Table des matières

Chapitre 1

Introduction

Ce mémoire, se voulant un résumé des travaux de Bhargava, n'entre pas dans les détails précis des démonstrations de chacun des théorèmes. Les preuves, souvent plus techniques que didactiques, ont été omises dans la plupart des cas. Toutefois, un lecteur intéressé à ces précisions pourra pour sa part consulter les articles de Bhargava ainsi que les livres annotés tout au long du texte sous forme de références. L'optique de se concentrer essentiellement sur les formes quadratiques et ses sujets connexes fut le guide pour ce qui est du choix des thèmes abordés dans ce mémoire. Ce chapitre est donc consacré aux préliminaires nécessaires à une lecture compréhensible du texte qui suivra. Elle constitue une introduction non exhaustive au langage associé aux formes quadratiques. Pour plus amples précisions sur ces formes, le lecteur pourra se référer principalement aux textes [12], [13] et [14].

Une forme quadratique binaire intégrale et primitive, que nous noterons plus simplement *forme quadratique*, est une expression du type

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

où a, b, $c \in \mathbb{Z}$ et pgcd(a,b,c)=1.

L'étude de ces formes ou plus précisément des équations diophantiennes $f(x, y) = n$ avec $x, y \in \mathbb{Z}$ a fait l'objet de nombreux traités de théorie des nombres. On peut se demander, par exemple, si ces équations ont des solutions dans $\mathbb{Z}$? Il fut remarqué qu'en regroupant celles-ci sous forme de classes d'équivalence, la question devenait plus aisée.

1.1 L'action de $SL_2(\mathbb{Z})$

Il nous est possible, en faisant agir naturellement le groupe multiplicatif $SL_2(\mathbb{Z})$ sur l'ensemble des formes quadratiques, de regrouper celles-ci en classes d'équivalence pour ainsi, comme mentionné précédemment, simplifier leur étude. Ces classes sont les orbites de l'action du groupe $SL_2(\mathbb{Z})$ définie comme suit :

$$Af(x,y) = a(rx+ty)^2 + b(rx+ty)(sx+uy) + c(sx+uy)^2,$$

où $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$ et $f(x,y)$ une forme quadratique.

Le même résultat est obtenu en appliquant la transformation

$$\begin{cases} x' = rx + ty, \\ y' = sx + uy. \end{cases}$$

Ce qui nous donne une nouvelle forme quadratique $f(x',y') = f'(x,y)$. Ainsi, par cette transformation, une solution (x'_1, y'_1) de $f'(x,y) = n$ en induit une seconde pour $f(x,y) = n$. Il devient donc naturel de considérer ces deux formes quadratiques comme équivalentes ($SL_2(\mathbb{Z})$-équivalentes), c'est-à-dire qu'il existe une matrice $A \in SL_2(\mathbb{Z})$ telle que $Af(x,y) = f'(x,y)$. Nous noterons la classe d'équivalence d'une forme quadratique par $[f(x,y)]$. Dans notre exemple $[f(x,y)] = [f'(x,y)]$.

Nous pouvons ici nuancer la définition d'équivalence en mentionnant l'équivalence au sens large ou au sens strict. L'équivalence définie ci-dessus est appelée l'équivalence stricte des formes quadratiques lorsque la matrice A appartient à $SL_2(\mathbb{Z})$, c'est-à-dire A est une matrice 2×2 de déterminant $+1$ à coefficients dans $\mathbb{Z}$. Si toutefois la matrice A appartient à $GL_2(\mathbb{Z})$, c'est-à-dire de déterminant $+1$ ou -1, alors nous parlerons de relation d'équivalence au sens large. On note également que l'équivalence au sens large donne naissance à moins de classes d'équivalence que celle au sens strict. Cette nuance entre équivalence au sens stricte et large est notamment abordée dans [14].

1.2 Loi de composition de Gauss

Ce qui nous intéressera par la suite sera de définir une structure de groupe sur les classes d'équivalence de formes quadratiques. Nous verrons que la loi de composition

de Gauss publiée dans son fameux *Disquisitiones Arithmeticae* [7] a évolué pour faire place à une loi plus générale, celle de Bhargava. Cette dernière non seulement englobe la loi de Gauss mais en génère également quatorze autres. Mais débutons par un court rappel sur la loi de composition de Gauss.

Définition. Le *discriminant* d'une forme quadratrique $f(x, y) = ax^2 + bxy + cy^2$ est donné par $\Delta = b^2 - 4ac$.

Définition. Deux formes quadratiques $f_1(x, y) = a_1x^2 + b_1xy + c_1y^2$ et $f_2(x, y) = a_2x^2 + b_2xy + c_2y^2$ de discriminant Δ sont dites *concordantes* si

(i) $a_1a_2 \neq 0$,
(ii) $b_1 = b_2$,
(iii) $a_2 \mid c_1$ et $a_1 \mid c_2$.

Définition. Soit deux formes quadratiques $f_1(x, y) = a_1x^2+b_1xy+c_1y^2$ et $f_2(x, y) = a_2x^2+b_2xy+c_2y^2$ de même discriminant et concordantes. Alors la *composition* de Gauss '$*$' de ces deux formes est

$$f_1(x, y) * f_2(x, y) = a_1a_2x^2 + bxy + cy^2,$$

où $b = b_1 = b_2$ et l'entier c est uniquement déterminé par le discriminant $\Delta = b^2 - 4(a_1a_2)c$, c'est-à-dire $c = \frac{(b^2-\Delta)}{4a_1a_2}$.

On note que sous la composition des formes quadratiques ainsi définie, le discriminant Δ est invariant. C'est-à-dire que $f_1(x, y) * f_2(x, y)$ a le même discriminant que $f_1(x, y)$ et $f_2(x, y)$. De plus, la classe d'équivalence déterminée par cette composition ne dépend pas des deux formes composées mais plutôt de leurs classes d'appartenance. Cette propriété découle des résultats suivants.

Lemme. *Soit C_1 et C_2 deux classes $SL_2(\mathbb{Z})$-équivalentes de formes quadratiques primitives de discriminant $\Delta \neq 0$. Soit un entier $m \in \mathbb{Z}$, $m \neq 0$. Alors, il existe une paire de formes quadratiques concordantes $f_1 = a_1x^2+bxy+cy^2 \in C_1$ et $f_2 = a_2x^2+bxy+cy^2 \in C_2$ telle que $pgcd(a_1, a_2) = 1$ et $pgcd(a_1a_2, m) = 1$.*

Démonstration. Choisissons $F_1 = (a_1, b_1, *) \in C_1$ telle que $a_1 \neq 0$ et $pgcd(a_1, m) = 1$

et où $*$ est déterminée par le discriminant. Pour faire cela, soit f un élément de la classe C_1 et soit r, s des entiers relativement premiers tels que $a_1 = f(r,s) \neq 0$ et $pgcd(a_1, m) = 1$. Soit de plus t et u appartenant à $\mathbb{Z}$ tels que $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ soit une matrice de $SL_2(\mathbb{Z})$. Alors, $F_1 = \gamma f = (a_1, b_1, *)$ est la forme quadratique désirée. De la même façon, on peut choisir $F_2 = (a_2, b_2, *) \in C_2$ telle que $a_2 \neq 0$ et $pgcd(a_2, a_1 m) = 1$.

Ensuite, il s'agit de trouver deux entiers n_1 et n_2 tels que $b_1 + 2a_1 n_1 = b_2 + 2a_2 n_2$. Cette équation peut être écrite sous la forme $a_1 n_1 - a_2 n_2 = (b_2 - b_1)/2$. Les solutions n_1 et n_2 existent puisque $b_1 \equiv \Delta \equiv b_2 (mod\ 2)$ et $pgcd(a_1, a_2) = 1$.

Clairement, les formes quadratiques

$$f_j = \begin{pmatrix} 1 & 0 \\ n_j & 1 \end{pmatrix} F_j = (a_j, b, *),$$

où $j \in 1, 2$ et $b = b_j + 2a_j n_j$, sont concordantes.

C.Q.F.D.

Proposition. *Soit C_1 et C_2 deux classes $SL_2(\mathbb{Z})$-équivalentes de formes quadratiques primitives de discriminant $\Delta \neq 0$. Soit $f_1 \in C_1$ et $f_2 \in C_2$ une paire de formes concordantes. Soit $g_1 \in C_1$ et $g_2 \in C_2$ une autre paire de formes concordantes. Alors, $f_1 * f_2$ est $SL_2(\mathbb{Z})$-équivalente à $g_1 * g_2$. On notera $f_1 * f_2 \sim g_1 * g_2$.*

Démonstration.

(1) Soit $f_j = (a_j, b, c_j)$ et $g_j = (a'_j, b', c'_j)$, $j \in 1, 2$. Puisque, $f_1 \sim g_1$ et que $pgcd(a_1, a'_2) = 1$, on a que f_1 est concordante avec g_1 et g_2. Montrons que $f_1 * f_2 \sim g_1 * g_2$.

Soit $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ une matrice de $SL_2(\mathbb{Z})$ telle que $\gamma f_2 = g_2$. On a donc la relation

$$\gamma \begin{pmatrix} a_2 & b/2 \\ b/2 & c_2 \end{pmatrix} = \begin{pmatrix} a'_2 & b/2 \\ b/2 & c'_2 \end{pmatrix} (\gamma^t)^{-1}.$$

En prenant les composantes diagonales de cette matrice on obtient $-sc_2 = ta'_2$. Puisque f_1 est concordantes à f_2, a_1 divise c_2. Ainsi, a_1 divise ta'_2 et alors a_1 divise t. On en

conclut que

$$\gamma' = \begin{pmatrix} r & sa_1 \\ t/a_1 & u \end{pmatrix}$$

appartient à $SL_2(\mathbb{Z})$. On note également que $\gamma'(f_1 * f_2) = f_1 * g_2$.

(2) L'hypothèse $b = b'$ et $pgcd(a_1, a_2') = 1$ implique que f_1 et g_2 sont concordantes. En appliquant deux fois l'étape 1 on a que $f_1 * f_2 \sim f_1 * g_2 \sim g_1 * g_2$.

(3) L'hypothèse étant $pgcd(a_1a_2, a_1'a_2') = 1$, prenons B, n et n' appartenant à $\mathbb{Z}$ tels que $b + 2a_1a_1n = b' + 1a_1'a_2'n' = B$. Fixons

$$F_1 = \begin{pmatrix} 1 & 0 \\ a_2n & 1 \end{pmatrix} f_1 = (a_1, B, *)$$

et

$$F_2 = \begin{pmatrix} 1 & 0 \\ a_1n & 1 \end{pmatrix} f_2 = (a_2, B, *) \in C_2.$$

Soit $H_1 = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} (f_1 * f_2) = (a_1a_2, B, *)$. Le calcul du discriminant de H_1 montre que $a_1a_2 \mid (B^2 - \Delta)/4$. Le discriminant de F_1 et F_2 montre que ces deux formes quadratiques sont concordantes. De façon similaire, les formes $G_j = (a_j', B, *) \in C_j$, $i = 1, 2$, sont concordantes et $H_2 = (a_1'a_2', B, *) \sim g_1 * g_2$. En appliquant maintenant l'étape 2 aux 4 formes $F_j, G_j \in C_j$, on conclut que $f_1 * f_2 \sim H_1 = F_1 * F_2 \sim G_1 * G_2 = H_2 \sim g_1 * g_2$.

Finalement, d'après le lemme précédent, il existe des formes concordantes $F_j = (A_j, B, *) \in C_j$ telles que $pgcd(A_1A_2, a_1a_2a_1'a_2') = 1$. Deux applications successives de l'étape 3 prouvent que $f_1 * f_2 \sim F_1 * F_2 \sim g_1 * g_2$.

C.Q.F.D.

Avec cette composition, nous obtenons une opération binaire bien définie sur l'ensemble des classes de formes quadratiques de discriminant Δ. Explicitement, si C_1 et C_2 sont deux classes d'équivalence de formes quadratiques de discriminant Δ avec $f_1(x, y) \in C_1$ et $f_2(x, y) \in C_2$ deux formes concordantes, alors nous pouvons composer C_1 et C_2 tout simplement en composant $f_1(x, y)$ et $f_2(x, y)$ et en prenant la nouvelle classe d'équivalence ainsi obtenue.

Précisons ici que tout comme nous avons nuancé la définition d'équivalence (au sens strict ou large), nous pouvons différencier celle de classe. Effectivement, l'ensemble des

formes quadratiques d'un discriminant fixé quotienté par la relation d'équivalence au sens large induira le groupe de classes au sens large, soit $Cl(\Delta)$. Le même ensemble de formes quotienté par la relation d'équivalence au sens strict, qui induira le groupe de classes au sens strict, sera noté $Cl^+(\Delta)$.

Par rapport à cette opération de composition sur l'ensemble des classes d'équivalence au sens strict, il y a un élément neutre C_0 qui est la classe de la forme quadratique

$$f_0(x,y) = \begin{cases} x^2 + xy + \dfrac{(1-\Delta)}{4}y^2 & \text{si } \Delta \equiv 1 \ (mod\ 4), \\ x^2 - \dfrac{\Delta}{4}y^2 & \text{si } \Delta \equiv 0 \ (mod\ 4). \end{cases}$$

Une telle forme existe pour tout $\Delta \equiv 0, 1 \ (mod\ 4)$ puisqu'en calculant le discriminant de $f_0(x,y)$ nous obtenons Δ.

Considérons également une forme quadratique $f = ax^2 + bxy + cy^2$ appartenant à une classe quelconque. Soit maintenant $g = cx^2 + bxy + ay^2$ qui est concordante à f. Alors, en composant selon la loi de Gauss f avec g nous obtenons

$$f * g = acx^2 + bxy + 1y^2 = \begin{pmatrix} r & -1 \\ 1 & 0 \end{pmatrix} f_0(x,y)$$

où

$$r = \begin{cases} \dfrac{-b}{2} & \text{si } 2 \mid \Delta, \\ \dfrac{-(b-1)}{2} & \text{sinon.} \end{cases}$$

Nous obtenons ainsi via la composition de Gauss, une structure de groupe abélien sur l'ensemble des classes d'équivalence. Il s'avère que ce groupe est fini. On peut consulter [13] pour plus amples détails sur ce résultat profond.

Chapitre 2

Lois de composition de Bhargava

Nous verrons ici qu'il existe un autre moyen de structurer les classes d'équivalence sous forme de groupe. En effet, grâce aux travaux du mathématicien Manjul Bhargava, notamment dans [1], il nous est possible d'associer une forme quadratique à un cube de dimension $2 \times 2 \times 2$ ou autrement dit, de relier l'espace des formes quadratiques à l'espace de ces mêmes cubes. Ainsi, Bhargava formula une loi encore plus générale que celle de Gauss au sens où elle donne naissance à d'autres lois de composition.

2.1 Loi du cube

Nous mettrons en relief dans cette section comment Bhargava réussit à extirper d'un cube $2 \times 2 \times 2$ trois formes quadratiques. Nous énoncerons également une loi fondamentale, celle du cube, à partir de laquelle nous retrouverons implicitement la loi de composition de Gauss vue précédemment. Il nous sera ainsi possible de relier l'espace des cubes et l'espace des formes quadratiques, mais voyons tout d'abord comment à l'aide de ce qu'il appelle les *coupes fondamentales* Bhargava génère ses trois formes.

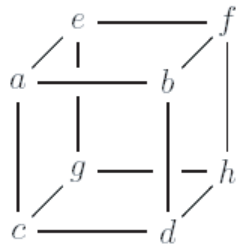
2.1.1 Cube et formes quadratiques

Il s'agit tout d'abord de considérer un vecteur de l'espace tensoriel

$$C_2 := \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$$

comme un cube de dimension $2 \times 2 \times 2$. En effet, puisque $C_2 \simeq \mathbb{Z}^8$, nous avons que C_2 est un groupe abélien libre de rang 8. Notons par $\{e_1, e_2\}$ la base standard de $\mathbb{Z}^2$. Nous obtenons ainsi avec les propriétés du produit tensoriel une base pour l'espace C_2 soit la base formée des vecteurs $e_i \otimes e_j \otimes e_k$ pour tout $1 \leq i, j, k \leq 2$.

La prochaine étape consiste à tisser le lien qui unit l'espace des cubes à celui des formes quadratiques. En fait, trois formes quadratiques peuvent être induites d'un cube $A \in C_2$. Pour ce faire, nous devons couper le cube selon trois plans distincts séparant celui-ci en deux matrices 2×2 pour chaque coupe.



Cube A

Ainsi, le cube A ci-haut peut s'écrire

$$ae_1 \otimes e_1 \otimes e_1 + be_1 \otimes e_2 \otimes e_1 + ce_2 \otimes e_1 \otimes e_1 + de_2 \otimes e_2 \otimes e_1$$
$$+ ee_1 \otimes e_1 \otimes e_2 + fe_1 \otimes e_2 \otimes e_2 + ge_2 \otimes e_1 \otimes e_2 + he_2 \otimes e_2 \otimes e_2,$$

ce qui nous permet d'associer un vecteur de C_2 à un cube entier ($a, b, c, d, e, f, g, h \in \mathbb{Z}$) et ainsi relier les deux espaces.

