Formes quadratiques binaires :
loi de composition de Gauss et théorie de Bhargava

9 mai 2007

1 Rappels : formes quadratiques binaires

On considère la forme quadratique binaire

$$f = (a, b, c) = ax^2 + bxy + cy^2,$$

avec $a, b, c \in \mathbb{Z}$.
On dit que f est primitive si $\text{pgcd}(a, b, c) = 1$.
On dit que deux f.q.b. f et g sont équivalentes si et seulement si il existe $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{PSL}_2(\mathbb{Z})$, telle que

$$g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y).$$

Cette relation d'équivalence préserve le discriminant ($D = b^2 - 4ac$) et la primitivité de la forme quadratique.

A partir de la fin du XVIIIème siècle, beaucoup de mathématiciens très célèbres, comme Legendre, Euler, Gauss, Dirichlet et Dedekind, se sont intéressés aux formes quadratiques binaires. Leur but était d'étudier les valeurs représentées par une forme quadratique f :

$$\{f(x, y) | x, y \in \mathbb{Z}\},$$

(elles ne sont pas modifiées par l'action de $\text{PSL}_2(\mathbb{Z})$).
En particulier, Gauss, dans ses *Disquisitiones Arithmeticae* (1801), calcule, en toute généralité, la loi de composition entre deux formes quadratiques binaires :

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

où X et Y sont des fonctions linéaires de (xz, xt, yz, yt). Cette loi lui permettait de donner une propriété de multiplicativité aux valeurs représentées par une forme quadratique.
La loi de Gauss peut s'écrire plus simplement quand les deux formes quadratiques binaires ont le même discriminant (ce qui a été traité par Dirichlet et Dedekind) et elle est expliquée par la multiplicativité de la norme dans $\mathbb{Z}[\sqrt{D}]$.
En effet, tous ces résultats, en langage moderne, reviennent au Théorème suivant :

Théorème 1 *Il existe une bijection canonique entre :*

1. *les classes d'isomorphismes de paires (S, I), où S est un anneau quadratique orienté de discriminant $D \neq 0$, et I une classe d'idéaux orientés de S ;*
2. *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 de formes quadratiques, l'ensemble des classes de formes primitives de discriminant $D \neq 0$ est un groupe, isomorphe au groupe des classes orientées $Cl^+(D)$.

(Pour la définition d'idéaux orientés on renvoie au Paragraphe 3, Définition 3.)
On va maintenant voir des généralisations très récentes ($\sim$ 2004), dûes à Bhargava, de ces problèmes que, comme on a vu, intéressent depuis des siècles les mathématiciens...

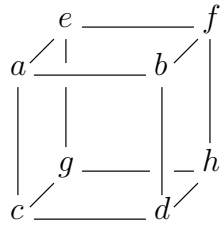
2 La loi du cube

Soit

$$\mathcal{C}_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2.$$

$\mathcal{C}_2$ est un groupe abélien libre de rang 8. On peut représenter tout élément $A \in \mathcal{C}_2$ comme un vecteur (a, b, c, d, e, f, g, h), ou mieux comme un cube

d'entiers :



On peut partitionner le cube A en deux matrices 2×2, de trois manières différentes (en coupant par rapport aux trois plans de symétrie) :

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix} \quad N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix} \quad N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}$$

On considère l'action de $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{C}_2$, où l'i-ème facteur $(i = 1, 2, 3)$ $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ agit sur $A \in \mathcal{C}_2$ en remplaçant (M_i, N_i) par $(rM_i + sN_i, tM_i + uN_i)$.
Les actions des trois facteurs commutent entre elles.
On définit aussi les formes quadratiques binaires :

$$Q_i^A(x, y) = -\operatorname{Det}(M_i x - N_i y), i = 1, 2, 3$$

et on remarque que Q_1 est invariante par l'action de $\{\mathrm{Id} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})\}$; en effet, cela arrive car les autres deux facteurs de Γ agissent sur Q_1 par opérations sur les lignes/colonnes. D'autre part, le premier facteur de Γ donne l'action standard de $\mathrm{SL}_2(\mathbb{Z})$ sur Q_1. Evidemment il en est de même pour les actions de Γ sur Q_2 et Q_3.
On rappelle que l'unique invariant polynomial d'une forme quadratique modulo $SL_2(\mathbb{Z})$ est son discriminant : $\mathrm{Disc}(Q_1)$. Or, il se passe que

$$\begin{aligned} \mathrm{Disc}(Q_1) = \quad & \mathrm{Disc}(Q_2) = \mathrm{Disc}(Q_3) = a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ & -2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh) \end{aligned}$$

et donc on peut définir $\mathrm{Disc}(A)$ comme cet unique invariant.

