattungen zahlentheoretischer Funktionen », *Monatsber. der Berl. Acad* (1865), § 174sqq.

[37] S. Mäki – *On the density of abelian number fields*, Ann. Acad. Sci. Fenn. Ser. A I Math. Dissertationes, vol. 54, 1985.

[38] G. Malle – « On the distribution of Galois groups », *J. Number Theory* **92** (2002), no. 2, p. 315–329.

[39] ———, « On the distribution of Galois groups, II », preprint, 2002.

[40] D.P. Roberts – « Density of cubic field discriminants », *Math. Comp.* **70** (2001), no. 236, p. 1699–1705.

[41] H. Rubenthaler – « Formes réelles des espaces préhomogènes irréductibles de type parabolique », *Ann. Inst. Fourier (Grenoble)* **36** (1986), no. 1, p. 1–38.

[42] H. Saito – « On a classification of prehomogeneous vector spaces over local and global fields », *J. Algebra* **187** (1997), no. 2, p. 510–536.

[43] ———, « Convergence of the zeta functions of prehomogeneous vector spaces », *Nagoya Math. J.* **170** (2003), p. 1–31.

[44] M. Sato – « Theory of prehomogeneous vector spaces (algebraic part)–the English translation of Sato's lecture from Shintani's note », *Nagoya Math. J.* **120** (1990), p. 1–34, traduit du japonais par M. Muro.

[45] M. Sato & T. Kimura – « A classification of irreducible prehomogeneous vector spaces and their relative invariants », *Nagoya Math. J.* **65** (1977), p. 1–155.

[46] M. Sato & T. Shintani – « On zeta functions associated with prehomogenous vector spaces », *Ann. of Math.* **100** (1974), p. 131–170.

[47] J.-P. Serre – « Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local », *C. R. Acad. Sci. Paris Sér. A-B* **286** (1978), no. 22, p. A1031–A1036.

[48] D. Shanks – « On Gauss and composition. I, II », in *Number theory and applications (Banff, AB, 1988)*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, p. 163–178, 179–204.

[49] T. Shintani – « On Dirichlet series whose coefficients are class numbers of integral binary cubic forms », *J. Math. Soc. Japan* **24** (1972), p. 132–188.

[50] ———, « On zeta-functions associated with the vector space of quadratic forms », *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **22** (1975), p. 25–66.

[51] C.L. Siegel – « The average measure of quadratic forms with given determinant and signature », *Ann. of Math. (2)* **45** (1944), p. 667–685.

[52] È.B. Vinberg – « The classification of nilpotent elements of graded Lie algebras », *Dokl. Akad. Nauk SSSR* **225** (1975), no. 4, p. 745–748.

[53] S. Wong – « Automorphic forms on GL(2) and the rank of class groups », *J. reine angew. Math.* **515** (1999), p. 125–153.

[54] D.J. Wright – « The adelic zeta function associated to the space of binary cubic forms. I. Global theory », *Math. Ann.* **270** (1985), no. 4, p. 503–534.

[55] ———, « Distribution of discriminants of abelian extensions », *Proc. London Math. Soc. (3)* **58** (1989), no. 1, p. 17–50.

[56] D.J. Wright & A. Yukie – « Prehomogeneous vector spaces and field extensions », *Invent. Math.* **110** (1992), no. 2, p. 283–314.

[57] A. Yukie – *Shintani zeta functions*, LMS Lect. Notes Series, vol. 183, Cambridge University Press, Cambridge, 1993.

[58] D. Zagier – « Cubic forms and cubic rings », 2001, *Explicit Methods in Number Theory* (Oberwolfach). Exposé.

Karim BELABAS

Université Paris-Sud
Département de Mathématiques (Bât. 425)
F-91405 Orsay Cedex
E-mail : Karim.Belabas@math.u-psud.fr