Première coupe : (*Devant-Derrière*)

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Deuxième coupe : (*Gauche-Droite*)

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \quad \text{et} \quad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}.$$

Troisième coupe : (*Haut-Bas*)

$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix} \quad \text{et} \quad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}.$$

Nous pouvons donc à partir de ce cube A et des matrices ainsi obtenues construire les trois formes quadratiques suivantes :

$$\begin{cases} Q_1^A(x,y) = -\text{Dét}(M_1x - N_1y), \\ Q_2^A(x,y) = -\text{Dét}(M_2x - N_2y), \\ Q_3^A(x,y) = -\text{Dét}(M_3x - N_3y). \end{cases}$$

Explicitement, nous obtenons les formes :

$$\begin{cases} Q_1^A(x,y) = (bc-ad)x^2 + (ah+ed-bg-cf)xy + (fg-eh)y^2, \\ Q_2^A(x,y) = (ce-ag)x^2 + (ah+bg-cf-ed)xy + (df-bh)y^2, \\ Q_3^A(x,y) = (eb-af)x^2 + (ah+cf-ed-bg)xy + (gd-ch)y^2. \end{cases}$$

2.1.2 Action de $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$

Comme nous avons pu le voir dans le chapitre d'introduction, le groupe multiplicatif $SL_2(\mathbb{Z})$ joue un rôle primordial dans le regroupement des formes quadratiques en classes d'équivalence. Il serait intéressant à présent de définir, le plus naturellement possible, une action de groupe agissant sur un cube $A \in C_2$. Définissons donc l'action du groupe $SL_2(\mathbb{Z})\times SL_2(\mathbb{Z})\times SL_2(\mathbb{Z})$ agissant sur un cube en opérant sur ses six matrices associées.

Soit

$$\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3) = \begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} \times \begin{pmatrix} r_2 & s_2 \\ t_2 & u_2 \end{pmatrix} \times \begin{pmatrix} r_3 & s_3 \\ t_3 & u_3 \end{pmatrix} \in SL_2(\mathbb{Z})\times SL_2(\mathbb{Z})\times SL_2(\mathbb{Z})$$

et $A \in C_2$ avec ses 6 matrices associées au moyen des 3 coupes fondamentales, c'est-à-dire M_1 et N_1, M_2 et N_2 ainsi que M_3 et N_3. Alors, l'action de Γ sur le cube A est définie en faisant agir, peu importe l'ordre, chacun des 3 éléments de $SL_2(\mathbb{Z})$ qui composent Γ.

Pour décrire complètement le cube A, il est évident qu'il suffit de considérer seulement l'une des trois coupes mentionnées plus haut. Pour décrire l'action de Γ sur A, il faut tout d'abord appliquer Γ_1 sur la coupe *Devant-Derrière* de A pour obtenir le cube A' dont la coupe respective *Devant-Derrière* sera

$$M_1' = r_1 M_1 + s_1 N_1 \quad \text{et} \quad N_1' = t_1 M_1 + u_1 N_1.$$

Il faut ensuite appliquer Γ_2 sur la coupe *Gauche-Droite* de A' pour ainsi obtenir le cube A'' dont la coupe *Gauche-Droite* sera

$$M_2'' = r_2 M_2' + s_2 N_2' \quad \text{et} \quad N_2'' = t_2 M_2' + u_2 N_2'.$$

Finalement, il faut appliquer Γ_3 sur la coupe *Haut-Bas* du cube A'' pour obtenir le cube A''' dont la coupe *Haut-Bas* sera

$$M_3''' = r_3 M_3'' + s_3 N_3'' \quad \text{et} \quad N_3''' = t_3 M_3'' + u_3 N_3''.$$

On démontrera dans un instant que l'ordre Γ_1, Γ_2, Γ_3 n'importe pas. Il suffira en fait de vérifier que Γ_1 suivi de Γ_2 donne le même résultat que Γ_2 suivi de Γ_1.

Cette description en étapes subséquentes peut également être considérée comme une composition des 3 éléments de Γ. En effet, puisque l'identité de $SL_2(\mathbb{Z})$, noté ici Id, n'altère en rien la coupe sur laquelle elle est appliquée, on a que

$$\Gamma = (Id \times Id \times \Gamma_3) \circ (Id \times \Gamma_2 \times Id) \circ (\Gamma_1 \times Id \times Id).$$

Il est toutefois primordial de souligner le fait que chacun des Γ_i doit opérer sur sa coupe respective. Par exemple, pour $\Gamma_1 \times Id \times Id$, Γ_1 agit sur la coupe *Devant-Derrière*. Si par inadvertance, dans le même exemple, Γ_1 agissait sur une autre coupe, alors il en résulterait un cube totalement différent n'ayant plus aucun lien avec la conception de Γ telle qu'imaginée par Bhargava. Sous cette action, il est possible de regrouper les cubes en classes d'équivalence de la même façon que $SL_2(\mathbb{Z})$ regroupe les formes quadratiques.

Le lemme suivant soulève le fait important que l'action des Γ_i commute, puisque selon Bhargava ([1]) celles-ci correspondent à des opérations matricielles commutatives de lignes et de colonnes dans $M_{2\times 2}(\mathbb{Z})$. Ainsi, comme nous le montrerons, le cube d'arrivée est invariant en ce qui concerne le choix de l'ordre des applications Γ_i.

Lemme. Soit $\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3)$. Alors les Γ_i pour $1 \leq i \leq 3$, commutent entre eux.

DÉMONSTRATION. Il est suffisant de démontrer que Γ_1 commute avec Γ_2. Soit $\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3)$ dont les entrées de Γ_1 et de Γ_2 sont explicitement données par

$$\Gamma_1 = \begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} \text{ et } \Gamma_2 = \begin{pmatrix} r_2 & s_2 \\ t_2 & u_2 \end{pmatrix}.$$

Soit un cube A dont les matrices associées aux deux premières coupes sont

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \text{ et } N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}.$$

On calcule premièrement l'action de Γ_1 appliquée à la coupe *Devant-Derrière* de A à laquelle on fera suivre celle de Γ_2 appliquée à la coupe *Gauche-Droite* du nouveau cube ainsi obtenu. On a donc pour Γ_1 par rapport à A :

$$M_1' = r_1 M_1 + s_1 N_1 \quad \text{et} \quad N_1' = t_1 M_1 + u_1 N_1,$$

c'est-à-dire

$$M_1' = \begin{pmatrix} r_1 a + s_1 e & r_1 b + s_1 f \\ r_1 c + s_1 g & r_1 d + s_1 h \end{pmatrix}, \; N_1' = \begin{pmatrix} t_1 a + u_1 e & t_1 b + u_1 f \\ t_1 c + u_1 g & t_1 d + u_1 h \end{pmatrix}.$$

Ces deux matrices définissent un autre cube que l'on notera A' dont la coupe *Gauche-Droite* correspond à

$$M_2' = \begin{pmatrix} r_1 a + s_1 e & r_1 c + s_1 g \\ t_1 a + u_1 e & t_1 c + u_1 g \end{pmatrix},$$

$$N_2' = \begin{pmatrix} r_1 b + s_1 f & r_1 d + s_1 h \\ t_1 b + u_1 f & t_1 d + u_1 h \end{pmatrix}.$$

On applique par la suite Γ_2 à cette coupe, ce qui définira un nouveau cube A'' dont les matrices M_2'' et N_2'' sont données par

$$M_2'' = r_2 M_2' + s_2 N_2' \quad \text{et} \quad N_2'' = t_2 M_2' + u_2 N_2',$$

c'est-à-dire

$$M_2'' = \begin{pmatrix} r_2 r_1 a + r_2 s_1 e + s_2 r_1 b + s_2 s_1 f & r_2 r_1 c + r_2 s_1 g + s_2 r_1 d + s_2 s_1 h \\ r_2 t_1 a + r_2 u_1 e + s_2 t_1 b + s_2 u_1 f & r_2 t_1 c + r_2 u_1 g + s_2 t_1 d + s_2 u_1 h \end{pmatrix},$$

$$N_2'' = \begin{pmatrix} t_2 r_1 a + t_2 s_1 e + u_2 r_1 b + u_2 s_1 f & t_2 r_1 c + t_2 s_1 g + u_2 r_1 d + u_2 s_1 h \\ t_2 t_1 a + t_2 u_1 e + u_2 t_1 b + u_2 u_1 f & t_2 t_1 c + t_2 u_1 g + u_2 t_1 d + u_2 u_1 h \end{pmatrix}.$$

Calculons maintenant l'ordre inverse en appliquant cette fois Γ_2 suivi de Γ_1. Lorsqu'on fait agir Γ_2 sur la coupe *Gauche-Droite* de A, on obtient

$$M_2' = r_2M_2 + s_2N_2 \quad \text{et} \quad N_2' = t_2M_2 + u_2N_2,$$

soit précisément

$$M_2' = \begin{pmatrix} r_2a + s_2e & r_2b + s_2f \\ r_2c + s_2g & r_2d + s_2h \end{pmatrix},$$

$$N_2' = \begin{pmatrix} t_2a + u_2e & t_2b + u_2f \\ t_2c + u_2g & t_2d + u_2h \end{pmatrix}.$$

Ces deux matrices définissent un autre cube que l'on notera A' dont la coupe *Devant-Derrière* correspond à

$$M_1' = \begin{pmatrix} r_2a + s_2e & t_2a + u_2b \\ r_2c + s_2d & t_2c + u_2d \end{pmatrix},$$

$$N_1' = \begin{pmatrix} r_2e + s_2f & t_2e + u_2f \\ r_2g + s_2h & t_2g + u_2h \end{pmatrix}.$$

On applique par la suite Γ_1 à cette coupe, ce qui définira un nouveau cube A'' dont les matrices M_1'' et N_1'' sont données par

$$M_1'' = r_1M_1' + s_1N_1' \quad \text{et} \quad N_1'' = t_1M_1' + u_1N_1',$$

c'est-à-dire

$$M_1'' = \begin{pmatrix} r_2r_1a + r_1s_2b + s_1r_2e + s_1s_2f & t_2r_1a + t_2s_1e + u_2r_1b + u_2s_1f \\ r_2r_1c + r_2s_1g + s_2r_1d + s_2s_1h & t_2r_1c + t_2s_1g + u_2r_1d + u_2s_1h \end{pmatrix},$$

$$N_1'' = \begin{pmatrix} r_2t_1a + r_2u_1e + s_2t_1b + s_2u_1f & t_2t_1a + t_2u_1e + u_2t_1b + u_2u_1f \\ r_2t_1c + r_2u_1g + s_2t_1d + s_2u_1h & t_2t_1c + t_2u_1g + u_2t_1d + u_2u_1h \end{pmatrix}.$$

La coupe *Gauche-Droite* de A'' correspond aux deux matrices suivantes :

$$M_2'' = \begin{pmatrix} r_2r_1a + r_2s_1e + s_2r_1b + s_2s_1f & r_2r_1c + r_2s_1g + s_2r_1d + s_2s_1h \\ r_2t_1a + r_2u_1e + s_2t_1b + s_2u_1f & r_2t_1c + r_2u_1g + s_2t_1d + s_2u_1h \end{pmatrix},$$

$$N_2'' = \begin{pmatrix} t_2r_1a + t_2s_1e + u_2r_1b + u_2s_1f & t_2r_1c + t_2s_1g + u_2r_1d + u_2s_1h \\ t_2t_1a + t_2u_1e + u_2t_1b + u_2u_1f & t_2t_1c + t_2u_1g + u_2t_1d + u_2u_1h \end{pmatrix}.$$

À la lumière de ces calculs, on constate que dans les deux cas, c'est-à-dire $\Gamma_2 \circ \Gamma_1$ et $\Gamma_1 \circ \Gamma_2$, la coupe *Gauche-Droite* de A'' est identique. Ainsi, peu importe l'ordre de

composition, on termine toujours en présence du même cube ce qui implique la commutativité de Γ.

C.Q.F.D.

Prenons par exemple le cube A dont la coupe *Devant-Derrière* correspond à

$$M_1 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \quad \text{et} \quad N_1 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

et l'action $\Gamma = (\Gamma_1, \Gamma_2, \Gamma_3) = \left(\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$.
Ainsi, Γ_1 appliquée à la coupe *Devant-Derrière* de A donne

$$M_1' = 2M_1 + 1N_1 = \begin{pmatrix} 3 & 6 \\ 5 & 5 \end{pmatrix} \quad \text{et} \quad N_1' = 1M_1 + 1N_1 = \begin{pmatrix} 2 & 4 \\ 3 & 3 \end{pmatrix},$$

Ces deux matrices définissent le nouveau cube A'. On applique par la suite Γ_2 à la coupe *Gauche-Droite* de A' ce qui donne

$$M_2'' = 2M_2' + 3N_2' = \begin{pmatrix} 24 & 25 \\ 16 & 15 \end{pmatrix} \quad \text{et} \quad N_2'' = 1M_2' + 2N_2' = \begin{pmatrix} 15 & 15 \\ 10 & 9 \end{pmatrix}.$$

Ces deux matrices sont également suffisantes pour décrire le nouveau cube A'' sur lequel on fait agir Γ_3 sur la coupe *Haut-Bas*. Ce qui donne

$$M_3''' = 1M_3'' + 0N_3'' = \begin{pmatrix} 24 & 16 \\ 15 & 10 \end{pmatrix} \quad \text{et} \quad N_3''' = 0M_3'' + 1N_3'' = \begin{pmatrix} 25 & 15 \\ 15 & 9 \end{pmatrix}.$$

De cette façon, on obtient le nouveau cube A''' par l'action de Γ sur le cube A.

2.1.3 Discriminant

Nous avons remarqué dans l'introduction de ce mémoire que les classes d'équivalence sont en nombre fini si le discriminant est fixé et infini autrement. Tout comme pour les formes quadratiques, il serait intéressant de pouvoir parler du discriminant d'un cube et ainsi être en mesure d'en tirer des conclusions analogues à celles sur le discriminant d'une forme quadratique. Pour ce faire, nous constaterons que les trois formes reliées au cube ont tous le même discriminant. Il suffit donc de poser le discriminant d'un cube

égal à celui des trois formes quadratiques associées.

Plus en détails, un simple calcul nous permet de montrer que le discriminant de Q_1 est

$$disc(Q_1) = a^2h^2+b^2g^2+c^2f^2+d^2e^2-2(abgh+cdef+acfh+bdeg+aedh+bfcg)+4(adfg+bceh).$$

En effet,

$$Q_1(x,y) = -\text{Dét}(M_1x - N_1y)$$

$$= -\text{Dét}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} x - \begin{pmatrix} e & f \\ g & h \end{pmatrix} y \right)$$

$$= -\text{Dét}\left(\begin{pmatrix} ax & bx \\ cx & dx \end{pmatrix} - \begin{pmatrix} ey & fy \\ gy & hy \end{pmatrix} \right)$$

$$= -\text{Dét} \begin{pmatrix} ax-ey & bx-fy \\ cx-gy & dx-hy \end{pmatrix}$$

$$= adx^2 - ahxy - edxy + ehy^2 - bcx^2 + bgxy + cfxy - fgy^2.$$

Ce qui, en regroupant les termes, nous donne la nouvelle forme quadratique

$$(ad-bc)x^2 + (bg+cf-ah-ed)xy + (eh-fg)y^2,$$

dont nous savons calculer le discriminant en utilisant la formule $B^2 - 4AC$ avec

$$\begin{cases} A = (ad-bc), \\ B = (bg+cf-ah-ed), \\ C = (eh-fg). \end{cases}$$

Nous obtenons ainsi le résultat escompté.

Par des calculs semblables, nous trouvons la même valeur pour le discriminant de Q_2 et de Q_3. Nous noterons tout simplement cette valeur commune le *discriminant du cube* A ou $Disc(A)$.

2.1.4 Composition de Gauss revue

Nous voilà prêts, après ces quelques préambules, à formuler la loi centrale des travaux de Manjul Bhargava, c'est-à-dire la loi du cube sous laquelle on retrouve implicitement la loi de composition de Gauss telle qu'imaginée autour des années 1800 ([7]).

Définition. *Loi du cube* : $Q_1^A + Q_2^A + Q_3^A = 0$, où Q_1^A, Q_2^A et Q_3^A sont trois formes quadratiques associées au cube $A \in C_2$.

Ici, la loi du cube doit se lire à équivalence près, soit $[Q_1^A] + [Q_2^A] + [Q_3^A] = 0$, où 0 représente l'élément neutre du groupe de classes de formes quadratiques et où le signe '+' correspond à la composition des formes. Autrement dit, la loi du cube stipule qu'en additionnant les trois formes quadratiques associées à un même cube, nous obtenons 0. À première vue cette loi peut sembler étrange mais voyons ce qui se cache sous celle-ci.

On peut remarquer le lien entre cette loi et la relation d'équivalence sous l'action des éléments de $SL_2(\mathbb{Z})$ en regardant l'action d'un élément γ. Prenons en effet $\Gamma = \gamma \times id \times id$ où γ est une matrice de $SL_2(\mathbb{Z})$. En faisant agir Γ sur un cube donné $A \in C_2$, nous obtenons un nouveau cube disons, $A' = \Gamma A$. Ce cube A', donne naissance à trois autres formes quadratiques. Nous avons donc d'un côté les trois formes quadratiques associées au cube A : Q_1^A, Q_2^A et Q_3^A et celles du nouveau cube A' : $Q_1^{A'}$, $Q_2^{A'}$ et $Q_3^{A'}$. Il s'avère que $Q_1^{A'}$ est égale à γQ_1^A. Montrons en effet cette dernière assertion.