Exemple
Toute forme quadratique binaire provient d'un cube.
Preuve
Soit (P, Q, R) la forme quadratique qu'on veut obtenir. On considère le cube $A = (a, b, c, d, e, f, g, h)$ où $a = -1, b = c = 0, d = P, e = 0, f = 1, g = R$ et $h = -Q$ et on calcule Q_1^A. On obtient

$$Q_1^A(x, y) = Px^2 + Qxy + Ry^2.$$

□

Définition 1 *On dit qu'un cube A est projectif si Q_1^A, Q_2^A et Q_3^A sont primitives.*
On écrit $[A]$ la classe d'équivalence de A modulo Γ.

On va définir maintenant une loi d'addition dur l'ensemble des f.q.b. primitives de même discriminant D.

La loi du cube :
Pour tous les triplets Q_1^A, Q_2^A, Q_3^A de f.q.b. primitives provenantes d'un cube A de discriminant D : la somme de Q_1^A, Q_2^A et Q_3^A est zéro.
Plus formellement : on considère le groupe abelien libre sur
{f.q.b. primitives de discriminant D} modulo le sous-groupe engendré par toutes les sommes $[Q_1^A] + [Q_2^A] + [Q_3^A]$.

Remarque : Grâce à la Loi du Cube on obtient automatiquement l'identification des formes $\mathrm{SL}_2(\mathbb{Z})$ équivalentes.
Preuve
Soit $A \in \mathcal{C}_2$ un cube projectif, auquel sont associées les formes quadratiques : Q_1^A, Q_2^A et Q_3^A, et soit $\gamma = \gamma_1 \times \mathrm{Id} \times \mathrm{Id} \in \Gamma$ (évidemment, la même démonstration marche aussi pour les autres deux composantes).
Soit $A' = \gamma A$. On a :

$$Q_1^{A'} = \gamma_1 Q_1^A, Q_2^{A'} = Q_2^A, Q_3^{A'} = Q_3^A.$$

Or comme $[Q_1^A] + [Q_2^A] + [Q_3^A] = 0$ et $[Q_1^{A'}] + [Q_2^{A'}] + [Q_3^{A'}] = [\gamma Q_1^A] + [Q_2^A] + [Q_3^A] = 0$, on conclut :

$$[Q_1^A] = [Q_1^{A'}] = [\gamma Q_1].$$

□

On va maintenant enoncer un théorème très important, dont on verra la démonstration dans la prochaine Section.

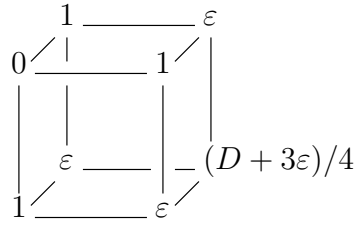
Théorème 2 *Soit D un entier $\equiv 0, 1 \mod 4$. soit $Q_{\mathrm{Id},D}$ une f.q.b. primitive de discriminant D, telle que il existe un cube A_0 avec $Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = Q_{\mathrm{Id},D}$.*
Alors, il existe une unique loi de groupe sur les classes d'équivalence de $\{$f.q.b. primitives de discriminant $D\}$ modulo $\mathrm{SL}_2(\mathbb{Z})$, telle que

1. *$[Q_{\mathrm{Id},D}]$ soit l'identité additive ;*
2. *pour tout cube projectif A de discriminant D, on a*

$$[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{\mathrm{Id},D}].$$

Inversement, étant donné Q_1, Q_2, Q_3 trois f.q.b. primitives de discriminant D, avec $[Q_1] + [Q_2] + [Q_3] = [Q_{\mathrm{Id},D}]$, il existe un cube projectif A de discriminant D, unique modulo Γ, tel que $Q_1^A = Q_1$,$Q_2^A = Q_2$ et $Q_3^A = Q_3$.

Remarque : On peut faire un choix naturel pour $Q_{\mathrm{Id},D}$:
– $Q_{\mathrm{Id},D} = x^2 - \frac{D}{4}y^2$,si $D \equiv 0 \mod 4$;
– $Q_{\mathrm{Id},D} = x^2 - xy + \frac{1-D}{4}y^2$ si $D \equiv 1 \mod 4$
ce qui corréspond au choix du cube A_0 (triplement symétriques) :



(1)

où $\varepsilon \equiv D \mod 4$. En particulier, si on fait ce choix pour l'identité de la loi de groupe, on obtient exactement la loi de composition de Gauss pour les formes quadratiques !!!

Théorème 3 *Pour le choix de A_0 donné par (1), la loi de groupe du Théorème 2 est la composition de Gauss du Théorème 1.*

On va maintenant définir une loi de groupe sur les cubes :

Théorème 4 *Soit D un entier $\equiv 0, 1 \mod 4$. Alors, il existe une unique loi de groupe sur les classes d'équivalence de cubes projectifs de discriminant D modulo $\mathrm{SL}_2(\mathbb{Z})$, telle que :*

1. *$[A_0]$ soit l'identité additive ;*

2. *pour tout* $i = 1, 2, 3$ *l'application* $\varphi_i : [A] \to [Q_i^A]$ *donne un homomorphisme de groupe vers* $\{$*f.q.b. primitives de discriminant* $D\}/\operatorname{SL}_2(\mathbb{Z})$ *avec la loi de groupe définie au Théorème 2.*

Preuve
Soient A et A' deux cubes projectifs de discriminant D. On a

$$([Q_1^A] + [Q_1^{A'}]) + ([Q_2^A] + [Q_2^{A'}]) + ([Q_3^A] + [Q_3^{A'}]) = [Q_{\mathrm{Id},D}],$$

alors, grâce à la deuxième partie du Théorème 2, il existe un cube projectif A'' de discriminant D tel que $[Q_1^{A''}] = ([Q_1^A]+[Q_1^{A'}])$, $[Q_2^{A''}] = ([Q_2^A]+[Q_2^{A'}])$ et $[Q_3^{A''}] = ([Q_3^A] + [Q_3^{A'}])$. On défiinit donc $[A''] = [A] + [A']$ et le théorème est demontré. □

3 Rélations avec classes d'idéaux dans des ordres quadratiques

3.1 Définitions

Soit D un entier $\equiv 0, 1 \mod 4$. Soit $S = S(D)$ l'unique anneau quadratique de disciminant D :

$$S(D) = \begin{cases} \mathbb{Z}[x]/(x^2) & \text{si } D = 0, \\ \mathbb{Z} \cdot (1,1) + \sqrt{D}(\mathbb{Z} \otimes \mathbb{Z}) & \text{si } D \geq 1 \text{ est un carré}, \\ \mathbb{Z}[(D + \sqrt{D})/2] & \text{sinon.} \end{cases}$$

Explicitement, $S(D)$ a une $\mathbb{Z}$-base $\langle 1, \tau \rangle$, où la multiplication est déterminé par la loi :

$$\tau^2 = D/4 \text{ si } D \equiv 0 \mod 4 \text{ ou } \tau^2 = \frac{D-1}{4} + \tau \text{ si } D \equiv 1 \mod 4.$$

Définition 2 *On dit que* S *est un* anneau quadratique orienté *si on donne le choix d'un isomorphisme* $\overline{\pi} : S/\mathbb{Z} \to \mathbb{Z}$. *Plus précisement, on choisit une des deux racines* $\sqrt{D}$, *on définit* $\pi : S \to \mathbb{Z}$, *par* $\pi(x) = \operatorname{Tr}(x/\sqrt{D}) = \frac{x-\sigma(x)}{\sqrt{D}}$. *On remarque que le noyau de* π *est* $\mathbb{Z}$ *et on déduit* $\overline{\pi}$. *On dit que la base* $\langle 1, \tau \rangle$ *de* S *est orientée positivement si* $\pi(\tau) > 0$.