Démonstration. Soit A le cube dont les matrices de la coupe *Devant-Derrière* sont

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Soit de plus $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$. Ainsi γ de (M_1, N_1) donne

$$M_1' = \begin{pmatrix} ra + se & rb + sf \\ rc + sg & rd + sh \end{pmatrix} \quad \text{et} \quad N_1' = \begin{pmatrix} ta + ue & tb + uf \\ tc + ug & td + uh \end{pmatrix}.$$

Alors, M_1' et N_1' donnent naissance au cube A'. De chacun de ces deux cubes, A et A', on peut mettre en évidence une des trois formes quadratiques associées. Dans le cas présent, on a

$$Q_1^A(x,y) = (bc-ad)x^2 + (ah+ed-bg-cf)xy + (fg-eh)y^2$$

$$Q_1^{A'}(x,y) = ((rb+sf)(rc+sg) - (ra+se)(rd+sh))x^2$$
$$+((ra+se)(td+uh) + (ta+ue)(rd+sh) - (rb+sf)(tc+ug) - (rc+sg)(tb+uf))xy$$
$$+((tb+uf)(tc+ug) - (ta+ue)(td+uh))y^2.$$

Pour simplifier la notation, utilisons les variables suivantes :

$$A = (bc-ad),$$
$$B = (ah+ed-bg-cf),$$
$$C = (fg-eh).$$

Ainsi, $Q_1^A(x,y)$ s'exprime plus simplement par

$$Q_1^A(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Si on calcule maintenant $\gamma Q_1^A(x,y)$, on obtient

$$\gamma Q_1^A(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}^t \begin{pmatrix} x \\ y \end{pmatrix}.$$

La matrice associée à la forme quadratique est donnée par

$$M_{\gamma Q_1^A} = \begin{pmatrix} r(rA+sB/2)+s(rB/2+sC) & t(rA+sB/2)+u(rB/2+sC) \\ r(tA+uB/2)+s(tB/2+uC) & t(tA+uB/2)+u(tB/2+uC) \end{pmatrix}.$$

En calculant par la suite

$$\begin{pmatrix} x & y \end{pmatrix} M_{\gamma_1 Q_1^A} \begin{pmatrix} x \\ y \end{pmatrix}$$

avec les valeurs préalablement attribuées à A, B et C, on obtient bien la forme quadratiques $Q_1^{A'}(x,y)$.

C.Q.F.D.

Cette démonstration est immédiate via la loi du cube qui stipule que la somme des trois formes quadratiques associées à un même cube est nulle. En effet, nous avons constaté qu'appliquer $\gamma \times Id \times Id$ à un cube A donnait un cube A' dont les formes quadratiques associées ne différaient de celles de A que pour $Q_1^{A'}$ et que pour obtenir cette dernière, il suffisait de calculer γQ_1^A. En reprenant essentiellement la même preuve, mais pour $Id \times \gamma \times Id$, on obtient que les formes quadratiques associées au cube A' ne diffèrent de celles de A que pour la deuxième forme et que $Q_2^{A'} = \gamma Q_2^A$. De même façon, $Id \times Id \times \gamma$ donne $Q_3^{A'} = \gamma Q_3^A$. Ainsi, $\gamma \times Id \times Id$ appliquée à A donne un cube A' dont les 3 formes quadratiques associées sont $Q_1^{A'} = \gamma Q_1^A$, $Q_2^{A'} = IdQ_2^A$ et $Q_3^{A'} = IdQ_3^A$. La loi du cube implique donc que

$$Q_1^A + Q_2^A + Q_3^A = 0 \quad \text{et} \quad \gamma Q_1^A + IdQ_2^A + IdQ_3^A = 0,$$

d'où $Q_1^A + Q_2^A + Q_3^A = \gamma Q_1^A + Q_2^A + Q_3^A$ et $Q_1^A = \gamma Q_1^A$. La dernière égalité veut dire que la classe de Q_1^A est la classe de γQ_1^A.

Ainsi, Q_1^A et $Q_1^{A'} = \gamma Q_1^A$ sont $SL_2(\mathbb{Z})$-équivalentes. Les deux autres formes restent fixes sous l'action de la matrice identité des composantes 2 et 3 de Γ. Ces calculs mettent en relief le fait que la loi du cube identifie les formes quadratiques qui sont $SL_2(\mathbb{Z})$-équivalentes, soit dans notre exemple Q_1^A et γQ_1^A.

2.2 Lois de groupe

2.2.1 Groupe de classes de formes quadratiques

Outre cette identification, la loi du cube est à la base du regroupement des formes quadratiques sous une structure de groupe. D'une manière analogue à celle de Gauss, Manjul Bhargava nous propose de regrouper les formes quadratiques selon des classes d'équivalence, sauf que dans le dernier cas, les classes seront construites à l'aide de l'action de $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ et de la loi du cube. Le théorème qui suit a été démontré par Bhargava et met en évidence l'existence d'une loi de groupe sur l'ensemble des classes de formes quadratiques. Notons par $[Q_i]$ la classe d'équivalence de la forme quadratique Q_i pour $i = 1, 2, 3$.

Théorème 1.1. *Soit $D \in \mathbb{Z}$ tel que $D \equiv 0, 1$ (mod 4) et soit $Q_{id,D}$ n'importe quelle forme quadratique primitive de discriminant D telle qu'il existe un cube A_0 avec*

$Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = Q_{id,D}$. *Alors, il existe une loi de groupe sur l'ensemble des classes de formes quadratiques primitives $SL_2(\mathbb{Z})$-équivalentes de discriminant D telle que* :

(1) $[Q_{id,D}]$ *est l'élément neutre additif de ce groupe.*

(2) $\forall A \in C_2$, *avec* $disc(A) = D$ *et* Q_1^A, Q_2^A et Q_3^A *primitives, nous avons à l'intérieur du groupe de classes de formes quadratiques primitives que la somme des classes de* Q_1^A, Q_2^A *et* Q_3^A *respectivement est la classe de la forme* $Q_{id,D}$:

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

Inversement, soit Q_1, Q_2 et Q_3 trois formes données telles qu'à l'intérieur du groupe de classes des formes quadratiques primitives de discriminant D nous ayons $[Q_1] + [Q_2] + [Q_3] = [Q_{id,D}]$. Alors il existe un cube $A \in C_2$ de discriminant D, unique à Γ-équivalence près, tel que $Q_1^A = Q_1$, $Q_2^A = Q_2$ et $Q_3^A = Q_3$.

Démonstration. Voir [1] section 3.3.

C.Q.F.D.

Autrement dit, le Théorème 1.1 stipule qu'en choisissant judicieusement un neutre additif, $[Q_{id,D}]$, la loi du cube à elle seule structure les classes de formes quadratiques primitives de discriminant D en un groupe. De plus, la loi de groupe sous-jacente à cette structure est unique.

Voyons à présent quel serait le choix le plus naturel pour $Q_{id,D}$. En introduction à ce mémoire, nous avons remarqué que le neutre pour la composition des classes d'équivalence chez Gauss, était la classe que l'on avait notée C_0 de la forme quadratique

$$f_0(x,y) = \begin{cases} x^2 + xy + \dfrac{(1-\Delta)}{4}y^2 & \text{si } \Delta \equiv 1 \ (mod\ 4), \\ x^2 - \dfrac{\Delta}{4}y^2 & \text{si } \Delta \equiv 0 \ (mod\ 4). \end{cases}$$

Choisissons donc notre forme $Q_{id,D}$, parallèlement aux travaux de Gauss ([7]), comme suit :

$$Q_{id,D} = \begin{cases} x^2 + xy + \dfrac{(1-\Delta)}{4}y^2 & \text{si } \Delta \equiv 1 \ (mod\ 4), \\ x^2 - \dfrac{\Delta}{4}y^2 & \text{si } \Delta \equiv 0 \ (mod\ 4). \end{cases}$$

Bien entendu, il nous est possible de prendre comme élément neutre une autre forme quadratique que celle choisie par Gauss. Notons cependant qu'en choisissant l'élément neutre additif tel que défini plus haut, nous obtenons la même loi de composition que celle de Gauss. De plus, comme mentionné dans le Théorème 1.1, cette loi est unique. En faisant varier l'élément neutre, nous pouvons obtenir d'autres lois de groupe sur l'ensemble des classes d'équivalence. C'est en ce sens que les lois de groupe étudiées par Manjul Bhargava englobent celle de Gauss puisqu'elle n'est qu'une des quatorze lois de composition sous-jacentes à ce qu'il appelle ses *Higher composition laws* ([1]). Chacune de ses lois nous permet de mieux comprendre les corps de nombres et leur groupes de classes.

On remarquera qu'il nous est possible pour $Q_{id,D}$, et ce peu importe la classe de congruence de Δ, d'exhiber un cube A_0 satisfaisant l'hypothèse du Théorème 1.1., c'est-à-dire, un cube où ses trois formes quadratiques sont toutes égales à $Q_{id,D}$. En effet, si l'on calcule les trois formes quadratiques associées aux deux cubes ci-bas, on obtient la forme $Q_{id,D}$ correspondant à la classe de congruence de Δ. Par exemple, dans le cas du cube de la figure 2.2, c'est-à-dire où $\Delta = D \equiv 0(mod\ 4)$, on obtient

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad N_1 = \begin{pmatrix} 1 & 0 \\ 0 & D/4 \end{pmatrix}.$$

$$M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad N_2 = \begin{pmatrix} 1 & 0 \\ 0 & D/4 \end{pmatrix}.$$

$$M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad N_3 = \begin{pmatrix} 1 & 0 \\ 0 & D/4 \end{pmatrix}.$$

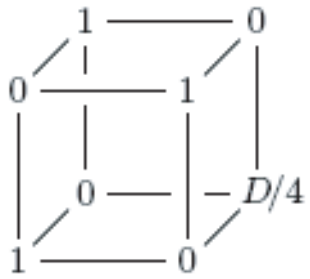
Ainsi, $Q_1^{A_0}(x,y) = -\text{Dét}(M_1x - N_1y) = -\text{Dét}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}x - \begin{pmatrix} 1 & 0 \\ 0 & D/4 \end{pmatrix}y\right) = -\text{Dét}\begin{pmatrix} -y & x \\ x & -Dy/4 \end{pmatrix} = x^2 - y^2D/4.$

De la même façon, on a $Q_2^{A_0}(x,y) = Q_3^{A_0}(x,y) = x^2 - y^2 D/4$.

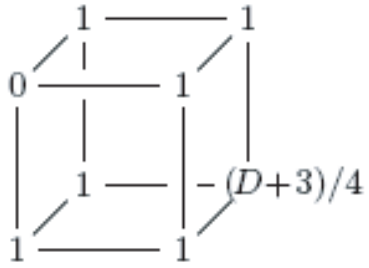
Par souci de commodité, nous noterons l'ensemble des classes de formes quadratiques primitives $SL_2(\mathbb{Z})$-équivalentes de discriminant D muni de cette unique loi de composition définie au Théorème 1.1 par $Cl((Sym^2\mathbb{Z}^2)^*; D)$.

2.2.2 Groupe de classes de cubes

Nous avons vu, dans les travaux de Bhargava, que la loi du cube et la structure de groupe sur les classes d'équivalence de formes vont de pair. Que cette complicité donnait naissance ou impliquait l'existence d'un cube A_0 dont les trois formes associées étaient égales à $Q_{id,D}$. En fait, nous allons voir que ce même cube joue un rôle primordial dans l'espace des cubes. Nous verrons qu'en prenant la classe d'équivalence du cube A_0 nous obtenons l'identité d'un nouveau groupe, le groupe des classes d'équivalence de cubes dont le discriminant est D. En ce sens, nous introduirons une nouvelle notation pour le cube A_0 soit $A_{id,D}$.



Cube $A_{id,D}$ si $D \equiv 0 \ (mod\ 4)$



Cube $A_{id,D}$ si $D \equiv 1 \ (mod\ 4)$

Définition. Un cube $A \in C_2$ est dit *projectif* si ses formes quadratiques associées

Q_1^A, Q_2^A et Q_3^A sont primitives.

Nous utiliserons, tout comme pour les formes quadratiques, une action de groupe afin de regrouper les cubes sous une relation d'équivalence. Toutefois, nous utiliserons l'action de Γ au lieu de celle de $SL_2(\mathbb{Z})$. Nous parlerons donc de cubes Γ-équivalents et de classes Γ-équivalentes et noterons tout simplement $[A]$ la classes d'équivalence du cube A.

Théorème 1.2. ([1]) *Soit $D \in \mathbb{Z}$ tel que $D \equiv 0, 1$ (mod 4) et soit $A_{id,D}$ le cube de la figure 2.3. Alors, il existe une unique loi de groupe sur l'ensemble des classes de cubes projectifs Γ-équivalents de discriminant fixé D telle que :*

(1) *$[A_{id,D}]$ soit l'élément neutre additif de ce groupe,*

(2) *les fonctions*

$$\begin{cases} f_1 : [A] \mapsto Q_1^A, \\ f_2 : [A] \mapsto Q_2^A, \\ f_3 : [A] \mapsto Q_3^A, \end{cases}$$

soit des homomorphismes de groupes dans $Cl((Sym^2\mathbb{Z}^2)^*; D)$.

De simples calculs nous permettent de relier les Théorèmes 1.1 et 1.2. En effet, en prenant deux cubes projectifs A et $A' \in C_2$ de discriminant D, nous pouvons en extraire 6 formes quadratiques. Soit Q_1^A, Q_2^A et Q_3^A les formes associées au cube A et $Q_1^{A'}$, $Q_2^{A'}$, $Q_3^{A'}$ celles associées à A'. Ainsi, d'après le Théorème 1.1, nous avons que

$$[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{id,D}] \quad \text{et} \quad [Q_1^{A'}] + [Q_2^{A'}] + [Q_3^{A'}] = [Q_{id,D}].$$

Nous obtenons donc en regroupant les termes

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

D'après la partie (2) du Théorème 1.1, nous savons qu'il existe un cube, disons $A'' \in C_2$, tel que :

$$[Q_1^{A''}] = (\ [Q_1^A] + [Q_1^{A'}]\ ),$$
$$[Q_2^{A''}] = (\ [Q_2^A] + [Q_2^{A'}]\ ),$$

$$[Q_3^{A''}] = (\ [Q_3^{A}] + [Q_3^{A'}]\ ).$$

Ainsi, nous pouvons définir la loi d'addition pour le groupe des classes de cubes projectifs de discriminant D comme

$$[A''] = [A] + [A']$$

et nous noterons $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2)$ ce groupe muni de cette loi.

2.2.3 Composition des formes cubiques binaires

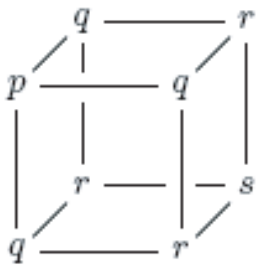
La loi de composition sur les cubes présentée précédemment induit non seulement une loi de composition sur les classes de formes quadratiques binaires mais également sur les classes de formes cubiques binaires $SL_2(\mathbb{Z})$-équivalentes. Nous allons voir qu'en réalité l'espace des formes cubiques binaires s'injecte de manière naturelle dans l'espace des cubes $2 \times 2 \times 2$.

On peut associer à la forme quadratique, $f(x, y) = px^2 + 2qxy + ry^2$, la matrice symétrique 2×2 suivante :

$$M_{f(x,y)} = \begin{pmatrix} p & q \\ q & r \end{pmatrix}.$$

Il nous est possible d'extrapoler cette association aux formes cubiques.

Soit $C(x, y) = px^3+3qx^2y+3rxy^2+sy^3$ une forme cubique. Associons-lui les matrices symétriques $\begin{pmatrix} p & q \\ q & r \end{pmatrix}, \begin{pmatrix} q & r \\ r & s \end{pmatrix}$ extraites des trois coupes possibles du cube suivant.



Cube $\iota(C)$

Si on note par $Sym^3\mathbb{Z}^2$ l'espace des formes cubiques binaires à coefficients centraux triplement symétriques, l'association précédente entre la forme $C(x,y)$ et la matrice $2\times 2\times 2$, qui peut être vue comme un cube $2\times 2\times 2$, n'est rien d'autre que l'inclusion naturelle de $Sym^3\mathbb{Z}^2$ dans l'espace des cubes. C'est-à-dire,

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

Définition. Une forme cubique $C(x,y) = px^3+3qx^2y+3rxy^2+sy^3$ est dite *projective* si son cube triplement symétrique $\iota(C)$ est projectif.

Il est intéressant de remarquer, après de simples calculs, que les trois formes quadratiques naissantes de ce cube $\iota(C)$, c'est-à-dire $Q_1^{\iota(C)}$, $Q_2^{\iota(C)}$ et $Q_3^{\iota(C)}$, sont toutes égales à $-\frac{1}{36}H(C)$ où $H(C)$ est défini comme le Hessien de $C(x,y)$. En résumé,

$$Q_1^{\iota(C)} = Q_2^{\iota(C)} = Q_3^{\iota(C)} = H(x,y)$$

où

$$H(x,y) = (q^2-pr)x^2+(ps-qr)xy+(r^2-qs)y^2$$

$$= -\tfrac{1}{36}\text{Dét}\begin{pmatrix} C_{xx} & C_{xy}\\ C_{yx} & C_{yy}\end{pmatrix}$$

$$= -\tfrac{1}{36}H(C).$$

Ainsi, ce calcul met en relief le fait qu'une forme cubique $C(x,y)$ est projective si et seulement si sa forme quadratique associée $H(x,y)$ est primitive. Dans ce cas, $pgcd((q^2-pr),(ps-qr),(r^2-qs)) = 1$.

En considérant comme identité le cube $A_{id,D}$ précédemment défini, on remarque que $A_{id,D}$ est un cube triplement symétrique et que sa pré-image par l'inclusion naturelle ι correspond à la forme cubique

$$\begin{cases} C_{id,D} = 3x^2y+\dfrac{D}{4}y^3 & \text{si } D\equiv 0 \ (mod\ 4),\\ C_{id,D} = 3x^2y+3xy^2+\dfrac{D+3}{4}y^3 & \text{si } D\equiv 1 \ (mod\ 4).\end{cases}$$

Notons la classe d'équivalence de $C(x,y) := C \in Sym^3\mathbb{Z}^2$ par $[C]$. Nous avons ainsi le théorème suivant de Bhargava analogue à celui des classes de formes quadratiques

montrant l'existence d'une unique loi de groupe.

Théorème 2. ([1]) *Soit $D \in \mathbb{Z}$ tel que $D \equiv 0, 1$ $(mod\ 4)$ et soit $C_{id,D}$ la forme cubique définie plus haut. Alors, il existe une unique loi de groupe sur l'ensemble des classes $SL_2(\mathbb{Z})$-équivalentes de formes cubiques binaires C de discriminant D telle que :*

(1) *$[C_{id,D}]$ soit l'élément neutre additif de ce groupe,*

(2) *la fonction $[C] \to [\iota(C)]$ est un homomorphisme de groupe dans $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$.*

On notera $Cl(Sym^3\mathbb{Z}^2; D)$ l'ensemble des classes d'équivalence de formes cubiques binaires projectives de discriminant D muni de cette loi.

Chapitre 3

Groupe de classes et idéaux

3.1 Rappels sur le groupe de classes

Lorsqu'un anneau commutatif unitaire $\mathbb{A}$ est contenu dans un corps $\mathbb{K}$, il n'est pas toujours vrai que $\mathbb{A}$ soit un domaine à idéaux principaux. Plus concrètement, ou plutôt dans le cas qui nous intéresse, nous prendrons comme anneau $\mathbb{A}$ l'anneau des entiers algébriques d'un corps de nombres et nous verrons que celui-ci n'est pas toujours un anneau à idéaux principaux.

Cependant, il nous est possible de prendre une mesure de l'éloignement de ce même anneau par rapport aux domaines à idéaux principaux. De mesurer, en quelque sorte, à quel point $\mathbb{A}$ s'éloigne de cette propriété. Cette mesure est donnée, comme nous le constaterons, par le nombre de classes, c'est-à-dire par la cardinalité du groupe de classes des idéaux fractionnaires de $\mathbb{A}$. Débutons par de brefs rappels et constatations sur le groupe de classes d'un corps de nombres (voir [8] pour plus amples détails).

Définition. Soit $\mathbb{A}$ un anneau commutatif unitaire sans diviseur de 0 (un domaine d'intégrité) et $\mathbb{K}$ son corps de quotients. Un $\mathbb{A}$-module M contenu dans $\mathbb{K}$ est un *idéal fractionnaire* de $\mathbb{A}$ s'il existe un $a \in \mathbb{A}$ non nul tel que $aM \subseteq \mathbb{A}$.

On remarque qu'en prenant $a = 1$ dans la définition précédente nous obtenons que tous les idéaux de $\mathbb{A}$, au sens usuel, sont fractionnaires et ceux-ci sont appelés idéaux entiers.

L'ensemble des idéaux fractionnaires, que nous noterons $\mathbb{F}$, muni de la loi de multiplication définie pour deux idéaux fractionnaires M et M' comme

$$MM' = \left\{ \sum_{i=1}^{n} m_i m_i' \mid m_i \in M, m_i' \in M', n \in \mathbb{N} \right\},$$

forme un groupe abélien où le neutre multiplicatif est tout l'anneau $\mathbb{A}$ et l'inverse de M est

$$M^{-1} := \{\alpha \in \mathbb{K} \mid \alpha M \subseteq \mathbb{A}\}.$$

Notons maintenant $\mathbb{P}_r$ l'ensemble des idéaux fractionnaires de $\mathbb{A}$ qui sont principaux. On remarque aisément que $\mathbb{P}_r$ est inclut dans $\mathbb{F}$ et on considère le groupe quotient suivant :

$$C(\mathbb{K}) := \mathbb{F}/\mathbb{P}_r$$

que l'on appelle le groupe de classes (des idéaux fractionnaires) de $\mathbb{K}$.

Définition. Soit $\mathbb{A}$ un domaine et $\mathbb{K}$ son corps des quotients. Deux idéaux fractionnaires M et M' sont dit *équivalents* s'il existe un $x \in \mathbb{K}$ non nul tel que $M = \langle x \rangle M'$ où $\langle x \rangle$ est l'idéal fractionnaire engendré par x.

Ainsi avec cette relation d'équivalence, nous constatons que $\mathbb{P}_r$ est simplement le sous-groupe des idéaux fractionnaires qui sont équivalents à l'idéal unité, soit tout le domaine $\mathbb{A}$.

Le nombre de classes d'équivalence de $C(\mathbb{K})$ sera noté par $h_{\mathbb{K}}$. C'est à proprement parler ce nombre qui nous permettra de prendre une mesure de l'éloignement de $\mathbb{A}$ de la propriété d'être un domaine à idéaux principaux. Plus $h_{\mathbb{K}}$ est grand, plus $\mathbb{A}$ s'éloigne du domaine à idéaux principaux.

Au point de vue historique, c'est à Gauss ([7]) que l'on doit une bonne partie de l'étude consacrée au groupe de classes d'un corps quadratique et à Kummer celle du groupe de classes d'un corps cyclotomique. Notons que parler d'un groupe de classes d'un corps est en soit un abus de language, les seuls idéaux d'un corps sont $\langle 0 \rangle$ et le corps lui-même. Il est donc sous-entendu qu'en parlant de groupe de classes d'un corps de nombres, nous voulons plutôt signifier le groupe de classes de l'anneau des entiers algébriques du corps en question.

3.2 Formes et idéaux

3.2.1 Fonction Trace

Dans la section qui suit, nous travaillerons dans un anneau R commutatif et unitaire dont le groupe additif est isomorphe à $\mathbb{Z}^2$, c'est-à-dire un groupe libre de rang 2. De tels anneaux sont appelés des anneaux quadratiques. Ce type d'anneaux introduit par Manjul Bhargava dans [3], permet une étude plus globale de certains aspects de la théorie algébrique des nombres puisqu'il inclut le cas spécifique d'anneaux des entiers d'un corps de nombres. Débutons par une définition qui est un cas particulier de ce type d'anneaux.

Définition. Soit $\mathbb{K}$ un corps de nombres de degré n sur $\mathbb{Q}$. Alors un *ordre* $\mathcal{O}$ de $\mathbb{K}$ est un sous-anneau de l'anneau des entiers $\mathcal{O}_K$ de $\mathbb{K}$ avec générateurs dans $\mathbb{Z}$ incluant 1.

Par définition (voir [8]), nous avons que tous les ordres d'un corps de nombres $\mathbb{K}$ sont contenus dans l'ordre maximal $\mathcal{O}_K$, l'anneau des entiers algébriques de $\mathbb{K}$.

Faisons maintenant un bref rappel sur une fonction qui nous sera d'une grande utilité dans ce qui suivra, la fonction Trace. Il existe un théorème d'algèbre qui démontre l'existence d'une bijection entre le groupe $M_n(\mathbb{Z})$ des matrices $n \times n$ à coefficients dans $\mathbb{Z}$ et le groupe $\mathcal{L}(\mathbb{A}, \mathbb{A})$ des endormorphismes d'un anneau $\mathbb{A}$. En effet, ce théorème stipule qu'en choisissant une base de $\mathbb{A}$, disons $(e_1, e_2, \ldots, e_n)$, nous pouvons associer à un endomorphisme $u \in \mathcal{L}(\mathbb{A}, \mathbb{A})$ une matrice $M_u \in M_n(\mathbb{Z})$ de la manière suivante : $u \longmapsto M_u := (u(e_1), u(e_2), \ldots, u(e_n))$.

Ainsi, pour tout endomorphisme u_α tel que $u_\alpha(x) = \alpha x$ avec α et x appartenant à l'anneau quadratique R, nous avons une matrice associée M_{u_α} et pouvons donc définir la trace de $\alpha \in R$ comme

$$Tr(\alpha) = Tr(u_\alpha) = Tr(M_{u_\alpha}).$$

Nous attacherons donc à ces anneaux quadratiques définis plus haut la fonction trace $Tr : R \longrightarrow \mathbb{Z}$ qui assigne à un élément $\alpha \in R$ la trace de l'endomorphisme $u_\alpha : R \longrightarrow R$.

3.2.2 Classes d'anneaux quadratiques

Grâce à cette fonction trace sur un anneau quadratique R, il nous est possible d'évaluer le discriminant de R en calculant $\text{Dét}(Tr(\alpha_i, \alpha_j)) =: Disc(R)$ où $\{\alpha_i\}$ est une $\mathbb{Z}$-base de l'anneau R.

Le mathématicien Stickelberger a démontré que pour un anneau R de rang fini comme $\mathbb{Z}$-module, $Disc(R) \equiv 0$ ou 1 $(mod\ 4)$. Ainsi, dans le cas qui nous intéresse particulièrement, c'est-à-dire un anneau quadratique fini de rang 2 possédant une $\mathbb{Z}$-base de la forme $\{1, \delta\}$ où δ est racine d'un polynôme quadratique à coefficients dans $\mathbb{Z}$, nous avons

$$Disc(R) = \text{Dét}(Tr(1, \delta)).$$

D'une manière tout à fait équivalente, nous pouvons calculer le discriminant de R par la formule suivante

$$Disc(R) = \text{Dét} \begin{pmatrix} 1 & \delta \\ 1 & \delta' \end{pmatrix}^2$$

où δ' est le conjugué de δ (voir [6]).

Si nous prenons par exemple x^2+ax+b comme polynôme minimal de δ avec $a, b \in \mathbb{Z}$, nous obtiendrons par de simples calculs la valeur du discriminant de R soit $a^2 - 4b \equiv 0$ ou 1 $(mod\ 4)$. Réciproquement, si nous prenons un entier $D \equiv 0$ ou 1 $(mod\ 4)$, il existe un unique anneau quadratique ayant comme discriminant D. C'est ce qu'affirme le théorème suivant.

Théorème 3. ([1]) *Étant donné un nombre $D \in \mathbb{Z}$ tel que $D \equiv 0$ ou 1 $(mod\ 4)$, il existe (à isomorphisme près) un unique anneau quadratique noté $S(D)$ ayant pour discriminant D. Cet anneau quadratique est donné par*

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

Explicitement, l'anneau quadratique $S(D)$ ainsi défini a comme base $\{1, \delta\}$ où la multiplication de δ par lui-même est donnée par

$$\delta^2 = \begin{cases} \dfrac{D}{4} & \text{si } D \equiv 0 \ (mod\ 4), \\ \dfrac{D-1}{4} + \delta & \text{si } D \equiv 1 \ (mod\ 4). \end{cases}$$

Tout comme pour la notion plus familière de corps quadratique, il existe deux automorphismes de $S(D)$ définis par un élément $x \in S(D)$ et son conjugué $x' \in S(D)$. Par exemple, dans le corps quadratique $\mathbb{Q}(\sqrt{2})$ les deux automorphismes de $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ sont définis par $\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$ et par $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$ où $a, b, \in \mathbb{Z}$. L'idée dans ce qui suivra sera d'éliminer un de ces deux automorphismes pour pouvoir associer à un entier D un anneau quadratique n'ayant qu'un seul automorphisme. L'élimination de cet automorphisme superflu permettra la création d'une bijection qui soit la plus naturelle possible.

Définissons la fonction $\pi : S(D) \to \mathbb{Z}$ par

$$\pi(x) = Tr\left(\frac{x}{\sqrt{D}}\right) = \frac{x - x'}{\sqrt{D}},$$

où x, $x' \in S(D)$ avec x' conjugué de x. En fixant une valeur de $\sqrt{D}$, nous obtenons par la fonction π une valeur dans $\mathbb{Z}$ qui est soit positive, soit négative. En effet, avec notre exemple de l'anneau des entiers algébriques de $\mathbb{Q}(\sqrt{2})$ on obtient, en appliquant π à un $x = a + b\sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})}$,

$$\pi(x) = \frac{x - x'}{\sqrt{D}} = \frac{(a + b\sqrt{2}) - (a - b\sqrt{2})}{\sqrt{2}} = 2b.$$

De même, $\pi(x) = -2b$, si nous avions arrêté notre choix sur $\sqrt{D} = -\sqrt{2}$. Cette latitude sur les valeurs $\sqrt{D}$ nous permet de définir une orientation sur un anneau quadratique.

Définition. Un *anneau quadratique orienté* est un anneau quadratique dont un choix de $\sqrt{D}$ a été fixé. C'est-à-dire où l'un des deux automorphismes de $S(D)$ a été

éliminé.

Cette définition d'anneau quadratique orienté nous amène au théorème fondamental de cette section associant à un entier D, dans notre cas un discriminant, son unique anneau quadratique orienté. Ainsi, en fixant $\sqrt{D}$ nous obtenons un isomorphisme qui sera canonique dans le sens où celui-ci ne dépend plus du choix de $\sqrt{D}$.

Théorème 4. ([1]) *Il existe une correspondance biunivoque entre les entiers congrus à* 0 *ou* 1 *modulo* 4 *et l'ensemble des classes d'anneaux quadratiques orientés isomorphes donnée par*

$$D \leftrightarrow S(D),$$

où $D = Disc(S(D))$.

Une fois la notion d'anneau quadratique orienté bien définie, nous sommes en mesure de parler de *base orientée* d'un tel anneau.

Définition. Soit $S(D)$ un anneau orienté. Une base $\{1, \delta\}$ est dite *orientée positive* si $\pi(\delta) > 0$ où $\pi : S(D) \to \mathbb{Z}$ est la fonction définie plus haut. Une base qui n'est pas orientée positive sera dite orientée *négative*.

Définition. Un anneau orienté R est dit *non-dégénéré* si $Disc(R) \neq 0$.

3.2.3 Classes d'anneaux cubiques

Tout comme nous l'avons fait pour les anneaux quadratiques, il est possible de regrouper sous forme de classes d'équivalence les anneaux cubiques. C'est-à-dire, les anneaux libres de rang 3 comme $\mathbb{Z}$-module. Soulignons que l'ordre maximal d'un corps de nombres de degré 3 sur $\mathbb{Q}$, soit l'anneau des entiers algébriques d'un corps cubique, fait partie de la famille des anneaux cubiques. La définition d'anneaux cubiques est simplement une généralisation moins stricte de la notion d'anneaux d'entiers dans le sens où elle englobe plus de candidats en exigeant simplement le fait d'être libre et de rang 3 comme $\mathbb{Z}$-module. Voyons maintenant comment il nous est possible de les

paramétriser.

Soit R un anneau cubique et soit $\{1, \omega, \theta\}$ une $\mathbb{Z}$-base pour R. Il nous est toujours possible, en translatant ω et θ par des éléments de $\mathbb{Z}$ d'obtenir $\omega \cdot \theta \in \mathbb{Z}$. Une telle base est appelée base normalisée ou base normale de R. Lorsqu'on multiplie les éléments d'une base normale $\{1, \omega, \theta\}$ de R, on peut réécrire certains termes de cette multiplication par une combinaison linéaire d'éléments de cette même base. En d'autres mots, il existe $a, b, c, d, l, m, n \in \mathbb{Z}$ tels que

$$\begin{cases} \omega\theta = n, \\ \omega^2 = m + b\omega - a\theta, \\ \theta^2 = l + d\omega - c\theta. \end{cases} \tag{3.1}$$

Avec cette table de multiplication, nous pouvons associer à un anneau cubique de base normale $\{1, \omega, \theta\}$ une forme binaire cubique à l'aide des mêmes coefficients $a, b, c, d \in \mathbb{Z}$ introduits ci-haut, soit la forme $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Réciproquement, à la forme cubique binaire $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, il est possible d'attacher un anneau cubique où la loi de multiplication est définie par (3.1). Il s'agit de déterminer les coefficients n, m et l en fonction de a, b, c, d donnés par la forme cubique. Ainsi, nous obtenons

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

Résoudre ce système comme nous venons de le faire implique des valeurs uniques pour n, m et l, soit $(n, m, l) = (-ad, -ac, -bd)$. Ainsi, une forme cubique donnée $f(x, y)$ impose une loi de multiplication sur des éléments qui formeront la base d'un anneau cubique $R(f)$ associé à $f(x, y)$.

Il nous est possible, par de simples calculs, de montrer que $disc(R(f)) = disc(f(x, y))$ et, par le fait même, établir une bijection entre les formes cubiques binaires et les anneaux cubiques.

Explicitement, en faisant agir une matrice de $GL_2(\mathbb{Z})$ sur une $\mathbb{Z}$-base $\{\omega, \theta\}$, nous obtenons une autre base de R, une fois celle-ci renormalisée. Puisque la base de départ $\{\omega, \theta\}$ est associée à une forme cubique $f(x, y)$, la transformation décrite plus haut agit non seulement sur cette base mais également sur sa forme implicitement associée. Nous avons donc l'isomorphisme suivant

Théorème 5. ([2]) *Il existe une bijection canonique entre les formes cubiques binaires $GL_2(\mathbb{Z})$-équivalentes et l'ensemble des classes d'anneaux cubiques (classes via isomorphismes d'anneaux), donnée par*

$$f \leftrightarrow R(f)$$

où $Disc(f) = Disc(R(f))$.

Démonstration. Voir [5].

C.Q.F.D.

Les sections 3.2.2 et 3.2.3 exhibent le lien étroit reliant formes binaires quadratiques (respectivement cubiques) et anneaux quadratiques (respectivement cubiques). Ainsi, l'étude de tels anneaux via les formes binaires est une approche qui pourrait s'avérer très enrichissante puisque, tout comme les formes quadratiques se classifient sous une relation d'équivalence, les anneaux quadratiques se regroupent également en classes d'équivalence via des isomorphismes d'anneaux. Il serait maintenant astucieux de construire un isomorphisme non seulement entre classes de formes binaires et classes d'anneaux, mais de réunir également, par l'entremise d'une autre correspondance, les classes d'idéaux.

3.2.4 Formes quadratiques binaires et idéaux

L'idée de cette section est de construire une bijection entre les idéaux orientés et les classes de formes quadratiques. Rappelons que $Cl((Sym^2\mathbb{Z}^2); D)$ est le groupe de classes des formes quadratiques binaires, primitives et $SL_2(\mathbb{Z})$-équivalentes. Ce groupe est quasi isomorphe au groupe de classes des anneaux quadratiques de discriminant D. Voyons en quoi ils diffèrent.

Définition. ([8]) Le *groupe de classes au sens étroit* (*narrow class group*) d'un anneau quadratique $S(D)$, noté $Cl^+(S(D))$, est défini comme étant le groupe des idéaux fractionnaires $\mathbb{F}$ quotienté par le groupe des idéaux fractionnaires principaux et positifs $\mathbb{P}_r^+$, c'est-à-dire les idéaux fractionnaires principaux générés par un élément dont tous les conjugués réels sont positifs. Ainsi,

$$Cl^+(S(D)) := \mathbb{F}/\mathbb{P}_r^+.$$

Il nous est possible, tout comme nous l'avons fait pour un anneau quadratique, de définir sur ses idéaux fractionnaires une orientation.