Définition 3 *Une classe d'idéaux orientés ("narrow") est la donnée d'un couple* (I, ε) *où* I *est un idéal fractionnaire de* S *dans* K, *de rang* 2 *comme*

$\mathbb{Z}$-module, et $\varepsilon = \pm 1$ est son orientation. On définit la multiplication d'idéaux orientés composante par composante, et la norme par :

$$\mathcal{N}((I,\varepsilon)) = \varepsilon \frac{|L/I|}{|L/S|},$$

où L est un réseau dans K qui contient S et I.

Définition 4 *Un triplet d'idéaux orientés (I_1, I_2, I_3) est dit ´equilibré ("balanced") si $I_1 I_2 I_3 \subseteq S$ et $\mathcal{N}(I_1)\mathcal{N}(I_2)\mathcal{N}(I_3) = 1$. Deux triplets (I_1, I_2, I_3) et (I'_1, I'_2, I'_3) sont équivalents si $I_1 = \kappa_1 I'_1$,$I_2 = \kappa_2 I'_2$ et $I_3 = \kappa_3 I'_3$, il existe $\kappa_1, \kappa_2, \kappa_3 \in K$ (une conséquence immédiate est que $\mathcal{N}(\kappa_1\kappa_2\kappa_3) = 1$).*
Par exemple, si S est un anneau de Dedekind, une classe d'équivalence de triplets équilibrés est simplement un triplet d'idéaux orientés dont le produit est l'idéal principal.

3.2 Résultat fondamental

Théorème 5 *Il existe une bijection canonique entre l'ensemble des Γ-orbites non dégénérées de $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ et l'ensemble des classes d'isomorphisme des couples $(S, (I_1, I_2, I_3))$ où S est un anneau quadratique orienté non dégénéré, et (I_1, I_2, I_3) est une classe d'équivalence de triplets équilibrés d'idéaux orientés de S.*
Sous cette bijection le discriminant d'un cube entier est égal au discriminant de l'anneau quadratique correspondant.

Preuve

– **Etant donné un couple $(S = S(D), (I_1, I_2, I_3))$ comme dans l'enoncé, on va lui associer un cube.**
On choisit une base orientée positivement $\langle 1, \tau \rangle$ de S telle que $\tau^2 - D/4 = 0$ ou $\tau^2 - \tau + (1-D)/4 = 0$, si $D \equiv 0, 1 \mod 4$ respectivement.
Soient $\langle \alpha_1, \alpha_2 \rangle$,$\langle \beta_1, \beta_2 \rangle$ et $\langle \gamma_1, \gamma_2 \rangle$ des $\mathbb{Z}$-bases de I_1, I_2, I_3 respectivement, avec orientation égale (differente) de $\langle 1, \tau \rangle$ si $\epsilon(I_j) = +1$ (-1, respectivement).
Comme $I_1 I_2 I_3 \subseteq S$ par définition, on peut écrire :

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk}\tau \tag{2}$$

pour 16 entiers a_{ijk} et c_{ijk} $i, j, k = 1, 2$. $A = (a_{ijk})$ est le cube qu'on va associer à $(S, (I_1, I_2, I_3))$.

- **Le cube obtenu ne dépend pas du choix des bases de I_1, I_2, I_3.**
  Supposons de remplacer $\langle\alpha_1, \alpha_2\rangle$,$\langle\beta_1, \beta_2\rangle$ et $\langle\gamma_1, \gamma_2\rangle$ par un autre ensemble des bases de I_1, I_2 et I_3 (avec la même orientation) : $\langle\alpha_1', \alpha_2'\rangle$,$\langle\beta_1', \beta_2'\rangle$ et $\langle\gamma_1', \gamma_2'\rangle$. La "matrice" de passage est $T \in \Gamma$ et on obtient la même transformation sur le cube obtenu, qui donc est equivalent au cube initial A.
- **Le cube obtenu ne dépend pas du choix du représentant de la classe d'équivalence du triplet équilibré**
  Il est évident que si on échange (I_1, I_2, I_3) par (I_1', I_2', I_3'), A ne change pas. Donc notre application est bien définie.
- **L'application ci-dessus est une bijection**
  Pour demontrer cela on va montrer que pour tout cube A il existe exactement un couple $(S, (I_1, I_2, I_3))$ (modulo équivalence) qui est envoyé en A par notre application.
  On fixe $A = (a_{ijk})$, et on considère le système (2) dans les inconnues $\alpha_i, \beta_j, \gamma_k, c_{i'j'k'}$. On va montrer que toutes ces inconnues sont en fait déterminées par A.

  1. S **(ou mieux** $\mathrm{Disc}(S)$**) est determiné par** A**.**
     On va montrer que le système (2) implique

     $$\mathrm{Disc}(A) = \mathcal{N}(I_1)^2\mathcal{N}(I_2)^2\mathcal{N}(I_3)^2 \cdot Disc(S), \tag{3}$$

     mais alors, vu que $\mathcal{N}(I_1)\mathcal{N}(I_2)\mathcal{N}(I_3) = 1$ par définition on obtiendra $\mathrm{Disc}(A) = \mathrm{Disc}(S)$ et on pourra conclure. Montrons donc la formule (3) : soit $S = S(D) = \mathbb{Z} + \mathbb{Z}\tau$ (D inconnue). Le cas plus simple est si $I_1^0 = I_2^0 = I_3^0 = S$, et donc $\alpha_1 = \beta_1 = \gamma_1 = 1$ et $\alpha_2 = \beta_2 = \gamma_2 = \tau$, dans ce cas là on obtient A_0, le cube identité, et donc $\mathrm{Disc}(A_0) = D = \mathrm{Disc}(S)$. Maintenant supposons de remplacer I_1^0 par un idéal fractionnaire quelconque I_1 de $\mathbb{Z}$-base $\langle\alpha_1, \beta_1\rangle$, alors il existe une transformation $T \in \mathrm{GL}_2(\mathbb{Q})$ qui envoye $\langle 1, \tau\rangle$ dans $\langle\alpha_1, \beta_1\rangle$, donc on transforme A_0 en A' en passant par la "matrice" $T \times \mathrm{Id} \times \mathrm{Id}$. Or, il est évident que cette action va envoyer $Q_2^{A_0}$ (ou $Q_3^{A_0}$) dans $\det(T) \cdot Q_2^{A_0}$ (respectivement $\det(T) \cdot Q_3^{A_0}$) et donc $\mathrm{Disc}(A') = \mathrm{Disc}(Q_2^{A'}) = \det(T)^2\,\mathrm{Disc}(Q_2^{A_0}) = \mathcal{N}(I_1)^2\,\mathrm{Disc}(A_0)$. Similement, si on change I_2 et I_3 en des idéaux fractionnaires quelconques, on multiplie le $\mathrm{Disc}(A_0)$ par $\mathcal{N}(I_2)^2$ et $\mathcal{N}(I_3)^2$, donc on obtient la formule (3).
  2. **Les** c_{ijk} **sont uniquement determinés par** A**.**
     Par associativité et commutativité de S on a

     $$\begin{aligned} & \alpha_i\beta_j\gamma_k \cdot \alpha_{i'}\beta_{j'}\gamma_{k'} = \alpha_{i'}\beta_j\gamma_k \cdot \alpha_i\beta_{j'}\gamma_{k'} = \alpha_i\beta_{j'}\gamma_k \cdot \alpha_{i'}\beta_j\gamma_{k'} \\ = \;& \alpha_i\beta_j\gamma_{k'} \cdot \alpha_{i'}\beta_{j'}\gamma_k, \end{aligned} \tag{4}$$

avec $i, j, k, i', j', k' = 1, 2$. On développe (4) avec (2), on impose les égalités des coefficients de 1 et de τ, et on impose
$\mathcal{N}(I_1)\mathcal{N}(I_2)\mathcal{N}(I_3) > 0$, pour obtenir 18 équations (linéaires et quadratiques) dans les c_{ijk} en termes des a_{ijk} et on obtient une solution unique avec $c_{ijk} \in \mathbb{Z}$.