Définition. Un *idéal orienté* est un couple (I, ε) où I est un idéal de l'anneau quadratique $S(D)$ et $\varepsilon = \pm 1$, donnant l'orientation de I.

Autrement dit, en définissant une $\mathbb{Z}$-base de I et en spécifiant l'orientation de cette même base par ε, nous retrouvons la définition ci-haut.

La multiplication d'idéaux orientés se fait composante par composante. Autrement dit, soit deux idéaux orientés (I_1, ε_1) et (I_2, ε_2) ; alors $(I_1, \varepsilon_1)(I_2, \varepsilon_2) = (I_1 I_2, \varepsilon_1 \varepsilon_2)$. La norme tant qu'à elle fait intervenir la notion de treillis (*lattice*). Un treillis de $\mathbb{R}^n$ par exemple est un groupe abélien libre de rang n, contenu dans $\mathbb{R}^n$, ayant une base qui est également une $\mathbb{R}$-base de $\mathbb{R}^n$. Ainsi, soit T un treillis dans le corps $\mathbb{K}$ des quotients de $S(D)$ contenant évidemment l'anneau quadratique $S(D)$ mais également l'idéal orienté (I, ε). On définit la fonction norme d'un idéal de la façon suivante :

$$N((I, \varepsilon)) = \varepsilon \frac{|T/I|}{|T/S(D)|}.$$

Définition. Deux idéaux orientés (I_1, ε_1) et (I_2, ε_2) de $S(D)$ sont dit *équivalents* s'il existe un $k \in \mathbb{K}$ tel que

$$(I_1, \varepsilon_1) = k \cdot (I_2, \varepsilon_2),$$

où $\mathbb{K}$ est le corps des quotients de $S(D)$.

Si (I_1, ε_1) et (I_2, ε_2) sont équivalents, nous dirons alors qu'ils appartiennent à la même classe d'idéaux orientés.

Toutes ces notions nous permettent de reformuler la définition du groupe de classes d'équivalence au sens étroit. En effet, $Cl^+(S(D))$ se redéfinit comme étant le groupe des idéaux orientés inversibles de $S(D)$ modulo le sous-groupe des idéaux orientés inversibles principaux de $S(D)$. Un élément de $Cl^+(S(D))$ est une classe représentée par un idéal orienté fractionnaire. Traditionnellement, le groupe de classes au sens étroit pour les idéaux n'était considéré que pour les ordres quadratiques $\mathcal{O}$ de discriminant positif. Il consistait en le groupe des idéaux fractionnaires de $\mathcal{O}$ modulo le sous-groupe des idéaux fractionnaires principaux engendrés par un élément ayant une norme positive. Les notions ci-dessus introduites par Manjul Bhargava nous permettent non seulement de traiter le cas où le discriminant de $\mathcal{O}$ est positif, mais également lorsque celui-ci est négatif.

Nous sommes maintenant en mesure de décrire la bijection entre formes quadratiques et idéaux orientés annoncée au début de cette section. Nous verrons d'une part une relation plus générale pour ensuite spécifier le cas des formes quadratiques primitives qui fera intervenir le groupe de classes au sens étroit d'idéaux. Rappelons tout d'abord que nous désignons par $(Sym^2\mathbb{Z}^2)$ l'espace des formes quadratiques binaires (primitives ou non) et que les idéaux des prochains théorèmes seront ceux d'un anneau quadratique $S(D)$ de discriminant D. Nous dirons de plus qu'un tel anneau est *non dégénéré* ou qu'un élément de $(Sym^2\mathbb{Z}^2)$, c'est-à-dire une forme quadratique, est *non dégénéré* si leur discriminant respectif est non nul.

Théorème 6. ([1]) *Il existe une bijection canonique entre l'ensemble des $SL_2(\mathbb{Z})$-orbites non dégénérées de l'espace $(Sym^2\mathbb{Z}^2)$ et l'ensemble des classes (via isomorphismes) de paires $(S(D), I)$, où $S(D)$ est un anneau quadratique orienté non dégénéré et I une classe d'idéaux orientés de $S(D)$. De plus, sous cette bijection, nous avons $Disc(S(D)) = Disc(f_{S(D)})$ où $f_{S(D)}$ est la forme quadratique représentant une classe (une orbite) en bijection avec l'anneau $S(D)$.*

Il est important de souligner que dans cette bijection la paire $(S(D), I)$ est constituée non d'un anneau et d'un idéal mais bien du représentant d'une classe d'anneaux quadratiques et d'un représentant d'une classe d'idéaux orientés de $S(D)$. C'est en faisant agir le groupe $SL_2(\mathbb{Z})$ sur l'espace des formes quadratiques $(Sym^2\mathbb{Z}^2)$ que nous obtenons des classes de formes quadratiques (section 1.1). Donc, il est équivalent dans le théorème précédent de parler de classes de formes ou de $SL_2(\mathbb{Z})$-orbites, ces mêmes orbites étant les classes en question. C'est grâce à la bijection du Théorème 6 qu'il nous est possible de tisser le lien entre classes de formes et classes d'idéaux orientés, pour

ainsi boucler la boucle qui unit formes quadratiques, anneaux quadratiques et finalement idéaux orientés.

Précisons également que dans l'énoncé du Théorème 6, nous prenons en considération l'espace $(Sym^2\mathbb{Z}^2)$ tout entier. Si d'un autre côté nous avions restreint notre espace aux formes quadratiques primitives, alors nous aurions eu le théorème suivant reliant ces classes de formes primitives au groupe de classes au sens étroit.

Théorème 7. ([1]) *La bijection du Théorème* 6 *se restreint à une autre correspondance biunivoque si l'espace* $(Sym^2\mathbb{Z}^2)$ *est réduit à l'ensemble des formes quadratiques primitives. Cette restriction est l'isomorphime de groupes suivant :*

$$Cl((Sym^2\mathbb{Z}^2)^*; D) \simeq Cl^+(S(D)).$$

3.3 Cubes et idéaux

Nous savons qu'il existe un lien qui unit les formes quadratiques et l'espace des cubes $2 \times 2 \times 2$ (section 2.1.1). Vu l'existence de cette correspondance et de la bijection entre formes quadratiques et idéaux orientés, nous est-il possible d'élargir notre canevas en y incluant l'espace des cubes ? Effectivement nous verrons, de manière tout à fait analogue à la section précédente, qu'il existe une bijection entre les classes de cubes et les classes de paires $(S(D), (I_1, I_2, I_3))$ composées d'un représentant d'une classe d'anneaux quadratiques et d'un triplet d'idéaux orientés spécialement choisis de $S(D)$. Mais tout d'abord, quelques définitions.

Définition. Soit $S(D)$ un anneau quadratique et $\mathbb{K}$ son corps de quotients. Un triplet d'idéaux orientés de $S(D)$, (I_1, I_2, I_3) est dit *balancé* si le produit $I_1I_2I_3$ est inclus dans $S(D)$ et si le produit des normes $N(I_1)N(I_2)N(I_3)$ est égal à 1.

Définition. Deux triplets d'idéaux orientés de $S(D)$, disons (I_1, I_2, I_3) et (I'_1, I'_2, I'_3), sont dit *équivalents* si

$$\begin{cases} I_1 = k_1 I_1', \\ I_2 = k_2 I_2', \\ I_3 = k_3 I_3', \end{cases}$$

où $k_1, k_2, k_3 \in \mathbb{K}$.

On peut rappeler ici que l'espace des cubes $2 \times 2 \times 2$ est noté $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ et qu'une orbite sous l'action de $\Gamma \in SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ définie à la section 2.1.2 est simplement une classe d'équivalence d'un cube. Ce groupe de classes d'équivalence muni d'une loi multiplicative était quant à lui noté C_2. Notons également qu'un cube $A \in C_2$ est dit non dégénéré si $Disc(A) \neq 0$. Avec ces définitions, nous avons le Théorème 8 qui est analogue au Théorème 6.

Théorème 8. ([1]) *Il existe une bijection canonique entre l'ensemble des* Γ*-orbites de l'espace des cubes non dégénérés et l'ensemble des classes (via isomorphismes) de paires* $(S(D), (I_1, I_2, I_3))$*, où* $S(D)$ *est le représentant d'un anneau quadratique orienté non dégénéré et* (I_1, I_2, I_3) *une classe de triplets d'idéaux balancés et orientés de* $S(D)$*.*

Démonstration. Voyons de plus près en quoi consiste cette bijection. Donnons-nous 3 idéaux orientés et balancés d'un anneau quadratique $S(D)$, soit I_1, I_2 et I_3, munis de leurs $\mathbb{Z}$-bases respectives $\langle \alpha_1, \alpha_2 \rangle$, $\langle \beta_1, \beta_2 \rangle$ et $\langle \gamma_1, \gamma_2 \rangle$. Supposons également qu'une base de $S(D)$ soit donnée par $\{1, \delta\}$. Ainsi, puisque le produit $I_1 I_2 I_3$ est par définition inclus dans $S(D)$, nous obtenons le système composé des 16 équations suivantes :

$$\alpha_i \beta_j \gamma_k = c_{ijk} \cdot 1 + a_{ijk} \cdot \delta,$$

où les a_{ijk} et $c_{ijk} \in \mathbb{Z}$ et où $1 \leq i, j, k \leq 2$.

Autrement dit, le membre de gauche de cette équation s'exprime à l'aide de la base de l'anneau quadratique $S(D)$. Pour établir la bijection, il suffit de suivre les 4 étapes de l'algorithme suivant.

Soit $S(D)$ un anneau quadratique et soit (I_1, I_2, I_3) un triplet de classes d'idéaux orientés et balancés de ce même anneau.

(1) Alors nous avons

$$S(D) \to A = (a_{ijk}),$$

où les a_{ijk} définis plus haut représentent les 8 sommets du cube A.

(2) Inversement, soit un cube $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Alors, nous avons

$$A \to S(D),$$

où $S(D)$ est défini par le discriminant de A, c'est-à-dire $S(D) = S(Disc(A))$.

(3) Les bases respectives des classes d'idéaux I_1, I_2 et I_3 sont données par

$$\alpha_i\beta_j\gamma_k = c_{ijk} \cdot 1 + a_{ijk} \cdot \delta,$$

(4) La structure des $S(D)$-modules $I_1 = \langle \alpha_1, \alpha_2 \rangle$, $I_2 = \langle \beta_1, \beta_2 \rangle$ et $I_3 = \langle \gamma_1, \gamma_2 \rangle$ se calcule à partir des 3 formes quadratiques associées au cube A, disons Q_1^A, Q_2^A et Q_3^A. Explicitement, nous avons

$$\begin{cases} Q_1^A(x,y) = p_1x^2 + q_1xy + r_1y^2, \\ Q_2^A(x,y) = p_2x^2 + q_2xy + r_2y^2, \\ Q_3^A(x,y) = p_3x^2 + q_3xy + r_3y^2. \end{cases}$$

où chaque Q_i^A $(1 \leq i \leq 3)$ est associé à un des systèmes suivants :

$$i = 1 : \quad \begin{cases} \delta\alpha_1 \ = \dfrac{q_1 + \varepsilon}{2} + p_1\alpha_2, \\ -\delta\alpha_2 = r_1\alpha_1 + \dfrac{q_1 - \varepsilon}{2}\alpha_2, \end{cases}$$

$$i = 2 : \quad \begin{cases} \delta\beta_1 \ = \dfrac{q_2 + \varepsilon}{2} + p_2\beta_2, \\ -\delta\beta_2 = r_2\beta_1 + \dfrac{q_2 - \varepsilon}{2}\beta_2, \end{cases}$$

$$i = 3 : \quad \begin{cases} \delta\gamma_1 \ = \dfrac{q_3 + \varepsilon}{2} + p_3\gamma_2, \\ -\delta\gamma_2 = r_3\gamma_1 + \dfrac{q_3 - \varepsilon}{2}\gamma_2, \end{cases}$$

où $\varepsilon = 0$ ou 1 dépendamment si $D \equiv 0$ ou 1 $(mod\ 4)$.

C.Q.F.D.

Tout comme nous l'avons fait au Théorème 7, il existe une version restreinte de la bijection entre les cubes et les idéaux intimement liée au groupe de classes au sens étroit. Pour ce faire, nous avions conservé uniquement les formes quadratiques primitives. Il serait naturel de restreindre notre espace de cubes à ceux possédant la caractéristique d'être projectif (dont les formes quadratiques associées sont primitives).

Théorème 9. ([1]) *La bijection du Théorème* 8 *se restreint à une autre correspondance biunivoque si l'espace des cubes* $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ *est réduit à l'ensemble des cubes projectifs. Cette restriction est l'isomorphime de groupes suivant :*

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

Chapitre 4

Paramétrisation via les anneaux résolvants

Nous avons vu, dans le chapitre 3 notamment, que certains anneaux quadratiques ou cubiques, reliés de près aux ordres d'un corps de nombres, s'étudient plus facilement sous une paramétrisation judicieuse des formes quadratiques binaires et ternaires. Ces paramétrisations sont d'autant plus efficaces puisque dans le cas d'un ordre maximal, celles-ci correspondent à la paramétrisation de l'anneau des entiers d'un corps de nombres. Dans le cas des anneaux quadratiques, nous avons établi la correspondance avec un ensemble d'entiers jouant le rôle de discriminants (des entiers congrus à 0 ou 1 modulo 4) via une bijection fortement influencée par le Théorème de Stickelberger ([6]). Nous avons d'un autre côté attaché aux anneaux cubiques une forme cubique binaire pour ainsi créer une bijection entre les classes de formes cubiques et les classes d'anneaux cubiques (via isomorphismes).

Dans le présent chapitre, nous verrons qu'il existe une autre méthode de paramétrisation commune aux deux types d'anneaux. Celle-ci prendra naissance à travers la théorie de Galois et se peaufinera par le biais de ce que nous définirons comme les anneaux résolvants. Non seulement ce genre de paramétrisation inclut les deux types d'anneaux précédemment vus, mais également les anneaux quartiques, c'est-à-dire des anneaux libres de rang 4 sur $\mathbb{Z}$. Débutons par un bref rappel de quelques définitions et concepts de la théorie de Galois qui nous seront nécessaires dans ce qui suivra.

4.1 Théorie de Galois

Définition. On appelle *extension normale* d'un corps $\mathbb{K}$ une extension algébrique N de $\mathbb{K}$ telle que tout polynôme irréductible de $\mathbb{K}[X]$ ayant une racine dans N ait toutes ses racines dans N. Au lieu de *extension normale* on dit parfois *corps de décomposition.*

Définition. Une extension algébrique L d'un corps $\mathbb{K}$ est dite *séparable* si et seulement si le polynôme minimal de tout élément de L n'admet que des racines simples.

Définition. Soit F une extension finie de $\mathbb{K}$. Alors, F est une *extension galoisienne* sur $\mathbb{K}$ si $|Aut(F/K)| = [F : K]$. En fait, une *extension galoisienne* est une extension normale séparable.

Définition. Soit $\mathbb{F}$ une extension d'un corps $\mathbb{K}$. Une extension galoisienne et minimale de $\mathbb{F}$ contenant le corps $\mathbb{K}$ est appellée la *fermeture galoisienne* de $\mathbb{K}$ sur $\mathbb{F}$. Nous noterons cette fermeture par $\overline{\mathbb{K}}$.

À la lumière de ces définitions (voir [9] pour plus amples détails), nous sommes maintenant en mesure d'introduire la notion de fermeture galoisienne d'un anneau, concept analogue à celui de fermeture galoisienne d'un corps. Il existe deux approches pour aborder ce concept, une plus constructive et l'autre plus intuitive. La deuxième approche sera amplement suffisante pour ce qui suivra.

Plaçons-nous, tout d'abord, dans un contexte qui nous permettra de mieux visualiser la transposition de la notion de fermeture galoisienne d'un corps sur celle d'un anneau. Soit $\mathbb{K}$ notre corps de référence, extension du corps $\mathbb{F}$ et dont la fermeture galoisienne usuelle sera notée $\overline{\mathbb{K}}$. Ainsi, nous avons $\mathbb{F} \subseteq \mathbb{K} \subseteq \overline{\mathbb{K}}$.

Prenons maintenant un ordre R inclus dans le corps $\mathbb{K}$. Alors la fermeture galoisienne de cet anneau peut être vue comme une extension séparable et normale de R, notée $\overline{R}$ qui est naturellement contenue dans la fermeture galoisienne usuelle $\overline{\mathbb{K}}$. On note également que tout comme l'anneau R, $\overline{R}$ est également un ordre, mais cette fois, un ordre de $\overline{\mathbb{K}}$.

Les initiés à la théorie de Galois se rappelleront que le groupe de Galois, noté $Gal(\mathbb{K}/\mathbb{F})$, c'est-à-dire le groupe des automorphismes de $\mathbb{K}$ laissant invariant le corps $\mathbb{F}$, peut être vu comme un groupe de permutations. En effet, supposons pour simplifier les choses, que $\mathbb{K}$ contienne toutes les racines d'un polynôme séparable $f(x) \in \mathbb{F}[X]$. Alors le groupe de Galois de ce polynôme est défini comme étant $Gal(\mathbb{K}/\mathbb{F})$. Autrement dit, c'est le groupe des $\mathbb{F}$-homomorphismes de $\mathbb{K}$ où $\mathbb{K}$ est le corps de décomposition de $f(x)$. Or, nous avons la proposition suivante.

Proposition. *Soit $f(x) \in \mathbb{F}[x]$ un polynôme de degré n. Le corps de décomposition de $f(x)$ est une extension de degré fini de $\mathbb{F}$. De plus, si l'on note par $\mathbb{K}$ ce corps de décomposition, nous avons*

$$[\mathbb{K} : \mathbb{F}] \mid n! \ .$$

Nous savons également qu'un élément $\sigma \in Gal(\mathbb{K}/\mathbb{F})$ associe à une racine de $f(x)$ une autre racine de ce dernier polynôme. Explicitement, étiquetons $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ les n racines du polynôme $f(x)$. Ainsi, pour $\sigma \in Gal(\mathbb{K}/\mathbb{F})$, nous obtenons $\sigma(\alpha_i) = \alpha_j$. Donc, pour un automorphisme donné du groupe de Galois du polynôme $f(x)$, celui-ci agit sur les racines comme une permutation du groupe S_n. Nous avons donc une injection, qui est en fait un homomorphisme de groupes, entre $Gal(\mathbb{K}/\mathbb{F})$ et S_n.

C'est cette correspondance entre le groupe de Galois et S_n qui suggère à Manjul Bhargava la notation de S_k-fermeture (S_k-*closure*) pour un anneau R libre de rang k sur $\mathbb{Z}$, notation beaucoup moins lourde que $Gal(\mathbb{K}/\mathbb{F})$-fermeture. Ainsi, suite à ce que nous avons défini plus haut et de manière intuitive, la fermeture galoisienne de l'anneau R, c'est-à-dire l'anneau $\overline{R} \subseteq \overline{\mathbb{K}}$, est équivalente au concept de S_k-fermeture de R.

En résumé, nous avons donc un anneau $R \subseteq \mathbb{K}$ allant de pair avec une S_k-fermeture $\overline{R} \subseteq \overline{\mathbb{K}}$ où, pour être clair,

- $\mathbb{K}$ est un corps de nombres (extension de $\mathbb{Q}$),
- $\overline{\mathbb{K}}$ est la fermeture galoisienne de $\mathbb{K}$,
- R un anneau libre de rang k contenu dans $\mathbb{K}$ (extension de $\mathbb{Z}$),
- $\overline{R}$ la S_k-fermeture de l'anneau R contenu dans $\overline{\mathbb{K}}$,
- $Gal(\overline{\mathbb{K}}/\mathbb{Q})$ le groupe de Galois de $\overline{\mathbb{K}}$ laissant fixe le corps des rationnels $\mathbb{Q}$.

On notera que dans ce qui précède, l'introduction du corps $\mathbb{F}$ n'avait pour but qu'une meilleure description des notions introduites. Puisque notre étude est axée sur les ordres d'un corps de nombres $\mathbb{K}$, nous pouvons fixer $\mathbb{F}$ comme étant ni plus ni moins que le corps des rationnels $\mathbb{Q}$, pour ainsi restreindre la généralité du texte au cas plus spécifique qui nous intéresse.

Définition. Soit $\alpha \in R$. Les éléments $\sigma(\alpha) \in \overline{R} \subseteq \overline{\mathbb{K}}$ avec $\sigma \in Gal(\overline{\mathbb{K}}/\mathbb{Q})$ sont appelés les *conjugués galoisiens* de α.

Grâce à cette définition nous avons le théorème suivant.

Théorème 10. ([3]) *L'anneau $\overline{R}$ est isomorphe à l'anneau engendré par tous les conjugués galoisiens des éléments de R dans $\overline{\mathbb{K}}$. C'est-à-dire,*

$$\overline{R} \cong \mathbb{Z}[\alpha : \alpha \text{ est un conjugué galoisien d'un élément de } R].$$

4.2 Anneaux résolvants

4.2.1 Résolvante quadratique d'un anneau cubique

Le théorème principal de ce chapitre unit les formes quadratiques ternaires et les couples composés d'un anneau cubique et de sa résolvante quadratique. Cette correspondance se fera par l'entremise d'une fonction quadratique permettant de passer d'un $\mathbb{Z}$-module de rang 3 à un $\mathbb{Z}$-module de rang 2. Nous avons vu, lors d'une paramétrisation précédente via l'ensemble des entiers congrus à 0 ou 1 modulo 4 qu'à un tel entier correspond, à isomorphisme près, un unique anneau quadratique $S(D)$. Il sera donc possible d'associer à un anneau cubique de discriminant D un unique anneau quadratique $S(D)$ de même discriminant. Ce que nous définirons comme l'anneau quadratique résolvant ou encore la résolvante quadratique.

Définition. Soit R un anneau cubique. La *résolvante quadratique* de R est l'unique anneau quadratique dont le discriminant est égal à celui de R. Cette résolvante sera

notée $S^{res}(D)$.

Il existe une fonction permettant de passer de l'anneau cubique R à son anneau quadratique résolvant. Effectivement, en utilisant le contexte décrit dans le préambule de cette section, on peut définir une fonction $\varphi_{3,2}$ reliant les deux types d'anneaux grâce aux conjugués galoisiens des éléments de R. Nous aurons besoin de la définition suivante.

Définition. Le *discriminant* d'un élément x appartenant à un corps de nombres $\mathbb{K}$ de degré n est donné par

$$Disc(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

où $x_1, \ldots, x_n$ sont les conjugués de x par rapport au corps $\mathbb{K}$.

Soit $x \in R$ et notons par x, x' et x'' ses 3 conjugués galoisiens contenus dans la S_3-fermeture de R, c'est-à-dire $\overline{R}$. Alors, nous avons

$$\varphi_{3,2}(x) = \frac{[(x-x')(x'-x'')(x''-x)]^2 + (x-x')(x'-x'')(x''-x)}{2}$$

qui est contenu dans un anneau quadratique et possède la propriété que $Disc(x) = Disc(\varphi_{3,2}(x))$. Nous pouvons construire grâce à ces éléments de $\overline{R}$ un nouvel anneau quadratique appelé l'anneau quadratique invariant de R, noté $S^{inv}(R)$, et dont la terminologie est due au fait que $\varphi_{3,2}$ préserve le discriminant. Concrètement, nous avons la définition suivante :

$$S^{inv}(R) = \mathbb{Z}[\varphi_{3,2}(x); x \in R].$$

On remarque, grâce à certaines propriétés de la fonction $\varphi_{3,2}$, que $S^{inv}(R) \subseteq S^{res}(D)$. De plus, $\varphi_{3,2}$ possède la caractéristique intéressante d'être invariant sous la translation d'un élément de $\mathbb{Z}$, c'est-à-dire $\varphi_{3,2}(x) = \varphi_{3,2}(x+c)$, pour tout $c \in \mathbb{Z}$. Cette particularité permet de quotienter l'anneau cubique de départ R et l'anneau quadratique résolvant d'arrivée $S^{res}(D)$ par $\mathbb{Z}$ de manière à restreindre $\varphi_{3,2}$ à une nouvelle fonction $\widetilde{\varphi}_{3,2} : R/\mathbb{Z} \to S^{res}(D)/\mathbb{Z}$. Ainsi, $\widetilde{\varphi}_{3,2}$ devient une fonction quadratique de $\mathbb{Z}^2 \to \mathbb{Z}$ nous permettant de lui attacher une forme cubique binaire.

Explicitement, soit R l'anneau cubique dont une $\mathbb{Z}$-base est donnée par $\{1, \omega_1, \omega_2\}$

et dont la structure sous-jacente est donnée par

$$\begin{cases} \omega_1\omega_2 = -ad, \\ \omega_1^2 = -ac + b\omega_1 - a\omega_2, \\ \omega_2^2 = -bd + d\omega_1 - c\omega_2. \end{cases}$$

avec $a, b, c, d \in \mathbb{Z}$ et prenons $x\omega_1 + y\omega_2 \in R$. On peut calculer concrètement le discriminant de cet élément pour ainsi lui associer une forme cubique. En voici les détails (voir [8] pour plus de précisions).

Posons $\theta = x\omega_1 + y\omega_2$. Ainsi,

$$Disc(\theta) = Disc(1, \theta, \theta^2).$$

Calculons tout d'abord

$$\theta^2 = (x\omega_1 + y\omega_2)(x\omega_1 + y\omega_2) = x^2\omega_1^2 + 2xy\omega_1\omega_2 + y^2\omega_2^2.$$

En substituant les valeurs de ω_1, ω_2 et de $\omega_1\omega_2$ par leur valeurs respectives données par la table multiplicative de R, on obtient

$$\theta^2 = x^2(-ac + b\omega_1 - a\omega_2) + 2xy(-ad) + y^2(-bd + d\omega_1 - c\omega_2).$$

Il est maintenant possible de construire un nouveau système qui exprimera 1, θ et θ^2 en fonction de 1, ω_1 et ω_2, c'est-à-dire

$$\begin{cases} 1 = 1 \cdot 1 + 0 \cdot \omega_1 + 0 \cdot \omega_2, \\ \theta = 0 \cdot 1 + x \cdot \omega_1 + y \cdot \omega_2, \\ \theta^2 = (-acx^2 - 2adxy - bdy^2) \cdot 1 + (bx^2 - dy^2) \cdot \omega_1 + (-ax^2 - cy^2) \cdot \omega_2. \end{cases}$$

Utilisons la proposition suivante.

Proposition. *$Disc(\theta) = Disc(1, \theta, \theta^2) = |Dét(c_{ij})|^2 Disc(R)$, où les c_{ij} sont les composantes des éléments 1, θ et θ^2 exprimés selon la base $\{1, \omega_1, \omega_2\}$.*

On obtient donc

$$\begin{aligned} Disc(\theta) &= \text{Dét}\left|\begin{pmatrix} 1 & 0 & 0 \\ 1 & x & y \\ -acx^2 - 2adxy - bdy^2 & bx^2 - dy^2 & -ax^2 - cy^2 \end{pmatrix}\right|^2 Disc(R) \\ &= 1 \cdot |(x)(-ax^2 - cy^2) - (y)(bx^2 - dy^2)|^2 Disc(R) \\ &= (ax^3 + bx^2y + cxy^2 + dy^3)^2 Disc(R). \end{aligned}$$

Nous avons donc produit une forme cubique binaire attachée à un anneau cubique dont la base et la table de multiplication ont été préalablement établies. Si l'on note D le discriminant de l'anneau R, nous avons la fonction $\widetilde{\varphi}_{3,2}$ qui donne naissance à la forme cubique

$$\frac{\sqrt{Disc(x\omega_1 + y\omega_2)/2}}{\sqrt{D}/2} = (ax^3 + bx^2y + cxy^2 + dy^3).$$

4.2.2 Résolvante cubique d'un anneau quartique

Il est possible, une fois la théorie bien établie pour les résolvantes quadratiques, d'élaborer celle des résolvantes cubiques d'un anneau quartique, c'est-à-dire un anneau libre de rang 4 sur $\mathbb{Z}$. Soit Q un anneau quartique. Nous allons, comme dans la section précédente, construire une fonction ayant pour origine Q et dont l'image aura un rôle important dans ce que l'on définira comme la résolvante cubique de ce même anneau Q.

Tout d'abord, prenons comme fonction polynômiale $\varphi_{4,3} : Q \to R$ qui à un élément $x \in Q$ lui associe naturellement un élément de même discriminant d'un anneau cubique R. Il s'agit encore ici de construire la S_4-fermeture de l'anneau quartique Q que l'on notera $\overline{Q}$ et de prendre dans cette fermeture les 4 conjugués galoisiens de x, soit x lui-même, x', x'' et finalement x'''. Ainsi, nous pouvons définir la fonction $\varphi_{4,3} : Q \to R$ comme étant

$$\varphi_{4,3}(x) = xx' + x''x''',$$

fonction qui jouera un rôle analogue à la fonction $\varphi_{3,2}$, mais à des rangs supérieurs d'anneaux. Cette fonction ne fut pas arbitrairement choisie puisqu'elle possède les propriétés

intéressantes de préserver le discriminant et d'avoir comme image des éléments appartenant à un même anneau cubique. En fait, si l'on se remémore le lien tissé entre groupe de Galois et groupe des permutations (voir [9]), nous pouvons mettre en bijection le groupe de Galois de $\overline{Q}$ et le groupe des permutations S_4. Vu sous cet angle, l'anneau cubique R n'est rien d'autre que le sous-anneau de $\overline{Q}$ laissé fixe par le sous-groupe diédral $D_4 \subseteq S_4$.

Puisque l'on sait désormais que le discriminant est conservé par $\varphi_{4,3}$, nous pouvons définir l'anneau cubique invariant.

Définition. Soit Q un anneau quartique. On notera $R^{inv}(Q)$ *l'anneau cubique invariant* comme étant l'anneau engendré par l'image de $\varphi_{4,3}$, c'est-à-dire

$$R^{inv}(Q) = \mathbb{Z}[\{\varphi_{4,3}(x) \ ; \ x \in Q\}].$$

Il est important de souligner qu'on rencontre ici une brisure entre la définition de résolvante cubique et celle de résolvante quadratique. Celle-ci est principalement dûe au fait que les anneaux cubiques se comportent un peu moins bien en termes d'unicité du discriminant. En effet, contrairement aux anneaux quadratiques pour lesquels à un discriminant fixé correspondait un seul anneau (à isomorphisme près), la situation est plus délicate pour les anneaux cubiques. Rien, *a fortiori*, ne nous permet de privilégier un choix de discriminant plus naturel qu'un autre. Il n'y a pas comme dans le cas quadratique de bijection naturelle entre les entiers congrus à 0 ou 1 modulo 4 et les anneaux cubiques en général. Il nous est cependant possible de contourner cette lacune simplement en acceptant plusieurs candidats potentiels comme résolvantes cubiques d'un même anneau quartique. Ceci soulève ainsi une différence notable entre les résolvantes quadratiques et les résolvantes cubiques : on a l'unicité à isomorphisme canonique près.

Définition. Soit Q un anneau quartique et $R^{inv}(Q)$ son anneau cubique invariant associé. Un *anneau cubique résolvant* de Q est un anneau cubique R tel que

(1) $Disc(Q) = Disc(R)$,
(2) $R^{inv}(Q) \subseteq R$.

Qu'en est-il de l'existence et de l'unicité des anneaux cubiques résolvants ?

Lemme. ([3]) *Soit T un anneau libre unitaire de rang k sur $\mathbb{Z}$. Alors, T possède comme sous-anneau $T_n = \mathbb{Z} + nT$, pour $n \in \mathbb{N}$. Inversement, tout anneau non trivial peut s'écrire comme T_n avec un unique n maximal et un unique anneau T.*

Cette dernière écriture est dite *primitive*.

Proposition. ([3]) *Soit Q un anneau quartique. Alors Q possède au moins un anneau cubique résolvant. De plus, si Q est primitif par rapport à l'écriture du lemme précédent, alors l'anneau cubique résolvant est unique et égal à $R^{inv}(Q)$.*

Puisque pour tout anneau quartique Q il correspond au moins un anneau cubique résolvant, la fonction $\varphi_{4,3} : Q \to R$ est bien définie et nous pouvons faire le même type de travail pour en extraire une paire de formes quadratiques ternaires judicieusement choisies.

Lemme. La fonction $\varphi_{4,3}$ est invariante par rapport à la translation par un entier.

Démonstration. En effet, soit $c \in \mathbb{Z}$. Alors, $\varphi_{4,3}(x) = xx' + x''x'''$ de sorte que

$$\begin{aligned}(x+c)(x'+c) + (x''+c)(x'''+c) &= (xx' + xc + x'c + c^2) + (x''x''' + x''c + x'''c + c^2) \\ &= xx' + x''x''' + c(x + x' + x'' + x''') + 2c^2 \\ &= \varphi_{4,3}(x) + cTr(x) + 2c^2.\end{aligned}$$

Puisque $cTr(x) + 2c^2 = d \in \mathbb{Z}$, nous avons $\varphi_{4,3}(x + c) = \varphi_{4,3}(x) + d$.

C.Q.F.D.

Cela nous permet, après avoir quotienté par $\mathbb{Z}$, de restreindre la fonction $\varphi_{4,3} : Q \to R$ à une nouvelle fonction $\widetilde{\varphi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$, abaissant à la fois le rang de l'anneau d'origine et celui d'arrivée. La fonction $\widetilde{\varphi}_{4,3}$ devient donc une fonction entre $\mathbb{Z}$-modules ou encore une fonction cubique de $\mathbb{Z}^3$ dans $\mathbb{Z}^2$ à laquelle nous pourrons attacher une paire de formes quadratiques ternaires intégrales bien définies sous $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$-équivalence. La prochaine section sera consacrée à cette correspondance.

4.3 Anneaux quartiques et formes quadratiques ternaires

Comme nous l'avons vu précédemment, nous pouvons associer à un anneau quartique Q et une de ses résolvantes cubiques R une fonction $\widetilde{\varphi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$ qui possède la propriété centrale de conserver le discriminant. Contrairement aux anneaux cubiques, les structures inhérentes aux anneaux quartiques sont plus complexes à calculer. En effet, la fonction $\widetilde{\varphi}_{3,2}$ s'explicitait aisément à l'aide de la structure des résolvantes quadratiques qui s'écrivait quant à elle assez bien. Or, la seule information que l'on peut extraire d'une résolvante cubique est le simple fait que ce soit un anneau libre de rang 3 d'un certain discriminant D. Information peu utile si nous voulons décrire la fonction $\widetilde{\varphi}_{4,3}$. Pour éviter ce problème, il suffit non pas de tenter d'associer au couple (Q, R) deux formes quadratiques ternaires, mais plutôt de prendre un couple de formes (f_1, f_2) et par la suite de calculer les structures possibles des deux anneaux Q et R.

Rappelons tout d'abord qu'une forme quadratique ternaire est un polynôme homogène de degré 2 en trois variables, typiquement

$$f(x, y, z,) = ax^2 + by^2 + cz^2 + uxy + vyz + wxz.$$

À cette forme, nous pouvons lui associer une matrice symétrique 3×3 correspondante (voir [14]) donnée par

$$M_f = \begin{pmatrix} a & u/2 & w/2 \\ u/2 & b & v/2 \\ w/2 & v/2 & c \end{pmatrix}$$

De plus, le déterminant d'un forme quadratique ternaire correspond au déterminant de sa matrice associée. Deux formes quadratiques ternaires $f(x, y, z)$ et $g(x, y, z)$ sont dites équivalentes s'il existe une matrice $\gamma \in GL_3(\mathbb{Z})$ telle que $\gamma f(x, y, z) = g(x, y, z)$ ou de manière tout à fait équivalente si $\gamma M_f \gamma^t = M_g$.