3. **On va montrer qu'il existe des $\alpha_i, \beta_j, \gamma_k$ qui donnent les a_{ijk}, c_{ijk} désirés.**
   Il est facile de voir que les paires $(\alpha_1, \alpha_2), (\beta_1, \beta_2)$ et (γ_1, γ_2) sont uniquement déterminés, grâce à (2), modulo un facteur scalaire non nul dans K.
   En outre, si l'on fixe (α_1, α_2) et (β_1, β_2), alors (γ_1, γ_2) est uniquement déterminé, ce qui nous assure que le triplet (I_1, I_2, I_3) est uniquement déterminé modulo équivalence.
4. **Il nous reste à montrer que $\langle \alpha_1, \alpha_2 \rangle$,$\langle \beta_1, \beta_2 \rangle$ et $\langle \gamma_1, \gamma_2 \rangle$ sont bien des idéaux de S.**
   Cela est facile à démontrer par calcul.

□

Définition 5 *On dit que un triplet équilibré (I_1, I_2, I_3) d'idéaux de S est projectif si I_1, I_2, I_3 sont inversibles comme S-modules.*

(Exemple : dans un anneau de Dedekind tout idéal fractionnaire est projectif.)
Il est facile de vérifier par calcul que le triplet (I_1, I_2, I_3) est projectif 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 $Cl^+(D) \times Cl^+(D)$ par la projection $(I_1, I_2, I_3) \to (I_1, I_2)$.
Si on restreint le Théorème 5 aux cubes projectifs, on obtient l'isomorphisme suivant :

Théorème 6 *La bijection du Théorème 5 se restreint à une corréspondance :*

$$\{\textit{cubes projectifs de discriminant } D\}/\Gamma \leftrightarrow Cl^+(D) \times Cl^+(D)$$

qui est un isomorphisme de groupes.

Preuve Conséquence des Théorèmes 1 et 3. □

Remarque
Avec un petit calcul on peut remarquer que les formes normes de I_1, I_2, I_3 sont exactement Q_1^A, Q_2^A et Q_3^A. Il est donc facile d'obtenir les Théorèmes 1 et 2.

4 Consequences

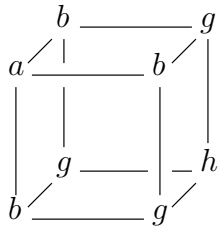
Comme on a dit, la loi du cube est une généralisation de la loi de composition de Gauss. En effet, en plus de nous donner la composition de formes quadratiques binaires, cette loi nous fournit aussi :

1. composition de formes cubiques binaires (classiques) ;
2. composition de couples de formes quadratique binaires (classiques) ;
3. composition de couples de 2-formes quaternaires alternantes ;
4. composition de 3-formes senaires alternantes.

On va donner comme exemple les deux premières, et on verra immédiatement que les énoncés (et les démonstrations) sont des cas particuliers des énoncés et des démonstrations qu'on a fait en général pour la loi du cube.

4.1 Formes cubiques binaires

On considère le cube triplement symétrique :



et on lui associe la forme cubique binaire $ax^3 + bx^2y + gxy^2 + hy^3$.
On obtient donc une inclusion :

$$\iota : \mathrm{Sym}^3 \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2,$$

de l'espace des cubes triplement symétriques (formes cubiques binaires) dans l'espace des cubes.
On appelle projective une forme cubique binaire si elle correspond à un cube projectif.
On a le Théorème suivant :

Théorème 7 *Soit D un entier $\equiv 0, 1 \mod 4$, et soit $C_{\mathrm{Id},D}$ la préimage du cube identité A_0 de discriminant D.*
Il existe une unique loi de groupe sur l'ensemble des classes d'équivalence modulo $\mathrm{SL}_2(\mathbb{Z})$ des formes cubiques binaires projectives C de discriminant D telle que :

1. *$[C_{\mathrm{Id},D}]$ est l'identité additive ;*
2. *L'application qui envoie $[C] \to [\iota(C)]$ est un homomorphisme de groupes dans le groupe des cubes modulo Γ.*

De façon semblable au Théorème 5 on a maintenant un Théorème qui nous donne une nouvelle vision des formes cubiques binaires :