4.3.1 Invariant fondamental

Soit $(Sym^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)$ l'ensemble des paires de formes quadratiques ternaires et intégrales. Soit également le groupe $G_{\mathbb{Z}} = GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$. Nous pouvons faire agir le groupe

$G_{\mathbb{Z}}$ sur une paire de formes quadratiques ternaires de la façon suivante :

$$(g_3, g_2)(f_1, f_2) = (r \cdot g_3 f_1 g_3^t + s \cdot g_3 f_2 g_3^t \ , \ t \cdot g_3 f_1 g_3^t + u \cdot g_3 f_2 g_3^t),$$

où $g_2 = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$, $g_3 \in GL_3(\mathbb{Z})$ et f_1, f_2 sont deux formes quadratiques ternaires.

Après une courte étude, de l'action de $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$ sur l'ensemble des couples de formes quadratiques ternaires (voir [3]), on se rend compte que celui-ci possède un unique invariant donné par

$$Disc(4(f_1 x + f_2 y))$$

et appelé le discriminant fondamental du couple (f_1, f_2).

4.3.2 Structure d'anneaux quartiques

Définition. Soit M un $\mathbb{Z}$-module de rang k. Alors l'*indice* du treillis engendré par les k vecteurs $v_1, v_2, \ldots, v_k$ de M est noté $Ind_M(v_1, v_2, \ldots, v_k)$. Il s'agit du déterminant de la transformation amenant $v_1, v_2, \ldots, v_k$ sur une $\mathbb{Z}$-base de M.

Cette définition tisse un premier lien entre l'anneau quartique Q, une de ses résolvantes cubiques R et la fonction $\widetilde{\varphi}_{4,3}$.

Proposition. *Soit Q un anneau quartique, R une résolvante cubique de Q. Alors $\forall\ x, y \in Q$, nous avons*

$$Ind_Q(1, x, y, xy) = \pm Ind_R(1, \widetilde{\varphi}_{4,3}(x), \widetilde{\varphi}_{4,3}(y)).$$

Démonstration. Puisque $Disc(Q) = Disc(R)$, on a l'équivalence suivante qui peut être vérifiée directement par le lecteur.

$$\text{Dét}\begin{pmatrix} 1 & 1 & 1 & 1 \\ x & x' & x'' & x''' \\ y & y' & y'' & y''' \\ xy & x'y' & x''y'' & x'''y''' \end{pmatrix} = \text{Dét}\begin{pmatrix} 1 & 1 & 1 \\ xx'+x''x''' & xx''+x'x''' & xx'''+x'x'' \\ yy'+y''y''' & yy''+y'y''' & yy'''+y'y'' \end{pmatrix}.$$

C.Q.F.D.

Le signe devant $\pm Ind_R(1, \widetilde{\varphi}_{4,3}(x), \widetilde{\varphi}_{4,3}(y))$ de la proposition précédente est simplement dû au fait qu'aucune précision n'a été apportée quant à l'orientation des deux anneaux Q et R. Pour régler ce problème, nous fixerons les bases en plus d'expliciter une fonction $\widetilde{\varphi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$ à laquelle nous pourrons concrètement attacher un couple de formes quadratiques ternaires. Fixons une fois pour toutes l'orientation de Q et R en choisissant leurs bases respectives $\{1, \alpha_1, \alpha_2, \alpha_3\}$ et $\{1, \omega_1, \omega_2\}$. Attachons à ces deux anneaux une fonction qui les reliera aux formes quadratiques ternaires, c'est-à-dire

$$\widetilde{\varphi}_{4,3}(x\overline{\alpha}_1 + y\overline{\alpha}_2 + z\overline{\alpha}_3) = f_1(x,y,z)\overline{\omega}_1 + f_2(x,y,z)\overline{\omega}_2$$

où $\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}_3, \overline{\omega}_1, \overline{\omega}_2$ correspondent à la réduction de $\alpha_1, \alpha_2, \alpha_3, \omega_1, \omega_2$ modulo $\mathbb{Z}$.

Définition. Soit $\{1, \alpha_1, \alpha_2, \alpha_3\}$ une base de l'anneau quartique Q et $\{1, \omega_1, \omega_2\}$ une base de l'anneau cubique R. Une fois translatée par un élément approprié de $\mathbb{Z}$, la base de Q est dite *normale* si

$$\begin{cases} \alpha_1\alpha_2 = a \cdot 1 + 0 \cdot \alpha_1 + 0 \cdot \alpha_2 + d \cdot \alpha_3, \\ \alpha_1\alpha_3 = a' \cdot 1 + 0 \cdot \alpha_1 + c' \cdot \alpha_2 + d' \cdot \alpha_3. \end{cases}$$

La base de R est dite normale si elle satisfait

$$\omega_1\omega_2 = a'' \cdot 1 + 0 \cdot \omega_1 + 0 \cdot \omega_2,$$

avec $a, c, d, a', c', d', a'' \in \mathbb{Z}$.

Ces bases normales de $Q/\mathbb{Z}$ et de $R/\mathbb{Z}$ seront précieuses puisqu'elles se prolongent de façon unique en des bases normales de Q et de R respectivement. Une fois de telles bases choisies, nous pouvons expliciter la structure multiplicative de Q avec le système

$$\alpha_i\alpha_j = c_{ij}^0 \cdot 1 + c_{ij}^1 \cdot \alpha_1 + c_{ij}^2 \cdot \alpha_2 + c_{ij}^3 \cdot \alpha_3, \tag{4.1}$$

où $i, j \in \{1, 2, 3\}$ et $c_{ij} \in \mathbb{Z}$. La définition de base normale est équivalente aux conditions $c_{12}^1 = c_{12}^2 = c_{13}^1 = 0$ de ce nouveau système.

Prenons maintenant deux éléments x et y de notre anneau quartique Q ayant pour base normale $\{1, \alpha_1, \alpha_2, \alpha_3\}$, c'est-à-dire

$$\begin{cases} x = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3, \\ y = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3, \end{cases}$$

où $r_i, s_i \in \mathbb{Z}$ et tentons de représenter le produit de deux éléments de Q à l'aide de la base de ce dernier anneau quartique. Nous retrouverons ainsi la loi multiplicative qui régit la structure de Q puisque x et y furent choisis arbitrairement. Ainsi, utilisant la table de multiplication (4.1) définie sur les éléments de la base normale de Q, on obtient en regroupant les termes

$$\begin{aligned} xy &= (r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3)\ (s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3) \\ &= c + t_1\alpha_1 + t_2\alpha_2 + t_3\alpha_3, \end{aligned}$$

où $c \in \mathbb{Z}$ et t_k, pour $k \in \{1, 2, 3\}$, est défini par

$$t_k = \sum_{1 \leq i,j \leq 3} c_{ij}^k r_i s_j.$$

Nous avons également, selon la définition d'indice, que

$$Ind_Q(1, x, y, xy) = \text{Dét} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & r_1 & r_2 & r_3 \\ 0 & s_1 & s_2 & s_3 \\ 0 & t_1 & t_2 & t_3 \end{pmatrix}$$

et

$$Ind_R(1, \widetilde{\varphi}_{4,3}(x), \widetilde{\varphi}_{4,3}(y)) = \text{Dét} \begin{pmatrix} 1 & 0 & 0 \\ 0 & f_1(r_1, r_2, r_3) & f_2(r_1, r_2, r_3) \\ 0 & f_1(s_1, s_2, s_3) & f_2(s_1, s_2, s_3) \end{pmatrix},$$

où f_1 et f_2 sont deux formes quadratiques ternaires.

Nous obtenons, en calculant explicitement ces deux indice, deux polynômes de degré 4 en $r_1, r_2, r_3, s_1, s_2, s_3$. De plus, d'après la proposition , ces deux polynômes que l'on notera $p(r_1, r_2, r_3, s_1, s_2, s_3)$ et $q(r_1, r_2, r_3, s_1, s_2, s_3)$ sont égaux pour tout $r_1, r_2, r_3, s_1, s_2, s_3$

$\in \mathbb{Z}$. En mettant en relation les coefficients des deux formes ternaires f_1 et f_2 et les c_{ij}^k dans ces deux polynômes, on obtient un système de 15 équations dont la solution est unique. Écrivons maintenant les deux formes ternaires quadratiques comme suit :

$$\begin{cases} f_1(x,y,z) = a_{11}x^2 + a_{12}xy + a_{13}xz + a_{22}y^2 + a_{23}yz + a_{33}z^2, \\ f_2(x,y,z) = b_{11}x^2 + b_{12}xy + b_{13}xz + b_{22}y^2 + b_{23}yz + b_{33}z^2. \end{cases}$$

En supposant que $a_{ij} = a_{ji}$ et que $b_{ij} = b_{ji}$ pour $i, j \in \{1,2,3\}$ nous pouvons définir 15 constantes intimement liées aux formes quadratiques ternaires f_1 et f_2, soit

$$\lambda_{kl}^{ij} = \lambda_{kl}^{ij}(f_1, f_2) = \text{Dét} \begin{pmatrix} a_{ij} & b_{ij} \\ a_{kl} & b_{kl} \end{pmatrix}.$$

Ainsi, on peut trouver l'unique solution du système

$$p(r_1, r_2, r_3, s_1, s_2, s_3) = q(r_1, r_2, r_3, s_1, s_2, s_3)$$

en explicitant les constantes du système d'équations pour chaque permutation (i,j,k) de $(1,2,3)$:

$$\begin{cases} c_{ii}^i = \pm\lambda_{ij}^{ik} + C_i, \\ c_{ii}^j = \pm\lambda_{ik}^{ii}, \\ c_{ij}^i = \pm\frac{1}{2}\lambda_{jj}^{ik} + \frac{1}{2}C_i, \\ c_{ij}^k = \pm\lambda_{ii}^{ij}, \end{cases} \tag{4.2}$$

où $\pm$ désigne le signe de la permutation et les constantes C_i sont définies par

$$\begin{cases} C_1 = \lambda_{11}^{23}, \\ C_2 = -\lambda_{22}^{13}, \\ C_3 = \lambda_{33}^{12}. \end{cases} \tag{4.3}$$

Il est à noter que ce système possède la propriété intéressante que tous les c_{ij}^k que l'on cherche à calculer sont tous des éléments de $\mathbb{Z}$. Caractéristique notable puisque l'on tentait d'associer à deux formes quadratiques ternaires intégrales la structure sous-jacente d'un anneau quartique définie par (4.1). Ne reste plus qu'à calculer concrètement

les c_{ij}^0 qui sont implicitement déterminés par les c_{ij}^1, c_{ij}^2, c_{ij}^3 en calculant les expressions $(\alpha_1\alpha_2)\alpha_3$ et $\alpha_1(\alpha_2\alpha_3)$ à l'aide encore une fois de (4.1). Explicitement on obtient les entiers

$$c_{ij}^0 = \sum_{r=1}^{3} c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k, \tag{4.4}$$

pour tout $k \in \{1,2,3\}\backslash\{j\}$.

En résumé, nous pouvons condenser la correspondance entre les anneaux quartiques et les formes quadratiques ternaires dans le théorème suivant.

Théorème 11. *Soit $(f_1(x,y,x), f_2(x,y,z))$ une paire de formes quadratiques ternaires, Q un anneau quartique de base $\{1,\alpha_1,\alpha_2,\alpha_3\}$ et R un anneau cubique de base $\{1,\omega_1,\omega_2\}$. Si le couple $(f_1(x,y,x), f_2(x,y,z))$ représente la fonction $\widetilde{\varphi}_{4,3}$ de la manière suivante*

$$\widetilde{\varphi}_{4,3}(x\overline{\alpha}_1 + y\overline{\alpha}_2 + z\overline{\alpha}_3) = f_1(x,y,z)\overline{\omega}_1 + f_2(x,y,z)\overline{\omega}_2$$

pour la paire d'anneaux (Q,R), où $\overline{\alpha}_1,\overline{\alpha}_2,\overline{\alpha}_3,\overline{\omega}_1,\overline{\omega}_2$ correspondent à la réduction de $\alpha_1,\alpha_2,\alpha_3,\omega_1,\omega_2$ modulo $\mathbb{Z}$, alors l'anneau quartique $Q(f_1(x,y,x), f_2(x,y,z)) = Q$ est uniquement déterminé par $f_1(x,y,x)$ et $f_2(x,y,z)$. Sa structure multiplicative est donnée par (4.1), (4.2), (4.3) *et* (4.4) *et on a de plus que*

$$Disc(Q) = Disc(f_1(x,y,x), f_2(x,y,z)).$$

Démonstration. Voir la construction précédente et [3].

C.Q.F.D.

4.3.3 Delone et Faddeev

Avant d'entamer l'étude de la paramétrisation des anneaux cubiques, faisons un bref retour historique en introduisant les travaux des mathématiciens B.N. Delone et D.K. Faddeev ([5]) sur les formes cubiques. Leurs travaux sont en quelque sorte précurseurs de ceux de Bhargava. Soit M un module d'un corps cubique dont la base unitaire est donnée par $\{1,\omega_1,\omega_2\}$. Rien *a priori* certifie que M soit un anneau cubique de

ce même corps. Toutefois, il faut et il suffit que les produits des éléments de la base de M appartiennent à M pour que ce module soit un anneau. Autrement dit, M est un anneau cubique si les produits ω_1^2, ω_2^2 et $\omega_1\omega_2$ sont dans M. Si d'un autre côté le déterminant de la transformation amenant la base du corps cubique de référence sur la base de l'anneau $\{1, \omega_1, \omega_2\}$ est non nul, alors il sera possible d'écrire les produits ci-haut comme combinaisons linéaires des éléments de la base de M, soit

$$\begin{cases} \omega_1^2 = A_0 + A_1\omega_1 + A_2\omega_2, \\ \omega_2^2 = B_0 + B_1\omega_1 + B_2\omega_2, \\ \omega_1\omega_2 = C_0 + C_1\omega_1 + C_2\omega_2. \end{cases} \tag{4.5}$$

Soit maintenant $\rho = a_0 + a_1\omega_1 + a_2\omega_2$ un élément engendrant le corps cubique et appartenant à l'anneau M. Posons également $\rho^2 = b_0 + b_1\omega_1 + b_2\omega_2$. Alors, il est possible de calculer ω_1 et ω_2 à l'aide de ρ et ρ^2, c'est-à-dire

$$\begin{cases} \omega_1 = \dfrac{-a_2\rho^2 + b_2\rho + a_2b_0 - a_0b_2}{\Delta}, \\ \omega_2 = \dfrac{-a_1\rho^2 - b_1\rho + a_0b_1 - a_1b_0}{\Delta}, \end{cases}$$

où $\Delta = a_1b_2 - a_2b_1$.

Donc tout $m \in M$ s'écrit sous la forme $\dfrac{\alpha + \beta\rho + \gamma\rho^2}{\Lambda}$. Ainsi, tous les éléments de M s'expriment comme une combinaison linéaire de 1, ρ et ρ^2 ayant un dénominateur commun Λ. Ce dénominateur en question est appelé l'indice de ρ et c'est grâce à ce dernier que nous pourrons relier l'anneau M aux formes cubiques binaires. En effet, il est possible de calculer Λ en termes des coefficients a_1 et a_2 de ρ de manière à obtenir

$$\Lambda = a_1^3A_2 + a_1^2a_2(2C_2 - A_1) + a_1a_2^2(B_2 - 2C_1) - a_2^3B_1.$$

On constate alors, en posant $a_1 = x$ et $a_2 = y$, que l'indice de ρ peut être vu comme la forme cubique binaire

$$f(x, y) = x^3A_2 + x^2y(2C_2 - A_1) + xy^2(B_2 - 2C_1) - y^3B_1.$$

C'est cette forme, notée forme-indice de la base $\{1, \omega_1, \omega_2\}$, que Delone et Faddeev mettent en bijection avec l'anneau cubique de départ M. Voyons quelques propriétés

intéressantes de cette forme cubique particulière.

Définition. Les bases $\{1, \omega_1, \omega_2\}$ et $\{1, \omega_1 + c_1, \omega_2 + c_2\}$, où $c_1, c_2 \in \mathbb{Z}$ sont dites des *bases unitaires parallèles*. L'ensemble des bases parallèles entre elles est appelé un *parallèle de bases unitaires*. Si de plus $\omega_1\omega_2 \in \mathbb{Z}$, alors la base est dite *normale*.

Proposition. *Il existe une et une seule base normale parmi toutes les bases parallèles de l'anneau cubique M.*

Proposition. *La même forme-indice correspond à toutes les bases unitaires parallèles d'un anneau cubique M.*

Ces deux propositions impliquent le théorème central de cette section, lequel relit les formes cubiques aux anneaux cubiques.

Théorème 12. *À toutes les formes cubiques binaires irréductibles à coefficients entiers correspond un parallèle de bases unitaires d'un anneau cubique appartenant à un corps cubique unitaire.*

Démonstration. Voir [5].

C.Q.F.D.

Autrement dit, il est possible d'attacher une forme cubique binaire à tous les anneaux cubiques appartenant à un corps cubique unitaire quelconque. Ainsi, et c'est là l'idée principale de Dalone et Faddeev, il existe une correspondance biunivoque ou de manière équivalente, il existe une paramétrisation entre les formes cubiques et les anneaux cubiques. Paramétrisation, comme nous l'avons précédemment vu, construite à l'aide de la structure multiplicative de l'anneau et de l'indice d'un élément typique de ce même anneau. Pour retrouver l'idée commune aux deux paramétrisations que nous allons voir sous peu, il s'agit d'écrire la forme-indice $f(x, y)$ associée à un anneau cubique comme $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ et de voir les éléments ω_1 et ω_2 de la

base de cet anneau comme étant les racines respectives des polynômes cubiques

$$\begin{cases} z^3 + bz^2 + acz + a^2d = 0, \\ z^3 - cz^2 + dbz - d^2a = 0. \end{cases}$$

De cette façon, $\{1, \omega_1, \omega_2\}$ correspond à une base unitaire normale d'un anneau cubique associé à la forme $f(x, y)$ et dont la table multiplicative est donnée par

$$\begin{cases} \omega_1\omega_2 = -ad, \\ \omega_1^2 = -ac + b\omega_1 - a\omega_2, \\ \omega_2^2 = -bd + d\omega_1 - c\omega_2. \end{cases}$$

Pour retrouver cette table, il suffit de remarquer la dépendance entre les coefficients A_i, B_i et C_i, pour $1 \leq i \leq 3$. En effet, on observe aisément que

$$\begin{cases} A_0 = A_2(C_1 - B_2) - C_2(A_1 - C_2), \\ B_0 = B_1(C_2 - A_1) - C_1(B_2 - C_1), \\ C_0 = A_2B_1 - C_1C_2, \end{cases}$$

ce qui nous permet de redéfinir des entiers a, b, c et d pour ainsi condenser l'écriture de la forme cubique Λ associée à l'anneau cubique M en écrivant plutôt $\Lambda = f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. Soulignons également le fait intéressant suivant.

Proposition. *Le discriminant de la forme-indice $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ est égal au discriminant de l'anneau cubique qui lui est associé.*

Généralement, dans la littérature ([6]), on associe à la notion d'indice la définition suivante.

Définition. Soit $\mathbb{K}$ un corps de nombres. Soit $\theta \in \mathcal{O}_{\mathbb{K}}$ tel que $\mathbb{K} = \mathbb{Q}(\theta)$. Alors, l'*indice* de θ, noté $ind(\theta)$, est l'entier positif donné par

$$Disc(\theta) = ind(\theta)^2 Disc(\mathbb{K}).$$

4.3.4 Structure d'un anneau cubique

Nous avons vu dans les sections précédentes l'intime relation entre la structure de l'anneau quartique Q du couple (Q, R) et les formes quadratiques ternaires. Mais qu'en est-il de la structure de l'anneau résolvant associé R ? Est-ce que sa structure multiplicative peut être aussi précisément déterminée par les formes quadratiques ternaires ? Nous verrons que c'est effectivement le cas. Outre la paramétrisation déjà connue via les formes cubiques binaires sous laquelle une forme $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ est associée un anneau cubique R de base $\{1, \omega_1, \omega_2\}$ avec la structure donnée en (4.5) et dont $Disc(f(x, y) = Disc(R)$, il nous est possible d'utiliser les formes quadratiques ternaires pour une paramétrisation différente bien que tout aussi efficace. En effet, les calculs suivants nous permettent de mettre en relief cette correspondance ([13]). Soit

$$M(f_1) = M(f_1(x, y, z)) = \begin{pmatrix} a & u/2 & w/2 \\ u/2 & b & v/2 \\ w/2 & v/2 & c \end{pmatrix}$$

et

$$M(f_2) = M(f_2(x, y, z)) = \begin{pmatrix} a' & u'/2 & w'/2 \\ u'/2 & b' & v'/2 \\ w'/2 & v'/2 & c' \end{pmatrix}$$

les deux matrices associées aux formes quadratiques ternaires $f_1(x, y, z)$ et $f_2(x, y, z)$.

Ainsi,

$$4 \cdot \text{Dét}(M(f_1)x - M(f_2)y))$$

$$= 4 \cdot \text{Dét}\left(\begin{pmatrix} a & u/2 & w/2 \\ u/2 & b & v/2 \\ w/2 & v/2 & c \end{pmatrix} x - \begin{pmatrix} a' & u'/2 & w'/2 \\ u'/2 & b' & v'/2 \\ w'/2 & v'/2 & c' \end{pmatrix} y\right)$$

$$= 4 \cdot \begin{pmatrix} ax - a'y & \dfrac{ux - u'y}{2} & \dfrac{wx - w'y}{2} \\ \dfrac{ux - u'y}{2} & bx - b'y & \dfrac{vx - v'y}{2} \\ \dfrac{wx - w'y}{2} & \dfrac{vx - v'y}{2} & cx - c'y \end{pmatrix}$$

$$= 4 \cdot (ax - a'y)\text{Dét}\begin{pmatrix} bx - b'y & \dfrac{vx - v'y}{2} \\ \dfrac{vx - v'y}{2} & cx - c'y \end{pmatrix} - 4 \cdot \left(\frac{ux - u'y}{2}\right)\text{Dét}\begin{pmatrix} \dfrac{ux - u'y}{2} & \dfrac{vx - v'y}{2} \\ \dfrac{wx - w'y}{2} & cx - c'y \end{pmatrix}$$

$$+4 \cdot \left(\frac{wx - w'y}{2}\right)\text{Dét}\begin{pmatrix} \dfrac{ux - u'y}{2} & bx - b'y \\ \dfrac{wx - w'y}{2} & \dfrac{vx - v'y}{2} \end{pmatrix}$$

$$= \alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3 = g(x, y),$$

ce qui permet de mieux voir le lien entre les formes quadratiques ternaires et les formes cubiques en associant à un couple de formes ternaires $(f_1,\ f_2)$, la forme cubique $g(x, y) = 4 \cdot \text{Dét}(M(f_1)x - M(f_2)y)$ ayant le même discriminant que l'anneau quartique $Q(f_1, f_2)$. En fait, cette forme $g(x, y)$ est égale à la forme cubique $f(x, y)$ précédemment calculée lors de la première paramétrisation. Effectivement, ce que le théorème suivant stipule n'est ni plus ni moins que l'équivalence des deux paramétrisations étudiées dans le cas d'un anneau cubique R.

Théorème 13. ([3]) *Soit R un anneau cubique et soit $f(x, y)$ sa forme cubique associée. Soit également une paire de formes quadratiques ternaires $(f_1(x, y, z), f_2(x, y, x))$ vérifiant $Disc(f_1(x, y, z), f_2(x, y, z)) \neq 0$. Alors, si $(f_1(x, y, z), f_2(x, y, x))$ représente la fonction $\widetilde{\varphi}_{4,3}$ de la façon*

$$\widetilde{\varphi}_{4,3}(x\overline{\alpha}_1 + y\overline{\alpha}_2 + z\overline{\alpha}_3) = f_1(x, y, z)\overline{\omega}_1 + f_2(x, y, z)\overline{\omega}_2$$

pour la paire d'anneaux (Q, R), où $\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}_3, \overline{\omega}_1, \overline{\omega}_2$ correspondent à la réduction de $\alpha_1, \alpha_2, \alpha_3, \omega_1, \omega_2$ modulo $\mathbb{Z}$, alors l'anneau cubique $R = R(f_1, f_2)$ est uniquement déterminé par les formes quadratiques ternaires $f_1(x, y, z)$ et $f_2(x, y, z)$. Nous avons également

que $Disc(R(f_1, f_2)) = Disc(f_1, f_2)$ *et que la table de multiplication de cet anneau est donnée par*

$$\begin{cases} \omega_1\omega_2 = -ad, \\ \omega_1^2 = -ac + b\omega_1 - a\omega_2, \\ \omega_2^2 = -bd + d\omega_1 - c\omega_2, \end{cases}$$

et l'équation

$$ax^3 + bx^2y + cxy^2 + dy^3 = 4 \cdot \text{Dét}(M(f_1)x - M(f_2)y)).$$

Nous venons donc de voir, par le biais de ces deux théorèmes, que pour un couple de formes quadratiques ternaires $(f_1(x, y, z), f_2(x, y, z))$, il est possible de déterminer un unique anneau quartique ainsi qu'un unique anneau cubique attachés à ces formes. L'unicité étant définie par la structure multiplicative imposée par ces mêmes formes ternaires. Mais à première vue, hormis la correspondance entre formes ternaires et anneaux, rien n'implique que R soit la résolvante cubique de Q. Nous verrons dans ce qui suit que l'anneau $R(f_1, f_2)$ est effectivement la résolvante cubique associée à l'anneau quartique $Q(f_1, f_2)$ et que $(f_1(x, y, z), f_2(x, y, z))$ décrit bien la fonction $\widetilde{\varphi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$.

Nous savons déjà que $Disc(Q) = Disc(R)$, il suffit donc de montrer que si $F = w + x\alpha_1 + y\alpha_2 + z\alpha_3$ est le polynôme caractéristique d'un élément typique de Q, alors il existe une constante $c \in \mathbb{Z}$ telle que le polynôme caractéristique G de l'élément $c + f_1(x, y, z)\omega_1 + f_2(x, y, z)\omega_2 \in R$ soit la résolvante cubique de F. Cette étape se calcule à l'aide des systèmes (4.1), (4.2), (4.3) et (4.4) pour ce qui est de déterminer F tandis qu'on se sert de la table multiplicative usuelle pour calculer G. Cette démarche via les polynômes caractéristiques permet d'énoncer la proposition voulue.

Proposition. *Soit* $(f_1(x, y, z), f_2(x, y, z))$ *un couple de formes quadratiques ternaires tel que* $Disc(f_1(x, y, z), f_2(x, y, z)) \neq 0$. *Soit également* $Q(f_1, f_2)$ *et* $R(f_1, f_2)$ *l'anneau quartique et cubique associés à* $(f_1(x, y, z), f_2(x, y, z))$ *via les Théorèmes* 12 *et* 13. *Alors, l'anneau* $R(f_1, f_2)$ *est la résolvante cubique de* $Q(f_1, f_2)$.

Nous avons également la proposition suivante illustrant bien la propriété de conservation du discriminant qu'implique la bijection implicite des deux théorèmes précédents.

Proposition. *La bijection du Théorème* 13 *préserve le discriminant. C'est-à-dire, soit* (Q, R) *une paire d'anneaux associée au couple de formes quadratiques ternaires* $(f_1(x, y, z), f_2(x, y, z))$. *Alors*

$$Disc((f_1(x, y, z), f_2(x, y, z)) = Disc(Q) = Disc(R).$$

Chapitre 5

Autres résultats

En 1770, Joseph Louis Lagrange énonça son fameux théorème sur la somme de quatre carrés marquant ainsi le début de la théorie universelle des formes quadratiques.

Théorème de Lagrange. *Tout entier positif s'exprime comme la somme d'au plus quatre carrés.*

Pour faire suite à ce dernier théorème, le mathématicien Adrien Marie Legendre énonce quant à lui le théorème des trois carrés pour ainsi permettre l'identification des entiers qui ont réellement besoin de quatre carrés pour être exprimés comme somme de carrés.

Définition. Une forme est dite *diagonale* si aucun croisement d'indéterminées n'apparaît dans son écriture, c'est-à-dire

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i^m,$$

pour un certain degré m. De plus une forme est dite *universelle* si elle représente tous les entiers. Utilisons la notation $[a, b, c, d]$ pour signifier la forme quadratique quaternaire $f(x, y, z, w) = ax^2 + by^2 + cz^2 + dw^2$.

En 1916 Ramanujan, croyait avoir exhibé les seules formes diagonales quadratiques quaternaires définies positives et universelles. Il fallut cependant corriger légèrement son travail en retranchant la forme $[1, 2, 5, 5]$ de sa liste, de sorte que la liste officielle

de ces formes universelles est la suivante :

$$[1,1,1,1],\ [1,1,1,2],\ [1,1,1,3],\ [1,1,1,4],\ [1,1,1,5],\ [1,1,1,6],$$
$$[1,1,1,7],\ [1,1,2,2],\ [1,1,2,3],\ [1,1,2,3],\ [1,1,2,5],\ [1,1,2,6],$$
$$[1,1,2,7],\ [1,1,2,8],\ [1,1,2,9],\ [1,1,2,10],\ [1,1,2,11],\ [1,1,2,12],$$
$$[1,1,2,13],\ [1,1,2,14],\ [1,1,3,3],\ [1,1,3,4],\ [1,1,3,5],\ [1,1,3,6],$$
$$[1,2,2,2],\ [1,2,2,3],\ [1,2,2,4],\ [1,2,2,5],\ [1,2,3,8],\ [1,2,3,9],$$
$$[1,2,3,10],\ [1,2,4,4],\ [1,2,4,5],\ [1,2,4,6],\ [1,2,4,7],\ [1,2,4,8],$$
$$[1,2,4,9],\ [1,2,4,10],\ [1,2,4,11],\ [1,2,4,12],\ [1,2,4,13],\ [1,2,4,14],$$
$$[1,2,5,6],\ [1,2,5,7],\ [1,2,5,8],\ [1,2,5,9],\ [1,2,5,10].$$

En 1948, la mathématicienne M. Willerding fit une tentative d'énumération de toutes les formes quaternaires pouvant être universelles. Tentative qui malheureusement comportait quelques lacunes puisque ladite liste, en plus de répéter deux fois une forme précise, fut rallongée par Manjul Bhargava quelques années plus tard.

En 1993, un développement intéressant fut apporté par les mathématiciens J.H. Conway et W. Schneeberger ([11]). Ils ont étudié les matrices entières des formes quadratiques en espérant trouver une constante c telle que si ces mêmes matrices entières représentaient tous les entiers jusqu'à cette constante c, alors ces formes, associées aux matrices entières seulement, étaient universelles. Parallèlement, s'il existait une telle constante c pour les matrices, se pourrait-il qu'il y ait une constante C pour laquelle une forme quadratique à coefficients entiers représentant tous les entiers plus petits ou égaux à C, les représenterait tous ? Autrement dit, transposer le problème de représentation des entiers initialement défini pour les formes relevant de matrices entières seulement au cas plus général des formes quadratiques à coefficients entiers. La différence entre ces deux problèmes résulte dans le fait que le premier considère seulement les formes dont les coefficients des indéterminées entrecroisés sont pairs. C'est-à-dire, dont la matrice associée est entière. Par comparaison, dans le deuxième problème on permet des coefficients impairs, donc une matrice dont les coefficients ne sont pas tous entiers. Ils énoncèrent un préambule au Théorème des 15, soit le Théorème des 290, qu'ils allaient par la suite peaufiner, notamment à l'aide d'ordinateurs, et dont Bhargava allait donner une autre preuve au début des années 2000.

Théorème des 290. ([10]) Soit $f(x,y)$ une forme quadratique binaire, définie po-

sitive et à coefficients entiers. Alors $f(x, y)$ représente tous les entiers si et seulement si elle représente tous les entiers jusqu'à 290.

En 2005, la valeur de la constante C pour les formes à matrices non entières fut fixée à 15 par Bhargava et Jonathan P. Hanke. Cette preuve donna naissance à l'énoncé du Théorème des 15 (15-*Theorem*).

Théorème des 15. ([10],[11]) *Si une forme quadratique définie positive possède une matrice entière représentant tous les entiers positifs jusqu'à* 15*, alors elle représente tous les entiers positifs.*

Chapitre 6

Conclusion

Les points centraux de ce mémoire sont sans aucun doute les Théorèmes 1.1 et 1.2 ainsi que leurs conséquences. Nous avons pu dériver de ces Théorèmes six autres lois de composition qui ont fait l'objet d'une étude plus approfondie. Elles ont notamment revisité la loi de composition de Gauss en plus de construire une loi de composition des cubes $2 \times 2 \times 2$. Elles ont également été définies sur les formes cubiques binaires et les paires de formes quadratiques binaires. Dans ses travaux, M. Bhargava poursuit l'étude de ces lois de composition sur les paires de formes quaternaires alternées ainsi que sur les formes alternées à six variables. En tout, quatorze lois furent élaborées à la lumière desquelles nous avons pu extraire des informations intéressantes concernant les anneaux de nombres et leurs groupes de classes. Dans chacun des six espaces mentionnés plus haut, un travail analogue à celui de Gauss fut accompli. En effet, tout comme Gauss le fit pour les formes quadratiques binaires, une action de groupe sur $\mathbb{Z}$ a été définie sur chacun de ces espaces. De plus, on a remarqué que ces actions avaient elles aussi la propriété de posséder un invariant unique ainsi qu'une propriété d'éléments projectifs, notion similaire à celle de formes primitives pour les formes binaires quadratiques. Finalement, nous avons équipé l'ensemble des orbites des éléments projectifs de discriminant fixé D de ces six espaces L, noté $Cl(L; D)$, d'une structure de groupe abélien. Par la suite nous avons vu comment ces mêmes lois de composition peuvent être remaniées en termes d'anneaux et de classes d'idéaux. Les travaux de Bhargava s'étendent également à la géométrie algébrique des nombres. Elle constitue en effet, pour ce qui est de la paramétrisation des anneaux quintiques, une magnifique interaction entre ce style de géométrie et la théorie des invariants.

Bibliographie

[1] Manjul Bhargava, *Higher composition laws* I : *A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. **159** (2004), no. 1, 217 - 250.

[2] Manjul Bhargava, *Higher composition laws* II : *On cubic analogues of Gauss composition*, Ann. of Math. **159** (2004), no. 2, 865 - 886.

[3] Manjul Bhargava, *Higher composition laws* III : *The parametrization of quartic rings*, Ann. Math. **159** (2004), 1329 - 1360.

[4] Manjul Bhargava, *Higher composition laws* IV : *The parametrization of quintic rings*, Ann. of Math., à paraître.

[5] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[6] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, 2004.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[8] Paulo Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Verlag, 2001.

[9] Jean-Pierre Escofier, *Théorie de Galois*, Sciences Sup, Dunod, 1997.

[10] Manjul Bhargava, *On the Conway-Schneeberger fifteen Theorem*, à paraître.

[11] J. H. Conway, *Universal quadratic forms and the Fifteen Theorem*, à paraître.

[12] Richard A. Mollin, *Quadratics*, CRC Press, 1996.

[13] D.A. Buell, *Binary Quadratic Forms : Classical Theory and Modern Computations*, Springer-Verlag, 1989.

[14] Daniel E. Flath, *Introduction to number theory*, Wiley, 1989.