Théorème 8 *Il y a une bijection canonique entre l'ensemble des $\mathrm{SL}_2(\mathbb{Z})$-orbites non dégénérées de l'espace $Sym^3\mathbb{Z}^2$ des formes cubiques binaires, et l'ensemble des classes d'équivalence des triplets (S, I, δ) où S est un anneau quadratique orienté non dégénéré , I est un idéal de S, et δ est un élément inversible de $K = S \otimes \mathbb{Q}$ tel que $I^3 \subseteq \delta \cdot S$ et $\mathcal{N}(I)^3 = \mathcal{N}(\delta)$.*
(Ici deux triplets (S, I, δ) et (S', I', δ') sont équivalents si il existe un isomorphisme $\phi : S \to S'$ et un élément $\kappa \in S' \otimes \mathbb{Q}$ tel que $I' = \kappa\phi(I)$ et $\delta' = \kappa^3\phi(\delta)$.)
Sous cette bijection, le discriminant d'une forme cubique binaire est égal au discriminant de l'anneau quadratique correspondant.

En particulier, si on se restreint aux formes cubiques binaires projectives, et l'on note $Cl_3(D)$ le groupe des classes d'idéaux dont l'ordre divise 3 dans $Cl(S(D))$, on obtient l'homomorphisme suivant :

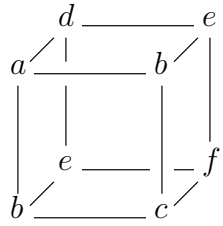
Corollaire 1 *Soit $S(D)$ l'anneau quadratique de discriminant D.*
Alors il y a un homomorphisme de groupes, naturel et surjectif,

$$\{f.cub.bin.proj.\ de\ discr\ D\ modulo\ \mathrm{SL}_2(\mathbb{Z})\} \to Cl_3(D),$$

qui envoie une forme cubique binaire C dans le $S(D)$-module I, où $(S(D), I, \delta)$ est le triplet correspondant à C dans le Théorème 8. En outre, la cardinalité du noyau de cet homomorphisme est $|U/U^3|$, où U est le groupe des unités de $S(D)$.

4.2 Couples de formes quadratiques binaires

On considère le cube doublement symétrique :



et on lui associe le couple de formes quadratiques binaires $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$.
On obtient donc une inclusion :

$$\nu : \mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2,$$

de l'espace des cubes triplement symetriques (formes cubiques binaires) dans l'espace des cubes.
On appelle projectifs les couples qui proviennent d'un cube projectif.
On a donc les Théorèmes suivants.

Théorème 9 *Soit $D \equiv 0, 1 \mod 4$ et soit $B_{\mathrm{Id},D}$ la préimage du cube identité par ν. Alors, il existe une unique loi de groupe sur l'ensemble des classes d'équivalence modulo $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ des couples projectifs de formes quadratiques binaires B de discriminant D, telle que :*

1. *$[B_{\mathrm{Id},D}]$ est l'idéntité additive ;*
2. *L'application qui envoye $[B] \to [\nu(B)]$ est un homomorphisme de groupes dans le groupe des cubes projectifs.*

Théorème 10 *Il existe une bijection canonique entre l'ensemble des $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-orbites non dégénérées dans l'espace $\mathbb{Z}^2 \otimes Sym^2\mathbb{Z}^2$, et l'ensemble des classes d'isomorphisme des couples $(S, (I_1, I_2, I_3))$, où S est un anneau quadratique orienté non dégénéré et (I_1, I_2, I_3) est une classe d'équivalence de triplets équilibrés de S telle que $I_2 = I_3$. Sous cette bijection, le discriminant d'un couple de formes binaires quadratiques est égal au discriminant de l'anneau quadratique correspondant.*

Références

[1] K. Belabas, *Paramétrisation de structures algébriques et densité de discriminants [d'après M. Bhargava]*, Séminaire Bourbaki, 56ème année, 2003-2004, n. 935.

[2] M. Bhargava, *Higher composition laws I : A new view on Gauss composition, and quadratic generalizations*, Annals of Mathematics, **159** (2004), 217-250.

[3] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer.