LOIS DE COMPOSITIONS DE BHARGAVA

EMMANUEL LECOUTURIER, SÉBASTIEN MIQUEL

SOUS LA DIRECTION D'OLIVIER TAÏBI

Table des matières

1. Introduction

Dans ses articles de la série *Higher composition laws* : *A new view on Gauss compostion and quadratic generalizations* ([1]), *On cubic analogues of Gauss composition* ([2]) et *The parametrization of quartic rings* ([3]), Bhargava décrit des paramétrisations de structures algébriques, comme des anneaux de degrés $2, 3, 4$ et des modules de ceux-ci.

On considère des couples judicieux (G, V) d'un groupe algébrique G et d'une représentation V. L'étude des orbites de cette action a déjà été étudiée sur des corps algébriquement clos et sur $\mathbb{Q}$ dans [7] et [12]. Bhargava s'intéresse lui aux orbites entières, munies d'une structure très riche. En fait dans l'études de ces divers couples (G, V), on peut noter des points communs. Premièrement, l'action possède un « unique invariant », appelé le discriminant. Quand le discriminant est non nul, on parle d'orbite non dégénérée. Ensuite, sur un corps algébriquement clos, tous les éléments de V de même discriminant (non nul) sont équivalents sous l'action de G. Il est en effet raisonnable de penser que sur un corps, l'étude des orbites est plus facile que sur $\mathbb{Z}$ (cf section 2.1 pour plus de détails).

Nous allons dans une première partie montrer comment Bhargava retrouve, dans un contexte plus général un résultat de Gauss sur les formes quadratiques.

Gauss dans son livre *Disquisitiones Arithmeticae* ([8]) étudie les classes d'équivalence de formes quadratiques binaires à coefficients entiers sous l'action de $SL_2(\mathbb{Z})$ par changement de variable :

$$(\gamma \cdot f)(x, y) = f((x, y)\gamma)$$

Il montre en particulier qu'il y a un nombre fini de classes et donne un algorithme très simple pour les déterminer. Il munit également cet ensemble d'une structure de groupe appelée composition de Gauss. Il s'avère que ce groupe est isomorphe au groupe des classes d'idéaux inversibles d'un certain anneau quadratique. Le groupe des classes d'idéaux d'un anneau est le groupe des d'idéaux « inversibles » (cf appendice) modulo les idéaux principaux. Ce groupe mesure le « défaut de principalité » de l'anneau puisqu'il est trivial ssi l'anneau est principal. Il est par ailleurs important de pouvoir dire si un idéal donné est principal, ce qui se voit en vérifiant si sa classe dans le groupe des classes d'idéaux est triviale. Ce couple $(G, V) = (SL_2(\mathbb{Z}), (\mathrm{Sym}^2\mathbb{Z}^2)^*)$ vérifie bien les conditions énoncées plus haut, à savoir qu'il y a un unique polynôme (abus de langage) en les coefficients de la forme invariant par $SL_2(\mathbb{Z})$, qu'on appelle discriminant, et que sur $\mathbb{C}$, toutes les formes d'un discriminant $D \neq 0$ fixé sont équivalentes sous l'action de $SL_2(\mathbb{C})$.

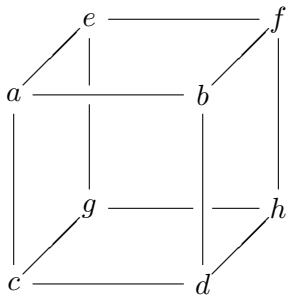
L'approche de Bhargava donne lieu à une méthode plus générale dont les applications découlent de calculs formels explicites. D'une part elle permet d'isoler certains sous-groupes du groupe des classes (par exemple le sous-groupe d'exposant 3 dans le cas quadratique et le sous-groupe d'exposant 2 dans le cas cubique), d'une autre, elle fournit de nombreuses nouvelles lois de composition sur des ensembles de formes.

La paramétrisation des anneaux cubiques présente une nouvelle difficulté, surmontée en écrivant explicitement les tables de multiplication de l'anneau et Bhargava démontre des résultats analogues à ceux du cas quadratique. Dans le cas quartique, cette paramétrisation est nettement plus compliquée : on paramétrise des couples (R, Q) où R est un anneau quartique et Q est un anneau cubique appelé résolvante cubique de R, qui n'est pas unique. Cela est lié à la résolution de l'équation de degré 4, qui se fait en se ramenant à une équation de degré 3 appelée « résolvante de Lagrange ».

Nous remercions Olivier Taïbi pour son aide sans laquelle nous n'aurions pas aussi bien compris les résultats (parfois miraculeux) de Bhargava.

2. Cas quadratique

2.1. **Cube d'entiers, formes quadratiques.** L'idée fondamentale de Bhargava est de considérer les orbites de l'action naturelle du groupe $\Gamma := SL_2(\mathbb{Z})^3$ sur l'espace $C = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, qu'il est pratique de représenter par des cubes d'entiers.



Plus précisement, on fait agir $(\gamma_1, \gamma_2, \gamma_3) \in \Gamma$ sur $x_1 \otimes x_2 \otimes x_3$ par

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

Un cube d'entier peut être découpé en 2 matrices 2×2 de 3 façons différentes :

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

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

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

On peut interpréter notre action sur ces matrices : le premier facteur de $SL_2(\mathbb{Z})$ agit sur le cube A en remplaçant (M_1, N_1) par (rM_1+sN_1, tM_1+uN_1), où $ru-st = 1$, γ_2 remplace (M_1, N_1) par $(M_1^t\gamma_2, N_1^t\gamma_2)$ et γ_3 par $(\gamma_3 M_1, \gamma_3 N_1)$.

Définition 1. *Une forme quadratique binaire à coefficients entiers est une forme quadratique $f(x, y) = ax^2 + bxy + cy^2$ avec a,b,c $\in \mathbb{Z}$. On définit le discriminant de f par $\Delta = b^2 - 4ac$. La forme f est dite primitive si pgcd$(a, b, c) = 1$.*

A un cube A, on peut alors associer trois formes quadratiques, données par

$$Q_i(x, y) = -\mathrm{Det}(M_i x - N_i y)$$

Explicitement, on a les formules :

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

L'action sur les cubes induit une action sur chaque forme : les facteurs γ_2 et γ_3 ne modifient pas Q_1 et on a $(\begin{pmatrix} r & s \\ t & u \end{pmatrix}, Id, Id).Q_1 = Q_1 \circ \begin{pmatrix} r & -t \\ -s & u \end{pmatrix}$, ce qui correspond à l'action classique de $SL_2(\mathbb{Z})$ sur les formes quadratiques.

On vérifie que les discriminants des Q_i sont égaux, on définit ainsi le discriminant d'un cube, qui est un invariant de l'action considérée. Explicitement :

$$Disc(A) = a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(edfg + bceh)$$

Définition 2. *On dit qu'un cube est projectif si ses trois formes associées sont primitives.*

Si A est un sous-anneau de $\mathbb{C}$, notons $G_A = SL_2(A)^3$ et $V_A = A^2 \otimes_A A^2 \otimes_A A^2$. Nous voulons étudier les orbites de l'action de $G_{\mathbb{Z}}$ sur $V_{\mathbb{Z}}$. Si $A \subset B \subset \mathbb{C}$ sont des sous-anneaux, deux éléments équivalents sur A (i.e. dans la même G_A-porbite) le sont sur B. Il est intéressant de se poser la question inverse : si deux

éléments de G_A sont équivalents sur B, alors le sont-ils sur A ? Par exemple si on prend $V_A = M_n(A)$ et $G_A = GL_n(A)$ qui agit par conjugaison, alors on a le résultat suivant : si $\mathbb{Q} \hookrightarrow K \hookrightarrow L \hookrightarrow \mathbb{C}$ sont des extensions de corps où $K \hookrightarrow L$ est galoisienne, alors deux matrices de $M_n(K)$ semblables sur L sont semblables sur K. Un exemple intéressant montrant la différence de complexité entre orbites entières et orbites sur un corps est celui des classes d'équivalence de matrices carrées. On sait que dans le cas des corps ces classes sont paramétrées par le rang, mais que par exemple sur $\mathbb{Z}$, il y a un autre invariant qui est la suite des facteurs invariants.

En tout cas, si on veut qu'il n'y ait pas trop d'orbites sur $\mathbb{Z}$, il faut qu'il y ait peu d'orbites sur $\mathbb{C}$ contenant un point de $V_{\mathbb{Z}}$. Dans notre cas ($V_A = A^2 \otimes_A A^2 \otimes_A A^2$), c'est effectivement le cas.

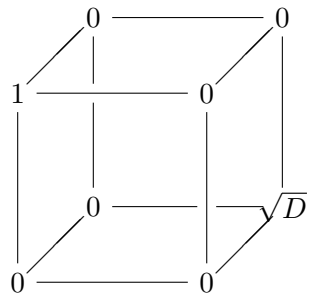
Proposition 1. *Toute forme non dégénérée (i.e de discriminant $D \neq 0$) q est $SL_2(\mathbb{C})$-équivalente à $x^2 - \frac{D}{4}y^2$. En outre* $\mathrm{Stab}(q) \simeq \mathbb{C}^*$.

Démonstration. Le premier point découle de la théorie classique des formes quadratiques sur un corps algébriquement clos. Pour le deuxième point, $\mathrm{Stab}(q)$ est conjugué à $\mathrm{Stab}(\sqrt{D}xy)$ qui est $\{\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}, \lambda \in \mathbb{C}^*\}$ (on fixe une racine carrée de D). □

La situation est similaire pour les cubes.

Proposition 2. *Tous les cubes non dégénérés (de discriminant non nul fixé) de $C = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ sont équivalents sous l'action de $SL_2(\mathbb{C})^3$.*

Démonstration. Soit c un cube non dégénéré de discriminant D. On note $f(c)$ le triplet de formes quadratiques associées. On remarque que f commute à l'action de $SL_2(\mathbb{C})^3$. Par la proposition précédente, on peut supposer que $f(c) = (\sqrt{D}xy, \sqrt{D}xy, \sqrt{D}xy)$ (on fait dans ce qui suit un choix de $\sqrt{D}$). On est ramené à montrer que tous les cubes de $f^{-1}((\sqrt{D}xy, \sqrt{D}xy, \sqrt{D}xy))$ sont équivalents. Montrons que tout cube de $f^{-1}((\sqrt{D}xy, \sqrt{D}xy, \sqrt{D}xy))$ est équivalent à :

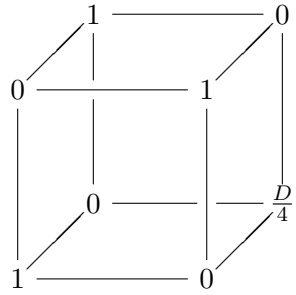


En effet, on peut supposer $a \neq 0$ quitte à faire des opérations élémentaires sur la première face (ce qui ne modifie pas $Q_1^A = \sqrt{D}xy$). En utilisant la matrice $\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$, on ne modifie pas Q_1^A et on peut remplacer a par 1. On fait des opérations sur les lignes de la première face pour obtenir $b = c = 0$ et cela ne modifie pas Q_1^A. Par les formules explicites des formes en fonction des coefficients du cube, on obtient $bc - ad = 0$, donc $d = 0$. En utilisant la formule pour le discriminant du cube, on voit que $h^2 = D \neq 0$. Sans changer la première face, on peut supposer $g = f = 0$ (opérations élémentaires sur la face arrière). Enfin, en retranchant un multiple de la face avant à la face arrière, on obtient $e = 0$, et le cube a bien la forme annoncée. □

On peut aussi étudier les orbites sur $\mathbb{Q}$ et cela nous sera utile dans la suite.

Proposition 3. *On note Γ' le sous-groupe de $GL_2(\mathbb{Q})^3$ constitué des triplets (A, B, C) de matrices telles que* $\mathrm{Det}(A) \cdot \mathrm{Det}(B) \cdot \mathrm{Det}(C) = 1$.
Alors tous les cubes d'un discriminant $D \neq 0$ fixé sont Γ'-équivalents.

Démonstration. On part d'un cube A de discriminant D quelconque. On sait que toute forme binaire est $SL_2(\mathbb{Q})$ équivalente à une forme du type $\lambda x^2 + \mu y^2$ où $\lambda,\ \mu \in \mathbb{Q}$. On peut donc supposer que $Q_1^A = \lambda x^2 + \mu y^2$, avec $-4 \cdot \lambda \cdot \mu = D \neq 0$. En faisant des opérations élémentaires sur M_1, on peut supposer que $c \neq 0$ ($M_1 \neq 0$ étant donné que $D \neq 0$), puis que $a = d = 0$. En retranchant un multiple de M_1 à N_1, on a $g = 0$. Ces opérations n'ont changé ni D ni Q_1^A. On peut multiplier M_1 par $\frac{1}{c}$ et N_1 par c : ça ne change pas D et Q_1^A reste de la forme $\alpha x^2 + \beta y^2$. On utilise l'expression explicite de Q_1^A : le coefficient en xy est nul, donc $f = 0$. On sait que $D = 4bceh \neq 0$, et on peut multiplier le cube par $\mathrm{Id} \times \mathrm{Id} \times \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & b \end{pmatrix}$ pour avoir $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $N_1 = \begin{pmatrix} e' & 0 \\ 0 & h' \end{pmatrix}$ et le discriminant reste le même. Donc $4e'h' = D \neq 0$. On multiplie alors le cube par $\mathrm{Id} \times \begin{pmatrix} \frac{1}{e'} & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & e' \end{pmatrix}$ (c'est à ce moment qu'on doit utiliser des éléments de Γ' et non de Γ), ce qui ne change pas M_1 mais remplace N_1 par $\begin{pmatrix} 1 & 0 \\ 0 & e'h' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{D}{4} \end{pmatrix}$. Tous les cubes sont donc Γ'-equivalents à □



2.2. **Lien entre les cubes et les classes d'idéaux dans des ordres quadratiques.**

Définition 3. *Un anneau de rang k est un anneau isomorphe à $\mathbb{Z}^k$ en tant que $\mathbb{Z}$-module. En particulier un anneau de rang 2 (resp. 3, 4) est appelé un anneau quadratique (resp. cubique, quartique).*

Définition 4. *Soit S un anneau de rang k. Pour $x \in S$, on note M_x la matrice de multiplication de x dans une base (α_i) choisie.*
On définit la trace d'un élément x de S par $Tr(x) = Tr(M_x)$ et sa norme $N(x) = \mathrm{Det}(M_x)$.
On définit aussi le polynôme caractéristique de x, noté χ_x, comme le polynôme caractéristique de M_x.
On définit le discriminant de x par $\mathrm{Disc}(x) = \mathrm{Disc}(\chi_x)$ où le discriminant d'un polynôme $P(X) = (X - \alpha_1)...(X - \alpha_n)$ est $\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$.
On définit aussi le discriminant d'une famille $(\alpha_1, ..., \alpha_n)$ de S par $\mathrm{Disc}(\alpha_1, ..., \alpha_n) = \mathrm{Det}((Tr(\alpha_i \alpha_j)))$
Si de plus $(\alpha_1, ..., \alpha_n)$ est une $\mathbb{Z}$-base de S, on pose $\mathrm{Disc}(S) = \mathrm{Disc}(\alpha_1, ..., \alpha_n)$, ce qui ne dépend pas de la base choisie.

Démonstration. Si on a une relation $(\alpha_1, ..., \alpha_n) = P(\beta_1, ..., \beta_n)$ où $P \in M_n(\mathbb{Z})$, alors on vérifie par linéarité de la trace que $(Tr(\alpha_i \alpha_j)) = P^t (Tr(\beta_i \beta_j)) P$, d'où $\mathrm{Disc}(\alpha_1, ..., \alpha_n) = \mathrm{Det}(P)^2 \mathrm{Disc}(\beta_1, ..., \beta_n)$. En particulier, si $(\alpha_1, ..., \alpha_n)$ et $(\beta_1, ..., \beta_n)$ sont deux bases de S, alors on peut trouver un tel $P \in GL_n(\mathbb{Z})$, donc $\mathrm{Det}(P)^2 = 1$ et $\mathrm{Disc}(\alpha_1, ..., \alpha_n) = \mathrm{Disc}(\beta_1, ..., \beta_n)$. □

Détaillons le cas particulier important où $S = \mathbb{Z}[\alpha]$ où α est un entier algébrique (i.e. annulé par un polynôme unitaire de $\mathbb{Z}[X]$, cf appendice pour plus de détails sur les entiers algébriques). Soit P le polynôme minimal (unitaire) de α sur $\mathbb{Q}$: on montre (cf appendice) que $P \in \mathbb{Z}[X]$ est irréductible et que si $n = deg(P)$, S est un anneau de rang n dont une base est $(1, \alpha, \alpha^2, ..., \alpha^{n-1})$. On va décrire simplement le discriminant des éléments de S. On va travailler dans le corps des fractions de S qui est $K = \mathbb{Q}(\alpha)$.

Définition 5. *On appelle morphisme de conjugaison un morphisme de corps $\sigma : \mathbb{Q}[\alpha] \to \mathbb{C}$.*

Proposition 4. *Il y a exactement $n = deg(P) = deg(\alpha)$ morphismes de conjugaison. Si on note $\alpha^{(i)}$ le i-ième conjugué de α (où $P(X) = (X - \alpha_1)(X - \alpha_2)(...)(X - \alpha_n)$ et $\alpha = \alpha_1$), le i-ième morphisme de conjugaison σ_i est donné par $\sigma_i(\alpha) = \alpha_i$.*

Démonstration. Soit σ un morphisme de conjugaison. Puisque σ est l'identité sur $\mathbb{Q}$, il est clair qu'il existe $i \in \{1, ..., n\}$ tel que $\sigma(\alpha) = \alpha_i$ et comme $(1, \alpha, ..., \alpha^{n-1})$ est une base de K, alors cette propriété détermine entièrement σ. Réciproquement, les morphismes σ_i de l'énoncé sont bien des morphismes de corps car on a un morphisme de corps $\mathbb{Q}[X] \to \mathbb{C}$ qui à Q associe $Q(\alpha_i)$ et cette flèche se factorise par $\mathbb{Q}[X]/(P) = K$. □

Définition 6. *Si $x \in S = \mathbb{Z}[\alpha]$, les n conjugués de x sont par définition $\sigma_1(x)$, ..., $\sigma_n(x)$.*

Proposition 5. *Si $x \in S$, $Tr(x) = \sigma_1(x) + ... + \sigma_n(x)$.*

Démonstration. Montrons la formule pour $x = \alpha^k$. On a $M_{\alpha^k} = M_\alpha^k$. La matrice de multiplication par α dans la base $(1, \alpha, ..., \alpha^{n-1})$ est la matrice compagnon associée à P qu'on peut donc trigonaliser, les coefficients diagonaux étant les $\sigma_i(\alpha)$. Alors $Tr(\alpha^k) = \sigma_1(\alpha)^k + ... + \sigma_n(\alpha)^k = \sigma_1(\alpha^k) + ... + \sigma_n(\alpha^k)$
Dans le cas général, on conclut par linéarité de la trace et des σ_i. □

Proposition 6. *Si $(\alpha_1, ..., \alpha_n)$ est une famille de S, alors*

$$\mathrm{Disc}(\alpha_1, ..., \alpha_n) = \mathrm{Det}(\sigma_j(\alpha_i))^2$$

Démonstration. On sait que $\sigma_k(\alpha_i\alpha_j) = \sigma_k(\alpha_i)\sigma_k(\beta_j)$, d'où la relation matricielle $(Tr(\alpha_i\alpha_j)) = (\sigma_i(\alpha_j))^t(\sigma_i(\alpha_j))$, et on passe au déterminant. □

Proposition 7. *Soit $x \in \mathbb{Z}[\alpha]$. Soit $d = [\mathbb{Q}(x) : \mathbb{Q}]$ le degré de x. Soit P_x le polynôme minimal unitaire de x (à coefficients entiers car x est un entier algébrique) et χ_x le polynôme caractéristique de x. Alors $\chi = P_x^{n/d} = (X - \sigma_1(x))(...)(X - \sigma_n(x))$.*

Démonstration. Soit y_1, ..., $y_{n/d}$ une $\mathbb{Q}(x)$-base de K sur $\mathbb{Q}(x)$. Alors on sait que

$$(y_1, xy_1, ..., x^{d-1}y_1, y_2, xy_2, ..., x^{d-1}y_2, ..., x^{d-1}y_{n/d})$$

est une base de K sur $\mathbb{Q}$. Dans cette base, la matrice de multiplication par x est une matrice diagonale par blocs dont les n/d blocs sont identiques, égaux à la matrice compagnon de P_x.

Pour la seconde égalité, on sait qu'il y a d morphismes de corps distincts $\tau_i : \mathbb{Q}(x) \to \mathbb{C}$, $i = 1, ..., d$. Or pour chaque i, τ_i s'étend en $n/d = [K : \mathbb{Q}(x)]$ différents morphismes $K \to \mathbb{C}$, et ce sont exactement les morphismes de conjugaison par cardinal (il y en a $n/d \cdot d = n$). On conclut car $P_x = (X - \tau_1(x))...(X - \tau_d(x))$ et $\chi_x = P_x^{n/d}$. □

On peut enfin expliquer le lien entre le discriminant d'un élément et le discriminant d'une famille d'éléments.

Corollaire 1. *Si $x \in \mathbb{Z}[\alpha]$, alors* $\mathrm{Disc}(x) = \mathrm{Disc}(1, x, ..., x^{n-1})$. *En particulier* $\mathrm{Disc}(\alpha) = \mathrm{Disc}(\mathbb{Z}[\alpha]) \neq 0$. *De plus si $deg(x) < n$ alors* $\mathrm{Disc}(x) = 0$.

Démonstration. On a $\mathrm{Disc}(\chi(x)) = \prod_{1 \leq i < j \leq n}(\sigma_i(x) - \sigma_j(x))^2$. Or on a vu que $\mathrm{Disc}(1, x, ..., x^{n-1}) = \mathrm{Det}(\sigma_j(x^i))^2 = \mathrm{Det}(\sigma_j(x)^i)^2 = \prod_{1 \leq i < j \leq n}(\sigma_i(x) - \sigma_j(x))^2 \neq 0$ (discriminant de Vandermonde).

Si $d = deg(x) < n$ alors $\mathrm{Disc}(x) = 0$ car χ_x a des racines multiples par la proposition précédente, donc $\mathrm{Disc}(x) = 0$.

□

Théorème 1. *(Classification des anneaux quadratiques)*
Le discriminant d'un anneau quadratique est un entier congru à 0 ou 1 modulo 4.
Réciproquement, pour tout tel D, il existe un unique (à isomorphisme près) anneau quadratique de discriminant D, donnée par

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

Plus précisemment, $S(D)$ a un base $(1,\tau)$, où la multiplication est définie par

$$\tau^2 = \frac{D}{4} \quad ou \quad \tau^2 = \frac{D-1}{4} + \tau$$

selon que D est congru à 0 ou 1 modulo 4.

Démonstration. En effet, si (α,β) est une base de S, on peut écrire $1 = u\alpha + v\beta$. Supposons par l'absurde que $d = pgcd(u,v) > 1$. Alors $1 = d(u'\alpha + v'\beta) = d^2(u'\alpha + v'\beta)^2 = d^2(u''\alpha + v''\beta)$ où $(u'\alpha + v'\beta)^2 = u''\alpha + v''\beta$ (u'' et v'' sont des entiers). Par unicité de l'écriture dans une base, $u = d^2u''$ et $v = d^2v''$, contradiction par définition de d.
Les entiers u et v sont donc premiers entre eux, et le vecteur (u,v) peut-être complété en un base de $\mathbb{Z}^2$. On obtient alors une base $(1,\tau)$ de S.
Soit r,s tels que $\tau^2 + r\tau + s = 0$. Alors $Tr(\tau) = -r$, $Tr(\tau^2) = r^2 - 2s$ donc $\mathrm{Disc}(S) = r^2 - 4s$ et on vérifie que la base $(1, \tau - \frac{r}{2})$ ou $(1, \tau - \frac{r+1}{2})$ convient. □

Chaque $S(D)$ est unique à isomorphisme près, mais possède 2 automorphismes d'anneau, selon le choix de $\sqrt{D}$, cela motive Bhargava à introduire une orientation : un anneau S est orienté si on a fait le choix d'une $\mathbb{Z}$-base orientée $(1,\tau)$.
De manière équivalente, on fait le choix d'une racine de D, qui munit S d'une projection $\pi : S \to \mathbb{Z}$ naturelle telle que $\pi(x) = Tr(\frac{x}{\sqrt{D}}) = \frac{x-x'}{\sqrt{D}}$, où x' est l'image de x par l'automorphisme non trivial de S.

Définition 7. *Soit S un anneau de rang k. Un idéal fractionnaire de S est un S-module inclus dans $K := S \otimes \mathbb{Q}$ et qui possède une $\mathbb{Z}$-base de rang k.*

Si S est orienté par une base $(1,\tau)$, une $\mathbb{Q}$-base (a,b) de K est positivement orienté si le determinant de la matrice de changement de base correspondante est positif.

Définition 8. *Un idéal orienté est une paire (I,ϵ), où I est un idéal fractionnaire et $\epsilon = \pm 1$.*
La multiplication de 2 idéaux orientés est définie composante par composante.

Par souci de clarté, on sous-entendra parfois l'orientation ϵ.

Définition 9. *Deux idéaux fractionnaires orientés sont dits équivalents si $(I_1,\epsilon_1) = (\kappa, sign(N(\kappa))).(I_2,\epsilon_2)$ pour un $\kappa \in K^\times$.*

Un idéal fractionnaire I est dit inversible s'il existe un idéal fractionnaire J tel que $I \cdot J = K$.

On définit le groupe étroit de classes d'idéaux comme le groupe des idéaux orientés inversibles, quotienté par cette relation d'équivalence. Par défaut, les idéaux principaux (κ) seront orientés par $\epsilon = \mathrm{sign}(N(\kappa))$. De plus, la multiplication des idéaux par un scalaire est définie par $\kappa \cdot I = (\kappa) \cdot I$ avec l'orientation précédente.

Définition 10. *(Norme d'un idéal orienté)*
Un réseau de K est un groupe abélien libre de rang 2 inclus dans K.
La norme d'un idéal orienté est définie par

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

où T est un réseau de K contenant $S(D)$ et I. Cette définition ne dépend pas de T.

Avec la convention précédente, on a alors $N((\kappa)) = N(\kappa)$ et $N(\kappa \cdot I) = N((\kappa)) \cdot N(I) = N(\kappa) \cdot N(I)$. La norme n'est pas toujours multiplicative. Plus précisément :

Proposition 8. *Soient I et J des idéaux fractionnaires de S. Si I est inversible, alors $N(IJ) = N(I)N(J)$.*

Démonstration. cf appendice pour la preuve et pour plus de détails sur la norme et l'inversibilité des idéaux. □

Définition 11. *On dit qu'un triplet (I_1, I_2, I_3) d'idéaux orientés est équilibré si $I_1I_2I_3 \subset S$ et $N(I_1)N(I_2)N(I_3) = 1$.*
Deux triplets équilibré (I_1, I_2, I_3) et (I'_1, I'_2, I'_3) sont dits équivalents s'il existe $\kappa_1, \kappa_2, \kappa_3 \in K$ tels que $I_i = \kappa_i \cdot I'_i$ et $\kappa_1\kappa_2\kappa_3 = 1$.

Notons que Bhargava n'a pas imposé la condition $\kappa_1\kappa_2\kappa_3 = 1$ dans sa définition mais cela pose un problème dans le théorème ci-dessous (nous donnerons un contre-exemple avec la définition de Bhargava).

On a une description très simple des triplets d'idéaux équilibrés dans le cas inversible.

Corollaire 2. *Si (I_1, I_2, I_3) est équilibré et que I_1 et I_2 sont inversibles, alors $I_1I_2I_3 = S$ (donc I_3 est inversible et $I_3^{-1} = I_1I_2$).*

Démonstration. Par la proposition précédente, $N(I_1I_2I_3) = N(I_1)N(I_2)N(I_3) = 1$, et comme $I_1I_2I_3 \subset S$, alors $I_1I_2I_3 = S$. □

2.3. **Correspondance entre cubes et triplets équilibrés.** On fixe un discriminant $D \equiv 0, 1 \bmod 4$ et un anneau quadratique orienté $S = S(D)$.

Définition 12. *Soient I_j $(j = 1, 2, 3)$ des idéaux orientés équilibrés de S et (α_1, α_2), (β_1, β_2), (γ_1, γ_2) des bases (positivement orientées) respectives de ces idéaux. De même pour des idéaux I'_j. On dit que $(I_j)_j$ et $(I'_j)_j$ (munis de leurs bases respectives) sont équivalents ssi $\exists \kappa_1, \kappa_2, \kappa_3 \in K := S \otimes \mathbb{Q}$ tels que $\kappa_1\kappa_2\kappa_3 = 1$ et $I'_j = \kappa_j \cdot I_j$, $\alpha_1 = \kappa_1\alpha'_1$, $\alpha_2 = \kappa_1\alpha'_2$, et de même pour β et γ.*

Théorème 2. *Soit $D \neq 0$ un entier congru à 0 ou 1 modulo 4.*
Il y a une bijection entre les cubes de discriminant D et les classes d'équivalences de triplets équilibrés $((I_1, (\alpha_1, \alpha_2)), (I_2, (\beta_1, \beta_2)), (I_3, (\gamma_1, \gamma_3)))$. De plus l'action de Γ commute à cette bijection.

Démonstration. On suppose pour simplifier $D \equiv 0 \bmod 4$. Soit $(1, \tau)$ la base orientée de S avec $\tau^2 = \frac{D}{4}$. On montre d'abord comment à un triplet d'idéaux associer un cube. Comme (I_1, I_2, I_3) est équilibré, on a $I_1I_2I_3 \subset S$. On peut donc écrire :

$$\alpha_i\beta_j\gamma_k = c_{ijk} + a_{ijk}\tau \tag{1}$$

où c_{ijk} et a_{ijk} sont des entiers $(1 \leq i, j, k \leq 2)$. On pose alors $A = (a_{ijk})$. Notons que A est juste la « matrice » de la forme trilinéaire $(x, y, z) \to \pi(xyz)$ dans les bases considérées des idéaux.

Si on change $(I_j)_j$ en un triplet équivalent (au sens de la définition précédente), on ne change pas le cube. De plus si on change de bases pour les idéaux avec un élément $g \in \Gamma$, alors on applique g au cube associé. Autrement dit notre application (qui à un triplet d'idéaux avec des bases associe un cube) commute à l'action de Γ. On dit qu'elle est équivariante. En fait si on étend cette application aux rationnels, elle est $GL_2(\mathbb{Q})^3$-équivariante.

La proposition 3 permet alors de ramener beaucoup de calculs au cas simple où $A = A_{id,D}$.

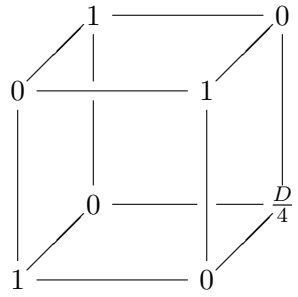
Le discriminant du cube est D car on a la relation suivante :

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

Pour la démontrer, commençons par prendre $I_1 = I_2 = I_3 = S$, $\alpha_1 = \beta_1 = \gamma_1 = 1$ et $\alpha_2 = \beta_2 = \gamma_2 = \tau$. On obtient alors le cube suivant, noté $A_{id,D}$

On a bien dans ce cas $\mathrm{Disc}(A) = \mathrm{Disc}(S) = D$.
Supposons maintenant que I_1 est quelconque. Soit $T \in GL_2(\mathbb{Q})$ la matrice de changement de base de (α_1, β_1) à $(1, \tau)$, le nouveau cube est alors obtenu par l'action de $(T \times id \times id)$ sur $A_{id,D}$ et Q_2 (et Q_3) est multipliée par $\mathrm{Det}(T) = N(I_1)$. De même pour I_2, I_3. Le discriminant du cube final est finalement multiplié par $N(I_1)^2N(I_2)^2N(I_3)^2$.

Réciproquement, soit $A = (a_{ijk})$ un cube (de discriminant D), nous allons montrer que (1) détermine uniquement (à équivalence près) les idéaux et leur base (i.e. on montre que notre application est injective).



On a les relations d'associativité suivantes :

$$\alpha_i\beta_j\gamma_k \times \alpha'_i\beta'_j\gamma'_k = \alpha'_i\beta_j\gamma_k \times \alpha_i\beta'_j\gamma'_k = \alpha_i\beta'_j\gamma_k \times \alpha'_i\beta_j\gamma'_k = \alpha_i\beta_j\gamma'_k \times \alpha'_i\beta'_j\gamma_k \tag{2}$$

En utilisant (1) et en identifiant les coefficients devant 1 et τ on obtient des équations liant les a_{ijk} aux c_{ijk}. Selon Bhargava, ce système auquel on ajoute la condition $N(I_1)N(I_2)N(I_3) > 0$ a une unique solution donnée par :

$$c_{ijk} = (i'-i)(j'-j)(k'-k) \times (a_{i'jk}a_{ij'k}a_{ijk'} + \frac{1}{2}a_{ijk}(a_{ijk}a_{i'j'k'} - a_{i'jk}a_{ij'k'} - a_{ij'k}a_{i'jk'} - a_{ijk'}a_{i'j'k})) \tag{3}$$

où $\{i,i'\},\{j,j'\},\{k,k'\} = \{1,2\}$.
En fait, ce n'est pas étonnant car il suffit de la vérifier pour $A = A_{id,D}$, puis par la proposition 3 et par trilinéarité, le résultat s'étend à tous les cubes.

Ce qui est plus surprenant, c'est que les c_{ijk} sont entiers. En effet, on vérifie que $a_{ijk}(a_{ijk}a_{i'j'k'} - a_{i'jk}a_{ij'k'} - a_{ij'k}a_{i'jk'} - a_{ijk'}a_{i'j'k}) \equiv 0 \bmod 2$ car $\mathrm{Disc}(A) \equiv 0 \mod 2$, et les c_{ijk} sont bien entiers.

On va montrer que (α_1,α_2), (β_1,β_2) et (γ_1,γ_3) sont déterminés à un facteur inversible près. Il suffit de le faire dans le cas $A = A_{id,D}$. En effet, par la proposition 3, on on peut trouver un couple $(M,N,P) \in GL_2(\mathbb{Q})^3$ tels que $\mathrm{Det}(M)\cdot\mathrm{Det}(N)\cdot\mathrm{Det}(P) = 1$ et $(M,N,P)\cdot A = A_{id,D}$. Les bases des idéaux I_1, I_2 et I_3 sont alors respectivement changées par M, N et P. Donc si on sait montrer que les bases sont déterminées dans le cas $A = A_{id,D}$, le résultat reste vrai en général.
Dans le cas $A = A_{id,D}$, les $\alpha_i\beta_j\gamma_k$ sont inversibles, or par (1), $\alpha_1\beta_j\gamma_k \times (c_{2jk} + a_{2jk}\tau) = \alpha_2\beta_j\gamma_k \times (c_{1jk} + a_{1jk}\tau)$ ce qui détermine le rapport $\frac{\alpha_1}{\alpha_2}$. À une constante κ_1 près, on a $\alpha_1 = c_{1jk} + a_{1jk}\tau$ et $\alpha_2 = c_{2jk} + a_{2jk}\tau$ ainsi que les relations analogues pour les β_j et γ_k. Notre application est bien injective.

Montrons maintenant la surjectivité. Soit A un cube de discriminant D. Par la proposition 3, il existe $g = (M,N,P) \in \Gamma'$ tel que $g\cdot A = A_{id,D}$. Il suffit alors de prendre pour bases de I_1, I_2 et I_3 les bases respectives $M^{-1}(1,\tau)$, $N^{-1}(1,\tau)$ et $P^{-1}(1,\tau)$. Alors A est bien associé à I_1, I_2 et I_3. Or on a vu que les c_{ijk} étaient alors déterminés et entiers. Donc $I_1I_2I_3 \subset S$.

Il nous reste pour finir à vérifier que les $\mathbb{Z}$-modules $I_1 = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$, I_2 et I_3 sont en fait des S-modules.

En utilisant (3), on vérifie que :

$$\tau\alpha_1 = \frac{q_1}{2}\alpha_1 + p_1\alpha_2$$
$$-\tau\alpha_2 = r_1\alpha_1 + \frac{q_1}{2}\alpha_2$$

où $Q_1^A = p_1x^2 + q_1xy + r_1y^2$.

En fait il suffit de vérifier cette formule dans le cas $A = A_{id,D}$ et de s'y ramener via des changements de bases.

Remarquons que $\mathrm{Disc}(A) = (N(I_1)N(I_2)N(I_3))^2\mathrm{Disc}(S)$, donc $(N(I_1)N(I_2)N(I_3))^2 = 1$. De plus, la solution (3) implique que $N(I_1)N(I_2)N(I_3) > 0$ et le triplet est bien équilibré.

□

Corollaire 3. *La bijection précédente induit une bijection entre les classes de triplets d'idéaux équilibré et les classes de cubes modulo* Γ.

Démonstration. Immédiat car la bijection est équivariante. □

Comme annoncé précédemment, ce corollaire n'est pas vrai si on n'impose pas $\kappa_1\kappa_2\kappa_3 = 1$ dans la définition 11 (pour simplifier, on dit que deux triplets sont équivalents au sens de Bhargava si on n'impose plus $\kappa_1\kappa_2\kappa_3 = 1$). En effet, deux triplets équilibrés équivalents sont équivalents au sens de Bhargava mais la réciproque est fausse. Prenons par exemple $S = \mathbb{Z}[7^3\sqrt{2}]$ et $(I_1, I_2, I_3) = (\mathbb{Z}[\sqrt{2}], \mathbb{Z}[7\sqrt{2}], 7^3(3+\sqrt{2})\mathbb{Z}[7\sqrt{2}])$. Alors $I_1I_2I_3 = 7^3(3+\sqrt{2})\mathbb{Z}[\sqrt{2}] \subset S$. De plus $N(I_1)N(I_2)N(I_3) = \frac{1}{7^3} \cdot \frac{1}{7^2} \cdot \frac{7^7}{7^2} = 1$ (la norme est prise par rapport à S). Le triplet (I_1, I_2, I_3) est donc équilibré. Soit $x = \frac{3-\sqrt{2}}{3+\sqrt{2}} = \frac{11-6\sqrt{2}}{7}$: $N(x) = 1$. Les deux triplets (xI_1, I_2, I_3) et (I_1, I_2, I_3) sont équivalents au sens de Bhargava. Mais s'ils étaient équivalent (à notre sens), il existerait κ_1, κ_2 et κ_3 tels que $\kappa_1\kappa_2\kappa_3 = 1$ et $xI_1 = \kappa_1 I_1$, $I_2 = \kappa_2 I_2$, $I_3 = \kappa_3 I_3$. Cela implique que $\kappa_2, \kappa_3 \in \mathbb{Z}[7\sqrt{2}]^\times \subset \mathbb{Z}[\sqrt{2}]^\times$ et que $\frac{x}{\kappa_1} = x\kappa_2\kappa_3 \in \mathbb{Z}[\sqrt{2}]^\times$. Donc $x \in \mathbb{Z}[\sqrt{2}]^\times$, ce qui n'est pas le cas car $x \notin \mathbb{Z}[\sqrt{2}]$.

Expliquons le lien entre les formes associées au cube et les idéaux.

Définition 13. *Soit S un anneau de rang k et I un idéal (orienté) non nul de S. On sait qu'il existe une $\mathbb{Z}$-base $(\alpha_1, ..., \alpha_n)$ (orientée) de I. On pose alors $q_I(x_1, ..., x_n) = \frac{N(\alpha_1 x_1 + ... + \alpha_n x_n)}{N(I)}$, où x_1, ..., $x_n \in \mathbb{Z}$. On dit que q_I est la forme norme associée à I (on sous-entend qu'on a choisi une base de I). Cette forme ne dépend pas de la classes d'équivalence de I, et changer de base (orientée) pour I revient à changer agir par $SL_n(\mathbb{Z})$ sur q_I.*

Proposition 9. *Avec les notations de la définition précédente, q_I est une forme quadratique à coefficients entiers.*

Démonstration. On sait que $N(I) = \epsilon(I)Card(S/I)$.
Si $x \in I$ alors $N(x) = \text{sign}(N(x))Card(S/(x))$. Or on a un morphisme de groupes surjectif $S/(x) \to S/I$, donc $N(x)$ divise $N(I)$. Donc q_I ne prend que des valeurs entières. En particulier les coefficients en x_i^2 sont entiers. Pour ce qui est du coefficient devant x_ix_j, il vaut $q_I(\alpha_i + \alpha_j) - q_I(\alpha_i) - q_I(\alpha_j)$ et est donc bien entier. □

Proposition 10. *Si A est un cube et (I_1, I_2, I_3) comme dans le théorème, alors Q_1^A est la forme norme associée à I_1 (et à sa base associée).*

Démonstration. C'est vrai dans le cas $A = A_{id,D}$ (par exemple si $D \equiv 0 \bmod 4$, $Q_i^A = x^2 - \frac{D}{4}y^2$). Dans le cas général, comme dans la preuve du théorème précédent, on peut envoyer les bases des trois idéaux sur $(1, \tau)$ par des éléments de $GL_2(\mathbb{Q})$, dont le déterminant est la norme de l'idéal correspondant. Par exemple, Q_1^A est multipliée par $N(I_2)N(I_3) = \frac{1}{N(I_1)}$, et donc correspond bien à la forme norme associée à la forme norme de $(I_1, (\alpha_1, \alpha_2))$.

Nous aurons en fait besoin d'expliciter les choses pour la proposition suivante, donc nous donnons une autre preuve calculatoire.

On note (α_1, α_2) la base associée à I_1. La forme norme de I_1 est $q_{I_1} = \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)}$. Soient x, y, z et t tels que $\alpha_1 = x + y\tau$ et $\alpha_2 = z + t\tau$. D'après la preuve du théorème, on a la structure de S-module de I_1 :

$$\tau\alpha_1 = \frac{q}{2}\alpha_1 + p\alpha_2$$

$$-\tau\alpha_2 = r\alpha_1 + \frac{q}{2}\alpha_2$$

où $Q_1^A = px^2 + rxy + qy^2$. En identifiant les coefficients devant 1 et τ, on trouve que $\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}$ appartient au noyau de

$$\begin{pmatrix} 1 & -\frac{q}{2} & 0 & -p \\ \frac{q}{2} & -\frac{D}{4} & p & 0 \\ 0 & r & 1 & \frac{q}{2} \\ r & 0 & \frac{q}{2} & \frac{D}{4} \end{pmatrix}$$

Après simplification, on obtient $x = \frac{q}{2}y + pt$ et $z = -ry - \frac{q}{2}t$, puis $N(\alpha_1 u + \alpha_2 v) = (pu^2 + quv + rv^2)(pt^2 + qyt + ry^2) = Q_1^A(u,v)N(I_1)$ où $N(I_1) = \begin{vmatrix} x & z \\ y & t \end{vmatrix} = xt - yz = pt^2 + qyt + ry^2 \neq 0$. □

Proposition 11. *Un cube est projectif si et seulement si le triplet associé est projectif.*

Démonstration. On suppose pour simplifier que D est pair. Soit I_1 le premier idéal. Montrons que I_1 est projectif (c'est à dire inversible, cf appendice pour la preuve de cette équivalence). On écrit à nouveau $\alpha_1 = x + y\tau$, $\alpha_2 = z + t\tau$, on note $\bar{I_1} = (\bar{\alpha_1} = x - y\tau, \bar{\alpha_2} = z - t\tau)$ et $Q(x,y) = px^2 + qxy + ry^2$ la première forme. On va montrer que $I_1\bar{I_1}$ est principal : sachant que $x = \frac{q}{2}y + pt$ et $z = -ry - \frac{q}{2}t$, on calcule :

$$\alpha_1\bar{\alpha_1} = pQ(t,y)$$
$$\alpha_2\bar{\alpha_2} = rQ(t,y)$$
$$\alpha_1\bar{\alpha_2} = -\frac{q}{2}Q(t,y) - Q(t,y)\tau$$
$$\alpha_2\bar{\alpha_1} = -\frac{q}{2}Q(t,y) + Q(t,y)\tau$$

Comme $pgcd(p,q,r) = 1$, on a bien $I_1\bar{I_1} = (Q(t,y))$, ce qui prouve que I_1 est inversible.

Réciproquement, supposons que la première forme $Q(x,y) = px^2 + qxy + ry^2$ n'est pas primitive. Posons $d = pgcd(p,q,r) > 1$ et supposons par l'absurde que l'idéal $I = I_1$ est projectif.
On a $I^2 = Q(t,y) \cdot (p, r, -\frac{q}{2} - \tau, -\frac{q}{2} + \tau >= Q(y,t) < d, -\frac{q}{2} + \tau, 2\tau)$. On va distinguer deux cas.

1) Si d divise $\frac{q}{2}$, alors $I^2 = Q(y,t) \cdot (d, \tau)$. On en déduit que $J = (d, \tau)$ est inversible, mais $J^2 = (d^2, d\tau, \frac{D}{4}) = dJ$ puisque d^2 divise $\frac{D}{4} = (\frac{q}{2})^2 - pr$, donc $J = (d)$, contradiction $(d > 1)$.

2) Sinon, d divise q mais d ne divise pas $\frac{q}{2}$. $J = (d, -\frac{q}{2} + \tau, 2\tau)$ est comme avant inversible. Or $J^2 = dJ$ (en utilisant le fait que d^2 divise D mais pas $\frac{D}{2}$), ce qui conduit de nouveau à une contradiction. □

Corollaire 4. *Soit $D \equiv 0, 1 \bmod 4$ tel que D n'est pas un carré parfait. Il y a une bijection entre les $SL_2(\mathbb{Z})$-classes de formes primitives de discriminant D et les classes d'idéaux (orientés) projectifs de $S = S(D)$.*

Ce résultat (dû à Gauss, cf [8]) est classique pour $D < 0$. Notons qu'on considère dans ce corollaire les formes définies positives ET définies négatives mais qu'on oriente les idéaux, ce qui donne le bon cardinal des deux cotés.

Comme pour le cas des cubes, on aurait pu énoncer un résultat plus fort dans lequel on ne passe pas aux classes déquivalences mais on considère les idéaux munis d'une base.

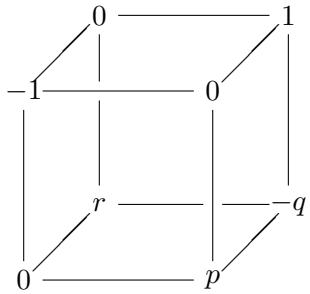
Démonstration. Soit I un idéal et (α, β) une base orientée. Soit q_I la forme norme associée à I (où la base orientée sous-entendue de I est (α, β)).

Si on change de base on ne change pas la classe de q_I et si on multiplie I par un scalaire on ne change pas q_I, notre application est bien définie de l'ensemble des classes d'idéaux vers les classes de formes.

Montrons la surjectivité. On aura besoin d'un petit lemme :

Lemme 1. *Si Q est une forme, il existe un cube A tel que $Q = Q_1^A$.*

Démonstration. On écrit $Q(x, y) = px^2 + qxy + ry^2$. On considère A ci-dessous :



et on vérifie que $Q = Q_1^A$. □

Soit donc Q une forme primitive de discriminant D. Soit A un cube tel que $Q = Q_1^A$ (lemme 1). Alors par la proposition 9, Q est une forme norme de I_1. De plus par la preuve de la proposition 9, I_1 est projectif.

Pour l'injectivité, soit I_1 un idéal projectif, on peut trouver un cube A dont I_1 est le premier idéal : il suffit de prendre I_2 tel que $I_1 I_2 = S$ et de prendre $I_3 = S$. Alors on a vu que la structure de S-module de I_1 était déterminée par les coefficients de « sa » forme norme. On conclut avec le résultat suivant :

Lemme 2. *Deux idéaux fractionnaires sont isomorphes en tant que S-module (orienté) si et seulement s'ils sont équivalents.*

Démonstration. On peut supposer $I \subset S$. Soit $\phi : I \to J$ un isomorphisme de S-module. Soient $x, y \in I$. On sait que $N(I) \in I$ (car dans S/I, $\overline{N(I)} = \overline{0}$). Alors $xN(I) \in I$ et $\phi(xN(I)) = x\phi(N(I)) = N(I)\phi(x)$, donc $\phi(x) = \frac{\phi(N(I))}{N(I)}x$. De plus $\frac{\phi(N(I))}{N(I)}$ est inversible car de même $\phi^{-1}(y) = \lambda \cdot y$, et $x = \lambda \cdot \frac{\phi(N(I))}{N(I)} \cdot x$, pour tout $x \in I$. En particulier pour $x = N(I)$, on a $\lambda \cdot \frac{\phi(N(I))}{N(I)} = 1$. □

□

Corollaire 5. *Soient Q_1 et Q_2 deux formes primitives. Alors il existe un cube A tel que $Q_1 = Q_1^A$ et $Q_2 = Q_2^A$.*

Démonstration. Découle du fait que deux idéaux projectifs se mettent sur un cube et du corollaire 2. □

Corollaire 6. *La bijection du théorème* 1 *induit une bijection entre $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$ et $Cl^+(D) \times Cl^+(D)$.*

On munit ainsi $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$ d'une structure de groupe dont l'élément neutre est $A_{id,D}$.

2.4. **Loi sur les formes.** On va maintenant munir les formes primitives de lois de groupe.

Théorème 3. *Soit $D \equiv 0, 1 \bmod 4$ et $Q_{id,D}$ une forme primitive telle qu'il existe un cube A_0 tel que $Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = Q_{id,D}$. Alors il existe une unique loi de groupe sur les $SL_2(\mathbb{Z})$ classes d'équivalence de formes primitives telle que :*
a) $[Q_{id,D}]$ est l'élément neutre (on note entre crochets les classes de formes).
b) Pour tout cube A de discriminant D, $[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{id,D}]$.

Démonstration. Soient Q_1 et Q_2 deux formes primitives. On a montré qu'il existait un unique cube A tel que $Q_1 = Q_1^A$ et $Q_2 = Q_2^A$. On note $Q_3 = Q_3^A$. On peut aussi trouver un unique cube A' tel que Q_3 et $Q_{id,D}$ soient sur A'. Soit $Q_3' = Q_3^{A'}$. Alors on pose : $[Q_1] + [Q_2] = [Q_3']$, ce qui ne dépend pas du choix de Q_1 et de Q_2 dans les classes associées.

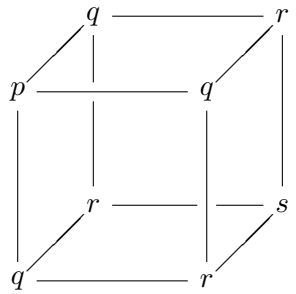
En fait en termes d'idéaux, cela correspond à $I_1 + I_2 = I_1 I_2 I_{id,D}^{-1}$. Le résultat découle de la condition $I_{id,D}^3 = 1$. □

En particulier la loi de composition de Gauss correspond au choix $A_0 = A_{id,D}$, i.e. à $Q_{id,D} = x^2 - \frac{D}{4}y^2$ ou $Q_{id,D} = x^2 - xy + \frac{1-D}{4}y^2$ et avec cette loi de groupe on a le résultat suivant.

Corollaire 7. *Les applications* $[A] \to [Q_i^A]$ *(*$i = 1, 2, 3$*) sont des morphismes de groupes.*

2.5. **Formes binaires cubiques et cubes triplement symétrique.** En imposant des symétries sur les cubes, on obtient des sous-groupes du groupe des cubes. En mettant ces sous-groupes en bijection avec certains ensembles de formes, Bhargava a découvert de nombreuses nouvelles lois de composition.

Un cube A est dit triplement symétrique s'il est de la forme suivante :



On note $Sym^3\mathbb{Z}^2$ l'ensemble des cubes triplement symétriques. Remarquons que pour un tel cube, $M_1 = M_2 = M_3 = \begin{pmatrix} p & q \\ q & r \end{pmatrix}$, $N_1 = N_2 = N_3 = \begin{pmatrix} q & r \\ r & s \end{pmatrix}$ et donc que les trois formes sont égales.

On associe à ce cube la forme binaire cubique $px^3 + 3qx^2y + 3rxy^2 + sy^3$. On fait agir de manière naturelle $SL_2(\mathbb{Z})$ sur cette forme, ce qui donne une action de $SL_2(\mathbb{Z})$ sur les cubes symétriques : si $\gamma \in SL_2(\mathbb{Z})$ agit sur $Sym^3\mathbb{Z}^2$, alors $({}^t\gamma, {}^t\gamma, {}^t\gamma)$ agit sur le cube correspondant.

Théorème 4. *La bijection du théorème 1 induit une bijection entre les cubes triplement symétriques et les classes d'équivalences de couples* $((I, (\alpha, \beta)), \delta)$ *où* $I^3 \subset \delta S$*,* $N(I)^3 = N(\delta)$ *et* (α, β) *est une base (orientée) de* I *(deux triplets sont dits équivalents ssi il existe* $\kappa \in (S \otimes \mathbb{Q})^\times$ *tel que* $((I', (\alpha', \beta')), \delta') = (\kappa \cdot I, (\kappa\alpha, \kappa\beta), \kappa^3\delta)$*).*

Démonstration. On doit essentiellement vérifier que dans la bijection du théorème 1, si les trois idéaux du triplet sont égaux à $(I, (\alpha, \beta))$ à un facteur près, alors le cube associé est triplement symétrique, et que réciproquement, si le cube est triplement symétrique, alors les 3 idéaux (et leur base) sont égaux à facteur près.

Si nos trois idéaux sont équivalents, ainsi que leur base, on peut écrire $\alpha_i\beta_j\gamma_k = \alpha_k\beta_i\gamma_j = \alpha_j\beta_k\gamma_i = \alpha_k\beta_j\gamma_i = \alpha_i\beta_k\gamma_j = \alpha_j\beta_i\gamma_k$. Donc on a les mêmes relations de permutations d'indices pour les a_{ijk}, ce qui signifie que $A = (a_{ijk})$ est triplement symétrique.

Réciproquement, si on a un cube triplement symétrique, les trois idéaux associés sont équivalents car les formes normes associées correspondent par la proposition 9 aux formes quadratiques du cube et sont égales. De plus les 3 bases des idéaux sont égales à facteur près. En effet, par la formule (3), les c_{ijk} sont aussi invariants par permutation d'indices. Donc de même pour les $\alpha_i\beta_j\gamma_k$, et par conséquent, $\frac{\alpha_1}{\beta_1} = \frac{\alpha_2}{\beta_2}$. De même pour les autres bases

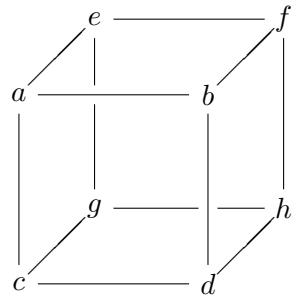
Pour conclure, on remarque juste qu'il y a une bijection entre les classes de couples $((I, (\alpha, \beta)), \delta)$ et les classes d'équivalences de triplets équilibrés de la forme $(\lambda_j \cdot I, (\lambda_j\alpha, \lambda_j\beta_j))_{j\in\{1,2,3\}}$ où I est un idéal de S via l'application $\phi : (\lambda_j I, (\lambda_j\alpha, \lambda_j\beta_j))_{j\in\{1,2,3\}} \to ((I, (\alpha, \beta)), (\lambda_1\lambda_2\lambda_3)^{-1})$ (l'application est bien définie car si on prend une autre écriture du triplet, I est remplacé par κI et $\delta = (\lambda_1\lambda_2\lambda_3)^{-1}$ est remplacé par $\kappa^3\delta$).

□

Corollaire 8. *La bijection précédente induit une bijection entre les classes d'équivalence de couples (I, δ) et les $SL_2(\mathbb{Z})$-orbites de formes binaires cubiques. Sous cette bijection, les idéaux projectifs correspondent aux classes de cubes triplement symétriques projectifs, noté $Cl(Sym^3\mathbb{Z}^2, D)$. On munit $Cl(Sym^3\mathbb{Z}^2, D)$ d'une structure de groupe évidente.*

Corollaire 9. *Il y a un morphisme surjectif $\phi : Cl(Sym^3\mathbb{Z}^2, D) \to Cl_3(S(D))$ (on note $Cl_3(S(D))$ le groupe des classes d'idéaux d'ordre 3 de $S(D)$) qui envoie une forme binaire cubique C vers la classe de l'idéal I associé. De plus le noyau de ce morphisme est de cardinal $Card(U/U^3)$ où U est le groupe des unités de S.*

2.6. **Couple de formes bilinéaires alternées sur $\mathbb{Z}^4$.** On considère l'injection de $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ vers $\mathbb{Z}^2 \otimes \wedge\mathbb{Z}^4$:



$$\to \quad \left(\begin{pmatrix} & & a & b \\ & & c & d \\ -a & -c & & \\ -b & -d & & \end{pmatrix}, \begin{pmatrix} & & e & f \\ & & g & h \\ -e & -g & & \\ -f & -h & & \end{pmatrix} \right)$$

Soit $\Gamma' = SL_2(\mathbb{Z}) \times SL_4(\mathbb{Z})$. Le groupe Γ' agit de manière naturelle sur $\mathbb{Z}^2 \otimes \wedge\mathbb{Z}^4$. On vérifie que Γ se plonge dans Γ' via : $(C, A, B) \longrightarrow (C, \begin{pmatrix} A & \\ & B \end{pmatrix})$ et que ces actions commutent avec l'injection précédente, i.e. que l'injection induit une application au niveau des classes d'équivalences.
On dit q'un élément $F \in \mathbb{Z}^2 \otimes \wedge\mathbb{Z}^4$ est projectif s'il est Γ'-équivalent à l'image d'un cube projectif.
A un $F = (M, N) \in \mathbb{Z}^2 \otimes \wedge\mathbb{Z}^4$, on peut associer une forme quadratique

$$Q^F(x, y) = -\text{Pfaff}(Mx - Ny) = -\sqrt{\text{Det}(Mx - Ny)}$$

où on a choisit le signe du Pfaffien tel que $\text{Pfaff}(\begin{pmatrix} & I \\ -I & \end{pmatrix}) = 1$.
On vérifie enfin que $\text{Disc}(F) := \text{Disc}(Q^F)$ est invariant par l'action de Γ' et que si F provient d'un cube A, alors $\text{Disc}(F) = \text{Disc}(A)$.

Nous allons donner une interprétation de ces formes avec des modules.

Définition 14. *Un idéal de rang n de S est un S-module inclus dans K^n (où comme d'habitude $K := S \otimes \mathbb{Q}$ est la $\mathbb{Q}$-algèbre associée à S) et de rang $2n$ en tant que $\mathbb{Z}$-module.*

On définit de même une orientation pour les idéaux de rang n :

Définition 15. *Une $\mathbb{Z}$-base $(\alpha_1, \beta_1, ..., \alpha_n, \beta_n)$ d'un idéal de rang n (M, ϵ) (avec $\epsilon = \pm 1$) est dite positive si le signe du déterminant de cette base dans la base $((1, 0, ..., 0), (\tau, 0, ..., 0), ..., (0, ..., 1), (0, ..., \tau))$ est celui de ϵ.*

Définition 16. *La norme de (M, ϵ) est $\epsilon \times Card(L/M) \times Card(L/S)^{-1}$ où L est un réseau de K^n contenant S^n et M.*

Le déterminant de M, noté $\text{Det}(M)$, est l'idéal engendré par les éléments de la forme $\text{Det}(x_1, ..., x_n)$ où x_1, ..., $x_n \in M$.

On dit que $(M_1, ..., M_k)$ (de rangs n_1, ..., n_k) est équilibré si $\text{Det}(M_1)...\text{Det}(M_k) \subset S$ et $N(M_1)...N(M_k) = 1$. On dit que $(M_1, ..., M_k)$ et $(N_1, ..., N_k)$ (deux k-tuples équilibrés) sont équivalents s'il existe λ_1, ..., λ_k dans $GL_{n_1}(K)$, ..., $GL_{n_k}(K)$ tels que $\text{Det}(\lambda_1)...\text{Det}(\lambda_k) = 1$.

Théorème 5. *Il y a une bijection entre les classes de couples* $((I,(\alpha_1,\alpha_2)),(M,(\beta_1,\beta_2,\beta_3,\beta_4)))$ *et les éléments de discriminant* D *de* $\mathbb{Z}^2\otimes\wedge\mathbb{Z}^4$.

Démonstration. La structure de la preuve est identique à celle du théorème 1, en écrivant les équations suivantes :

$$\alpha_i \mathrm{Det}(\beta_j,\beta_k) = c_{jk}^{(i)} + a_{jk}^{(i)}\tau$$

□

Cette bijection induit une bijection au niveau des classes d'équivalence.

Bhargava remarque que l'injection $\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2 \to \mathbb{Z}^2\otimes\wedge\mathbb{Z}^4$ correspond à l'application $(S,(I_1,I_2,I_3)) \to (S,(I_1,I_2\oplus I_3))$.

De plus, elle induit une bijection entre les classes de couples $(S,(I,M))$ où I et M sont des S-modules projectifs et $Cl(\mathbb{Z}^2\otimes\wedge\mathbb{Z}^4,D)$ (l'ensemble des classes projectives). Cela munit $Cl(\mathbb{Z}^2\otimes\wedge\mathbb{Z}^4,D)$ d'une structure de groupe. En fait, un théorème d'annulation de Serre (cf [11]) affirme qu'un module M projectif de rang k sur un anneau S de dimension de Krull 1 est déterminé par son déterminant $\mathrm{Det}(M)$. Dans le cas projectif, $\mathrm{Det}(M) = I^{-1}$, et $M = S\oplus I^{-1}$. Par conséquent, on a un isomorphisme de groupe $Cl(\mathbb{Z}^2\otimes\wedge\mathbb{Z}^4,D) \to Cl((Sym^2\mathbb{Z}^2)^*,D)$ (on envoie (I,M) sur I). Cette bijection peut se réécrire en termes de formes quadratiques : on envoie la forme Q^F sur la classe d'une forme norme de I.

3. Paramétrisation des anneaux cubiques

On rappelle qu'un anneau cubique est un anneau (orienté) isomorphe (en tant que groupe additif) à $\mathbb{Z}^3$.

Définition 17. *Une forme binaire cubique à coefficients entiers est de la forme* $f(x,y) = ax^3+bx^2y+cxy^2+dy^3$ *où* a, b, c *et* d *sont des entiers. On agit par* $GL_2(\mathbb{Z})$ *sur les formes cubiques par* $\gamma\cdot f(x,y) = \mathrm{Det}(\gamma)^{-1}f(\gamma^t\cdot(x,y))$.

Théorème 6. *Paramétrisation des anneaux cubiques de Delone et Faddeev (*[6]*)*
Il y a une bijection entre les anneaux cubiques (à isomorphisme près) et les $GL_2(\mathbb{Z})$*-classes de formes binaires cubiques* $f(x,y) = ax^3+bx^2y+cxy^2+dy^3$ *où* a, b, c, $d\in\mathbb{Z}$. *On note* $R(f)$ *l'anneau associé à* f *par cette bijection. De plus* $\mathrm{Disc}(R(f)) = \mathrm{Disc}(f)$.

Démonstration. Soit R un anneau cubique. On prend une $\mathbb{Z}$-base $(1,\omega,\theta)$ de R (c'est possible comme dans le cas quadratique). Quitte à translater ω et θ par des entiers on peut supposer $\omega\theta\in\mathbb{Z}$. On dit que $(1,\omega,\theta)$ est une base normale de R. On obtient la table de multiplication suivante :

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

Choisir une autre base $(1,\omega',\theta')$ revient à multiplier, dans $R/\mathbb{Z}$, $(\overline{\omega},\overline{\theta})$ par une matrice de $GL_2(\mathbb{Z})$. On associe à R la forme $f: R/\mathbb{Z}\to\mathbb{Z}$ telle que $f(\xi) = 1\wedge\xi\wedge\xi^2$ (on vérifie que ça ne dépend que de la classe de ξ modulo $\mathbb{Z}$). Explicitement, si $\xi = x\omega+y\theta$, $f(\xi) = (1\wedge\theta\wedge\omega)(ax^3+bx^2y+cxy^2+dy^3)$.
Notre application est donc bien définie au niveau des classes d'équivalence (remarquer que l'importance du facteur $\mathrm{Det}(\gamma)$ dans la définition précédente). Réciproquement, étant donnée une classe $f = ax^3+bx^2y+cxy^2+dy^3$, on associe $R(f)$ ayant la table de multiplication suivante :

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

On vérifie que $\omega\theta\times\theta = \omega\times\theta^2$ et que $\omega^2\times\theta = \omega\times\omega\theta$. Cela entraine que la loi de multiplication est bien associative. Si on avait choisit un autre représentant que f, on n'aurait pas changé R.

Le calcul du discriminant est immédiat. □

3.1. **Analogue des cubes dans le cas cubique.** On va maintenant donner des bijections entre orbites intégrales de certains espaces et des ensembles liés au groupe de classe d'anneaux cubiques.

On considère l'action de $\Gamma = GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$ sur $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$. On représente les éléments de $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ par des couples (A, B) de matrices 3×3. On associe la forme $f(x, y) = \mathrm{Det}(Ax - By)$, dont la $GL_2(\mathbb{Z})$ classe d'équivalence est invariante sous l'action de Γ. En particulier, $\mathrm{Disc}(f)$ est invariant de l'action de Γ. On le note $\mathrm{Disc}(A, B)$.

Définition 18. *On dit que* $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ *est non dégénéré si* $\mathrm{Disc}(A, B) \neq 0$.

Pour simplifier les calculs, comme dans le cas quadratique on va étudier les orbites sur $\mathbb{Q}$. Plus précisément, soit $G = \{(M, N) \in GL_3(\mathbb{Q}) \times GL_3(\mathbb{Q}),\ \mathrm{Det}(M) \cdot \mathrm{Det}(N) = 1\}$. Le groupe G agit naturellement sur $V_{\mathbb{Q}} := \mathbb{Q}^2 \otimes_{\mathbb{Q}} \mathbb{Q}^3 \otimes_{\mathbb{Q}} \mathbb{Q}^3$ par $(M, N) \cdot (A, B) = (M \cdot A \cdot {}^tN, M \cdot N \cdot {}^tP)$. La forme $f(x, y) = \mathrm{Det}(Ax - By)$ associée est invariante sous l'action de G. On définit alors de même le discriminant de (A, B).

Proposition 12. *Soit* $(A, B) \in V_{\mathbb{Q}}$ *non dégénéré et* $f(x, y) = \mathrm{Det}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$ *sa forme associée. Alors tous les éléments de* $V_{\mathbb{Q}}$ *au dessus de* f *sont dans la même orbite sous* G.

Démonstration. On rappelle que la droite projective $\mathbb{P}^1(\mathbb{Q})$ est l'ensemble des droites vectorielles de $\mathbb{Q}^2$. Le fait que $f \neq 0$ implique qu'il y a un nombre fini de points $(\lambda, \mu) \in \mathbb{P}^1(\mathbb{Q})$ tels que $f(\lambda, \mu) = 0$ (observer que comme f est homogène, cela ne dépend pas du représentant choisi). Donc il y a un nombre fini de $(\lambda, \mu) \in \mathbb{P}^1(\mathbb{Q})$ tels que $\mathrm{Ker}(\lambda A + \mu B) \neq \{0\}$. Comme $\mathrm{Disc}(A, B) \neq 0$, $\lambda A + \mu B$ n'est jamais nul, donc il existe un nombre fini de droites $\mathbb{Q} \cdot X$ telles que (AX, BX) est liée, et en particulier il existe un X tel que (AX, BX) est libre.

On peut alors trouver X, $Y \in \mathbb{Q}^3$ tels que les familles (AX, BX, Y) et $({}^tAY, {}^tBY, X)$ sont libres. En effet, $\mathrm{Det}(AX, BX, Y)$ et $\mathrm{Det}({}^tAY, {}^tBY, X)$ sont des polynômes non nuls en les coordonnées de X et Y, car les fonctions polynomiales associées ne sont pas identiquement nuls par ce qui précède. Donc le polynôme $\mathrm{Det}(AX, BX, Y) \times \mathrm{Det}({}^tAY, {}^tBY, X)$ est non nul, et comme $\mathbb{Q}^6$ est infini, la fonction polynomiale associée est non nulle, d'où l'existence de X et Y tels que (AX, BX, Y) et $({}^tAY, {}^tBY, X)$ sont libres.

Quitte à faire deux changements de bases via un élément de G, on peut supposer $X = Y = (1, 0, 0)$, $AX = (0, 0, \lambda)$ $(\lambda \neq 0)$, ${}^tAY = (0, 0, 1)$, $BX = (0, 1, 0)$ et ${}^tBY = (0, 1, 0)$. Autrement dit, on peut supposer que

$$(A, B) = \left(\begin{pmatrix} 0 & 0 & \lambda \\ 0 & * & * \\ 1 & * & * \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & * & * \\ 0 & * & * \end{pmatrix} \right)$$

On multiplie ensuite la première ligne de A et B par $\frac{1}{\lambda}$, et la deuxième colonne par λ : c'est une opération avec un élément de G. On arrive alors à

$$(A, B) = \left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & * & * \\ 1 & * & * \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & * & * \\ 0 & * & * \end{pmatrix} \right)$$

On peut ensuite faire des opérations élémentaires sur (A, B) pour arriver à

$$(A, B) = \left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & s & 0 \\ 1 & 0 & t \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & u & 0 \\ 0 & 0 & v \end{pmatrix} \right)$$

On calcule explicitement $\mathrm{Det}(Ax-By) = -sx^3+ux^2y-txy^2+vy^3 = ax^3+bx^2y+cxy^2+dy^3$, donc

$$(A,B) = \left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & -a & 0 \\ 1 & 0 & -c \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & b & 0 \\ 0 & 0 & d \end{pmatrix} \right)$$

□

3.2. **Classes d'idéaux des anneaux cubiques et Γ-orbites.** On rappelle quelques définitions. On pose $K := R \otimes \mathbb{Q}$ qui est une $\mathbb{Q}$-algèbre.

Définition 19. *On dit qu'un couple d'idéaux fractionnaires (I, I') (orientés) est équilibré si $II' \subset R$ et $N(I)N(I') = 1$. On dit que (I_1, I_1') est équivalent à (I_2, I_2') si $\exists \kappa \in K^\times$ tel que $I_1' = \kappa I_1$ et $I_2' = \kappa^{-1} I_2$.*

Théorème 7. *Il y a une bijection entre les Γ-orbites non dégénérées de $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ et les classes de couples $(R, (I, I'))$ où R est un anneau cubique non dégénéré et (I, I') est une classe de couple d'idéaux équilibré de R.*

Démonstration. Soit R un anneau cubique non dégénéré et (I, I') un couple équilibré. On se fixe une base $(1, \omega, \theta)$ de R avec $\omega\theta \in \mathbb{Z}$. Soit $(\alpha_1, \alpha_2, \alpha_3)$, $(\beta_1, \beta_2, \beta_3)$ des bases de I et I' de même orientation que $(1, \omega, \theta)$. Comme $II' \subset R$, on peut écrire

$$(*) \alpha_i\beta_j = c_{ij} + b_{ij}\omega + a_{ij}\theta$$

On obtient alors deux matrices $A = (a_{ij})$ et $B = (b_{ij})$, et donc un élément (A, B) de $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$.

Si on change $(1, \omega, \theta)$ en $(1, \omega', \theta')$, on peut écrire :

$$\begin{cases} \omega' = q + r\omega + s\theta \\ \theta' = t + u\omega + v\theta \end{cases}$$

avec $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in GL_2(\mathbb{Z})$. Le couple (A, B) est alors changé par le même élément de $GL_2(\mathbb{Z})$. Changer les bases de I et I' revient de la même manière à agir sur le couple (A, B) par des matrices de $SL_3(\mathbb{Z})$. Il est aussi simple de vérifier que (A, B) ne dépend pas du représentant (I, I') puisque qu'on peut prendre des bases $(\kappa\alpha_1, \kappa\alpha_2, \kappa\alpha_3)$, $(\kappa^{-1}\beta_1, \kappa^{-1}\beta_2, \kappa^{-1}\beta_3)$.
On obtient donc une application bien définie au niveau des classes d'équivalence.

Remarquons d'abord que $(*)$ et le système

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

impliquent $\mathrm{Det}(Ax - By) = N(I)N(I')(ax^3 + bx^2y + cxy^2 + dy^3)$. En effet, on commence par le cas $I = I' = R$ avec les même bases $(1, \omega, \theta)$. On obtient :

$$(A,B) = \left(\begin{bmatrix} & & 1 \\ & -a & \\ 1 & & -c \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & b & \\ & & d \end{bmatrix} \right)$$

auquel cas l'identité est vérifiée. Supposons à présent que les bases de I et I' sont transformées par des applications T, $T' \in GL_3(\mathbb{Q})$. Alors $\mathrm{Det}(Ax - By)$ est multiplié par $\mathrm{Det}(T)\mathrm{Det}(T') = N(I)N(I')$, ce qui prouve le résultat dans le cas général. Or $N(I)N(I') = 1$, donc (3)$\mathrm{Det}(Ax - By) = f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ et A et B déterminent l'anneau $R = R(f)$.

Prouvons que les c_{ij} sont uniquement déterminés pas les a_{ij}, les b_{ij} et les équations d'associativité et de commutativité $(\alpha_i\beta_j)(\alpha_{i'}\beta_{j'}) = (\alpha_i\beta_{j'})(\alpha_{i'}\beta_j)$ et en les développant en utilisant $(*)$, $(**)$ et (3), on obtient un système d'équations en les c_{ij} qui, selon Bhargava, a une et une seule solution :

$$(4)c_{ij} = \sum_{i'<i'',j'<j} \begin{pmatrix} i & i' & i'' \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} j & j' & j'' \\ 1 & 2 & 3 \end{pmatrix} \begin{vmatrix} a_{ij} & a_{ij'} \\ a_{i'j} & a_{i'j'} \end{vmatrix} \begin{vmatrix} b_{ij} & b_{ij''} \\ b_{i''j} & b_{i''j''} \end{vmatrix}$$

où $\begin{pmatrix} i & j & k \\ 1 & 2 & 3 \end{pmatrix}$ désigne la signature de la permutation (i,j,k) de $(1,2,3)$.
En fait ce n'est pas surprenant car il suffit de vérifier cette formule pour

$$(A,B) = \left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & -a & 0 \\ 1 & 0 & -c \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & b & 0 \\ 0 & 0 & d \end{pmatrix} \right)$$

et on s'y ramène par la proposition 12. Ce qui est plus surprenant, c'est que cette solution soit entière !

Montrons l'injectivité de notre application. Quitte à faire un changement de base, on peut supposer que $(\alpha_1,\alpha_2,\alpha_3) = (\beta_1,\beta_2,\beta_3) = (1,\omega,\theta)$. Alors les α_i et β_j sont inversibles dans K. Le système $(*)$ impose les coordonnées homogène de $(\alpha_1,\alpha_2,\alpha_3)$, on a

$$\alpha_1 : \alpha_2 : \alpha_3 = c_{1j} + b_{1j}\omega + a_{1j}\theta : c_{2j} + b_{2j}\omega + a_{2j}\theta : c_{3j} + b_{3j}\omega + a_{3j}\theta$$

Donc à scalaire près, I est déterminé. De plus le choix d'une base $(\alpha_1,\alpha_2,\alpha_3)$ de I détermine uniquement le choix d'une base $(\beta_1,\beta_2,\beta_3)$. Le choix de (I,I') est donc unique à équivalence près.

Pour montrer la surjectivité, on se donne (A,B). Il existe un élément de G qui envoie (A,B) sur

$$\left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & -a & 0 \\ 1 & 0 & -c \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & b & 0 \\ 0 & 0 & d \end{pmatrix} \right)$$

(proposition 12). Dans ce cas, on a vu qu'on pouvait prendre $(\alpha'_1,\alpha'_2,\alpha'_3) = (\beta'_1,\beta'_2,\beta'_3) = (1,\omega,\theta)$. Il suffit alors de tirer en arrière ces bases par le même élément de G pour obtenir (A,B).
On pose $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$ et $I' = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \mathbb{Z}\beta_3$. Il reste à voir que I et I' sont des R-modules. Bhargava remarque qu'on a la structure de R-module suivante (où $|CC'C''|$ désigne le déterminant de la matrice dont les 3 colonnes sont C, C' et C'') :

$$\begin{aligned}
-\omega\alpha_1 &= |B_1A_2A_3|\alpha_1 + |A_1B_1A_3|\alpha_2 + |A_1A_2B_1|\alpha_3 \\
-\omega\alpha_2 &= |B_2A_2A_3|\alpha_1 + |A_1B_2A_3|\alpha_2 + |A_1A_2B_2|\alpha_3 \\
-\omega\alpha_3 &= |B_3A_2A_3|\alpha_1 + |A_1B_3A_3|\alpha_2 + |A_1A_2B_3|\alpha_3 \\
-\theta\alpha_1 &= |A_1B_2B_3|\alpha_1 + |B_1A_1B_3|\alpha_2 + |B_1B_2A_1|\alpha_3 \\
-\theta\alpha_2 &= |A_2B_2B_3|\alpha_1 + |B_1A_2B_3|\alpha_2 + |B_1B_2A_2|\alpha_3 \\
-\theta\alpha_3 &= |A_3B_2B_3|\alpha_1 + |B_1A_3B_3|\alpha_2 + |B_1B_2A_3|\alpha_3
\end{aligned}$$

De même on a la structure de R-module de I' avec des lignes au lieu des colonnes. A nouveau, ces formules se vérifient dans le cas particulier où les bases sont égales à $(1,\omega,\theta)$ et s'en déduisent dans le cas général par linéarité. □

Corollaire 10. *Le stabilisateur d'un élément non dégénéré $(A,B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ est égal à un produit semi-direct $Aut(R) \rtimes U^+(R_0)$ où $(R,(I,I'))$ correspond à (A,B), $R_0 = End_R(I) \cap End_R(I')$ et $U^+(R_0)$ est le groupe des unités de R_0 de norme positive.*

Démonstration. Premièrement, si un élément de $g = (\gamma_1,\gamma_2,\gamma_3) \in GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z}) \subset \Gamma$ stabilise (A,B) alors la base $(1,\omega,\theta)$ de la preuve du théorème précédent est envoyée sur une base $(1,\omega',\theta')$ ayant la même table de multiplication (cf $(**)$), c'est à dire que $\gamma_1 \in Aut(R)$. Ensuite, on a montré que les bases $(\alpha_1,\alpha_2,\alpha_3)$ et $(\beta_1,\beta_2,\beta_3)$ de I et I' sont déterminées à scalaire près. Donc γ_2 agit par multiplication par κ et γ_3 par multiplication par κ^{-1} pour un certain $\kappa \in K^\times$. Donc $N(\kappa) = \mathrm{Det}(\gamma_1) = 1$ et $\gamma_1 = \gamma_2^{-1} \in R_0$. □

Dans le cas projectif, on peut expliciter ce stabilisateur.

Proposition 13. *Soit I un idéal projectif de R. Alors $End_R(I) = R$.*

Démonstration. On sait que $J = End_R(I) = \{x \in K, xI \subset I\}$ est un idéal (fractionnaire) de S. Clairement, $R \subset J$. Réciproquement, $JI \subset I$ donc en multipliant des deux côtés par I^{-1} (avec $II^{-1} = R$), on a $J \subset R$. □

Le stabilisateur précédent est donc $Aut(R) \rtimes U^+(R)$ ce qui est analogue au cas des formes quadratiques binaires où le stabilisateur est $U^+(R)$.

3.3. **Ajout de conditions de symétrie.** Comme dans le cas quadratique on peut s'intéresser à l'espace $\mathbb{Z}^2 \otimes Sym^2\mathbb{Z}^3$ qui correspond aux couples (A, B) de matrices symétriques ou en termes d'idéaux aux deux mêmes classes d'idéaux.

On a les résultats suivants.

Théorème 8. *Il y a une bijection canonique entre les orbites non dégénérées de l'action naturelle de $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ sur $\mathbb{Z}^2 \otimes Sym^2\mathbb{Z}^3$ et les classes d'équivalence de triplets (R, I, δ) où $I^2 \subset (\delta)$ et $N(\delta) = N(I)^2$ (deux tels triplets sont équivalents s'il existe un isomorphisme d'anneaux $\phi : R \to R'$ et $\kappa \in (R' \otimes \mathbb{Q})^\times$ tels que $I' = \kappa\phi(I)$ et $\delta' = \kappa^2\phi(\delta)$).*

De plus cette bijection préserve le discriminant

On peut aussi, comme dans le cas quadratique, considérer la flèche naturelle $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \to \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$. Explicitement,

$$(A, B) \to \left(\begin{bmatrix} & A \\ -A^t & \end{bmatrix}, \begin{bmatrix} & B \\ -B^t & \end{bmatrix} \right)$$

On a une action naturelle de $\Gamma' = GL_2(\mathbb{Z}) \times SL_6(\mathbb{Z})$ sur $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$. De plus, on peut plonger Γ dans Γ' de telle manière que l'action de Γ commute avec notre flèche. Concrètement, ce plongement est donné par : $(\gamma_1, \gamma_2, \gamma_3) \to \left(\gamma_1, \begin{bmatrix} \gamma_2 & \\ & \gamma_3 \end{bmatrix} \right)$.

On associe à un élément $(U, V) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ une forme binaire cubique $f(x, y) =$Pfaff$(Ux - Vy)$, qui est invariante sous l'action de Γ'. On pose alors $\mathrm{Disc}(U, V) = \mathrm{Disc}(f)$.

Proposition 14. *La flèche $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \to \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ préserve le discriminant.*

Démonstration. $\mathrm{Det}(Ux - Vy) = \mathrm{Det}(Ax - By)^2$ donc $\mathrm{Pfaff}(Ux - vY) = \mathrm{Det}(Ax - By)$ et $\mathrm{Disc}(U, V) = \mathrm{Disc}(A, B)$. □

On rappelle la définition suivante (où $K = R \otimes \mathbb{Q}$) :

Définition 20. *Un R-module libre de rang 2 $M \subset K^2$ est dit équilibré si $Det(M) \subset R$ et $N(M) = 1$. On dit que deux modules équilibrés M et N sont équivalents s'ils sont isomorphes en tant que R-modules (ou de manière équivalente s'il existe un élément de $SL_2(K)$ envoyant M sur N).*

Théorème 9. *Il y a une bijection canonique entre les orbites non dégénérées de l'action de Γ' sur $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ et l'ensembles des classes d'équivalence de couples (R, M) où R est un anneau cubique non dégénéré et M est une classe de module de rang 2 équilibré. Cette bijection préserve le discriminant.*

On omet la preuve qui, dans sa structure est similaire à celle du théorème 2. Cf [2].

Corollaire 11. *Le stabilisateur d'un élément non dégénéré $(U, V) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ est un produit semi-direct $Aut(R) \rtimes End_R(M)$ où (R, M) est donnée par le théorème précédent.*

On peut remarquer que $End_R(M)$ est juste l'ensemble des matrices de $SL_2(K)$ envoyant M sur M.

3.4. **Lois de compositions associées.** Nous allons maintenant décrire un analogue cubique de la loi de composition de Gauss. Comme dans le cas quadratique, il y a une notion de primitivité pour les éléments de nos espaces, et on munit ces espaces projectifs d'une structure de groupe liée au groupe de classe.

Définition 21. *On dit q'un élément* (A, B) *de* $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ *est projectif si les idéaux* I *et* I' *lui correspondant sont projectifs.*

Définition 22. *On définit* $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$ *comme l'ensemble des* $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ *tels que* $\mathrm{Disc}(Ax - By) = f(x, y)$ *où* f *est une forme binaire cubique.*

On note $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3, f)$ *l'ensemble des classes* (A, B) *projectives de* $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$.

On a une structure de groupe évidente sur $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3, f)$: si (A_1, B_1) et (A_2, B_2) correspondent respectivement à (I_1, I_1') et (I_2, I_2'), on définit $(A_1, B_1) \times (A_2, B_2)$ comme la classe d'un élément associé à $(I_1 I_2, I_1' I_2')$.

Théorème 10. *Il y a un isomorphisme de groupes entre* $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3, f)$ *et le groupe de classes de* $R(f)$ *(noté* $Cl(R(f))$*).*

On définit de même $Cl(\mathbb{Z}^2 \otimes Sym^2(\mathbb{Z}^3), f)$ en passant par les idéaux. On a une loi de groupe évidente sur cet ensemble (on multiplie les idéaux et les δ composante par composante).

Théorème 11. *Il y a un morphisme de groupe surjectif naturel* $Cl(\mathbb{Z}^2 \otimes Sym^2(\mathbb{Z}^3), f) \to Cl_2(R(f))$ *où* $Cl_2(R(f))$ *est l'ensemble des classes d'idéaux d'ordre divisant* 2*. Le noyau est isomorphe à* $U_R/\{U_R^2, \pm 1\}$ *où* U_R *est le groupe des unités de* R*.*

Démonstration. On associe à $(R(f), I, \delta)$ l'idéal I qui est bien d'ordre 2 car $N(I^2) = N(I)^2 = N(\delta)$ et $I^2 \subset \delta$, ce qui implique $I^2 = \delta$. Le calcul du noyau est automatique. □

4. Paramétrisation des anneaux quartiques

On a vu que les anneaux quadratiques et cubiques étaient paramétrisés respectivement par le discriminant et les classes d'équivalence de formes binaires cubiques à coefficients entiers. Nous allons maintenant nous intéresser au cas des anneaux quartiques.

Définition 23. *Soit* R *un anneau de rank* k *et* $\alpha \in R$*. On définit* $\mathrm{Disc}(\alpha)$ *comme le discriminant de son polynôme caractéristique.*

On souhaite définir un analogue de la clôture galoisienne pour les anneaux. On se donne un anneau R de rang k. On note I_R l'idéal de $R^{\otimes k}$ engendré par les éléments de la forme $(x \otimes 1 \otimes ... \otimes 1) + (1 \otimes x \otimes 1 \otimes ... \otimes 1) + ... + (1 \otimes 1 \otimes ... \otimes x) - Tr(x)$.

Définition 24. *La* S_k*-clôture d'un anneau* R *de rang* k *est* $\overline{R} := R^{\otimes k}/J_R$ *où* $J_R = \{r \in R^{\otimes k}, \exists n \in \mathbb{Z}^* : nr \in I_R\}$

Le fait d'avoir quotienté par J_R permet d'avoir une injection naturelle $\overline{R} \hookrightarrow \overline{R} \otimes \mathbb{Q}$.

Proposition 15. *Si* $F_\alpha(x) = x^k - a_1 x^{k-1} + ... \pm a_k$ *est le polynôme caractéristique de* $\alpha \in R$*, alors la* i*-ième fonction symétrique élémentaire en les* k *éléments* $\alpha \otimes 1 \otimes ... \otimes 1$*,* $1 \otimes \alpha \otimes 1 \otimes ... \otimes 1$*, ...,* $1 \otimes 1 \otimes ... \otimes \alpha$ *est congrue à* a_i *modulo* J_R*.*

Démonstration. Soit $s_i = (\alpha \otimes 1 \otimes ... \otimes 1)^i + (1 \otimes \alpha \otimes 1 \otimes ... \otimes 1)^i + ... + (1 \otimes 1 \otimes ... \otimes \alpha)^i$ la i-ième somme de newton. Soit σ_i la i-ième fonction symétrique élémentaire. On sait qu'il existe $n_i \in \mathbb{Z}$ tel que $n_i \sigma_i = P_i(s_1, ..., s_k)$ où P_i est un polynôme dans $\mathbb{Z}[X_1, ..., X_k]$ (qui est universel). On sait que $s_j \equiv Tr(\alpha^j)$ mod I_R. Donc $n_i \sigma_i \equiv P_i(Tr(\alpha), ..., Tr(\alpha^k))$ mod I_R. Soit $A = m_\alpha$ la matrice de multiplication par α dans une $\mathbb{Z}$-base de R. Alors $A \in M_k(\mathbb{Z})$. Notons que F_α est le polynôme caractéristique de A. Mais alors on a l'identité $n_i a_i = P_i(Tr(A), ..., Tr(A^k))$ car on peut se placer dans $\mathbb{C}$ et trigonaliser. D'où $n_i \sigma_i \equiv n_i a_i$ mod I_R et donc $\sigma_i \equiv a_i$ mod J_R. □

Définition 25. *Les conjugués d'un éléments $x \in R$ sont par définition $x \otimes 1 \otimes ... \otimes 1$, $1 \otimes x \otimes 1 \otimes ... \otimes 1$, ..., $1 \otimes 1 \otimes ... \otimes x$.*

Le groupe symétrique S_k agit naturellement sur $\overline{R}$ et permute les conjugués d'un élément $x \in R$.

Proposition 16. *Le sous anneau de $\overline{R} \otimes \mathbb{Q}$ des éléments invariants par S_k est $\mathbb{Q}$. Par conséquent, le sous anneau de $\overline{R}$ des éléments invariants par S_k est $\mathbb{Z}$.*

Démonstration. Montrons que l'anneau des invariants par S_k de $\overline{R} \otimes_{\mathbb{Z}} \mathbb{Q}$ est $\mathbb{Q}$. On a une projection $\pi : x \to \frac{\sum_{\sigma \in S_k} \sigma \cdot x}{k!}$ de $\overline{R} \otimes_{\mathbb{Z}} \mathbb{Q}$ dans l'anneau des invariants.

Pour $(n_1, ..., n_k) \in \mathbb{Z}^k$, on considère $(n_1e_1 + ... + n_ke_k) \otimes ... \otimes (n_1e_1 + ... + n_ke_k) \in R$ où $(e_1, ..., e_k)$ est une base de R. Cette expression, une fois développée, est égale à $\sum_{(r_1,...,r_k) \in \mathbb{N}^k,\ r_1+...+r_k=k} n_1^{r_1} ... n_k^{r_k} S_{r_1,...,r_k}$ où $S_{r_1,...,r_k}$ est $\pi(x)$ où x est un tenseur pur dans lequel e_i apparaît r_i fois. Notre but est de montrer que $S_{r_1,...,r_k}$ s'exprime comme combinaison linéaire de tenseurs de la forme $x \otimes x \otimes ... \otimes x$. Pour cela, on voit $(n_1e_1 + ... + n_ke_k) \otimes ... \otimes (n_1e_1 + ... + n_ke_k)$ comme un polynôme à k variables en n_1, ..., n_k. On peut utiliser les dérivées partielles discrètes : si $P = P(n_1, ..., n_k)$, $\partial_i P(n_1, ..., n_k) := P(n_1, ..., n_{i-1}, n_i + 1, n_{i+1}, ..., n_k) - P(n_1, ..., n_k)$. On vérifie que si $P = \sum_{r_1+...+r_k=k} a_k X^{r_1} ... X^{r_k}$, et que si $r_1 + ... + r_k = k$, alors $\partial_1^{r_1} ... \partial_k^{r_k} P = r_1! ... r_k! a_k$. En appliquant ceci à $P(n_1, ..., n_k) = (n_1e_1 + ... + n_ke_k) \otimes ... \otimes (n_1e_1 + ... + n_ke_k)$, on obtient que $r_1! ... r_k! S_{r_1,...,r_k}$ est combinaison linéaire (à coefficient dans $\mathbb{Z}$) de tenseurs de la forme $x \otimes x \otimes ... \otimes x$. Or dans $\overline{R}$, $x \otimes ... \otimes x = N(x) \in \mathbb{Z}$ (par la proposition précédente). D'où le résultat voulu : $\overline{R}^{S_k} = \overline{R} \cap \mathbb{Q} = \mathbb{Z}$ car les éléments de $\overline{R}$ sont des entiers algébriques (cf appendice). □

Pour être sûr d'obtenir une bonne notion de « clôture galoisienne » sur des anneaux, on veut que la propriété classique sur la dimension soit vérifiée, c'est à dire que le rang de $\overline{R}^G$ est $[S_k : G]$ si G est un sous-groupe de S_n (classiquement, on met le G en exposant pour signifier qu'on regarde les invariants par G). On remarque que pour calculer le rang sur $\mathbb{Z}$, il est équivalent de calculer la dimension en tensorisant avec $\mathbb{Q}$. Cela nous amène à la notion d'algèbre étale.

Définition 26. *Une $\mathbb{Q}$-algèbre A est dite étale si $A \simeq K_1 \times ... \times K_n$ où K_i est une extension finie de $\mathbb{Q}$.*

Proposition 17. *Si A et B sont des $\mathbb{Q}$-algèbres étales, alors $A \otimes_{\mathbb{Q}} B$ est une $\mathbb{Q}$-algèbre étale.*

Démonstration. Cf [4] Paragraphe 6. □

On note $\overline{\mathbb{Q}}$ l'ensemble des nombres algébriques de $\mathbb{C}$, qui est une clôture algébrique de $\mathbb{Q}$.

Proposition 18. *Soit A une $\mathbb{Q}$-algèbre non dégénérée (i.e.* $\mathrm{Disc}(A) \neq 0$*). Alors A est étale sur $\mathbb{Q}$.*

Démonstration. Cf [4] Paragraphe 6. □

Proposition 19. *Si $A = K_1 \times ... \times K_n$ est une $\mathbb{Q}$-algèbre étale où K_i est une extension finie de $\mathbb{Q}$, alors*

$$\mathrm{Hom}_{\mathbb{Q}\text{-}Alg}(A, \overline{\mathbb{Q}}) = \bigsqcup_{i=1}^{n} \mathrm{Hom}_{\mathbb{Q}}(K_i, \overline{\mathbb{Q}})$$

On note $F(A) = \mathrm{Hom}_{\mathbb{Q}\text{-}Alg}(A, \overline{\mathbb{Q}})$, c'est un ensemble fini de cardinal $\dim_{\mathbb{Q}}(A)$.

Démonstration. Si $f \in \mathrm{Hom}_{\mathbb{Q}\text{-Alg}}(A, \overline{\mathbb{Q}})$, alors $f((1, ..., 1)) = 1 = f((1, 0, ..., 0)) + ... + f((0, ..., 0, 1))$. Or $f((1, 0, ..., 0))^2 = f((1, 0, ..., 0)^2) = f((1, 0, ..., 0))$ donc $f((1, 0, ..., 0))$ vaut 0 ou 1, et de même pour les autres termes. Comme on est en caractéristique 0, un seul de ces termes vaut 1 et les autres 0. On en déduit qu'il existe un unique $1 \leq i \leq n$ et un unique $\phi_i \in \mathrm{Hom}_{\mathbb{Q}}(K_i, \overline{\mathbb{Q}})$ tels que $f = \phi_i \circ p_i$ où $p_i : A \to K_i$ est la projection sur le facteur K_i. □

On pose $G = Gal(\overline{\mathbb{Q}}/\mathbb{Q}) := Hom_{\mathbb{Q}}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}})$. On a une action naturelle de G sur $F(A)$ (si $f \in F(A)$ et $\sigma \in G$, alors $\sigma \cdot f = \sigma \circ f$).

On a la propriété fonctorielle suivante.

Proposition 20. *Soient A et B deux $\mathbb{Q}$-algèbres étales. Alors :*

$$F(A \otimes_{\mathbb{Q}} B) = F(A) \times F(B)$$

Démonstration. On remarque que si $f \in F(A)$ et $g \in F(B)$, alors $f \otimes g \in F(A \otimes_{\mathbb{Q}} B)$. De plus cette application de $F(A) \times F(B)$ vers $F(A \otimes_{\mathbb{Q}} B)$ est injective. On conclut par cardinal. □

Proposition 21. *On a une anti-équivalence de catégories entre la catégorie des $\mathbb{Q}$-algèbres étales et la catégorie des ensembles finis munis une action de $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ qui se factorise par $\mathrm{Gal}(L/\mathbb{Q})$ pour une certaine extension galoisienne L de $\mathbb{Q}$ (L dépend a priori de la $\mathbb{Q}$-algèbre étale).*

Explicitement, on a les deux foncteurs contravariants suivants :

$$F : A \to \mathrm{Hom}_{\mathbb{Q}\text{-}Alg}(A, \overline{\mathbb{Q}})$$

et

$$E : X \to \{(x_f)_{f \in X} \in \overline{\mathbb{Q}}, \forall f \in X \text{ et } \forall \sigma \in G \ x_{\sigma \cdot f} = \sigma(x_f)\}$$

Ces deux foncteurs vérifient que $F(E(X))$ est canoniquement isomorphe à X et $E(F(A))$ est canoniquement isomorphe à A.

Démonstration. Montrons que $E(X)$ est une $\mathbb{Q}$-algèbre étale de dimension $n = Card(X)$. On commence par remarquer que si $(x_f)_{f \in X} \in E(X)$, alors $\forall f \in X$ et $\forall \sigma \in G$ tel que $\sigma \cdot f = f$ (i.e. $\sigma \in \mathrm{Stab}(f)$), alors $x_f = x_{\sigma \cdot f} = \sigma(x_f)$, donc $x_f \in \overline{\mathbb{Q}}^{\mathrm{Stab}(f)}$. Soit $\{f_1, ..., f_n\}$ un système de représentants de $G\backslash X$. Alors $(x_f)_{f \in X}$ est entièrement déterminé par x_{f_1}, ..., x_{f_n} car si $f \in X$, il existe $\sigma \in G$ et un unique $i \in \{1, ..., n\}$ tel que $f = \sigma \cdot f_i$, et alors $x_f = \sigma(x_{f_i})$. Réciproquement, si on se donne des $x_{f_i} \in \overline{\mathbb{Q}}^{\mathrm{Stab}(f_i)}$, on peut poser $x_f = \sigma(x_{f_i})$ avec $f = \sigma \cdot f_i$. Il suffit de vérifier que x_f est bien défini, mais c'est le cas car si on écrit $f = \tau \cdot f_i$, alors $\sigma\tau^{-1} \in \mathrm{Stab}(f_i)$ et $\sigma(x_{f_i}) = \tau(x_{f_i})$ car $x_{f_i} \in \overline{\mathbb{Q}}^{\mathrm{Stab}(f_i)}$. Au final, $\dim_{\mathbb{Q}}(E(X)) = \sum_{i=1}^{n} \mathrm{Card}(\mathrm{Stab}(f_i)) = \mathrm{Card}(X)$.

Le fait que ces deux applications soient des foncteurs est évident. Donnons les isomorphismes canoniques annoncés dans la proposition.

L'application $\eta(A) : x \to (f(x))_{f \in F(A)}$ est bien définie de A vers $E(F(A))$ (évident) et injective car si $A = K_1 \times ... \times K_r$, alors on connait les composantes de x selon les K_i si l'on connait les $f(x)$ pour $f \in \mathrm{Hom}_{\mathbb{Q}\text{-Alg}}(A, \overline{\mathbb{Q}}) = \bigsqcup_{i=1}^{r} \mathrm{Hom}_{\mathbb{Q}}(K_i, \overline{\mathbb{Q}})$. Cette application est surjective car on a montré que $\dim(E(F(A))) = \mathrm{Card}(F(A)) = \dim(A)$.

L'autre isomorphisme canonique $\psi(X)$ de X vers $F(E(X))$ se traite de même.

□

On pose $\overline{A} = A^{\otimes n}/I$ où I est l'idéal engendré par les $x \otimes ... \otimes 1 + ... + 1 \otimes ... \otimes x - \mathrm{Tr}(x)$.

Notre but est de montrer que $\dim_{\mathbb{Q}}(\overline{A}^H) = [S_n : H]$ si H est un sous-groupe de S_n (l'exposant signifie qu'on considère l'ensemble des éléments invariants par H). Pour cela on commence par expliciter $F(\overline{A})$. On rappelle que $F(A^{\otimes n}) = F(A)^n$, donc on peut voir $F(\overline{A})$ (qui correspond aux morphismes de $F(A^{\otimes n})$ nuls sur I) comme un sous-ensemble de $F(A)^n$.

Proposition 22. *Soit $n = Card(F(A))$.*
On a $F(\overline{A}) = \{(f_1, ..., f_n) \in F(A)^n, \forall i \neq j, f_i \neq f_j\}$.

Démonstration. Soient $(f_1, ..., f_n) \in F(A)^n$ tel que $f_1 \otimes ... \otimes f_n$ s'annule sur I, i.e. pour tout $x \in A$, $f_1(x) + ... + f_n(x) = \mathrm{Tr}(x)$. Or on sait que $\mathrm{Tr}(x) = \sum_{f \in F(A)} f(x)$. Par le lemme d'indépendance des caractères, on conclut que tous les f_i sont distincts. La réciproque est évidente avec ce qu'on a fait. □

On sait que S_n agit naturellement à gauche sur $\overline{A}$. On a aussi une action à droite naturelle de S_n sur $F(\overline{A})$. Comme $F(\overline{A}) = S_n$ (cf proposition précédente, c'est un abus de langage car il faudrait plutôt dire

que $F(\overline{A})$ est un S_n-torseur), cette action correspond à la multiplication à droite dans S_n. Il est évident que cette action commute à l'action du groupe de Galois G.

Proposition 23. *Soit H un sous-groupe de S_n. Alors :*

$$F(\overline{A}^H) = F(\overline{A})/H$$

(le membre de gauche est l'ensemble des orbites $F(\overline{A})$ par H).

Démonstration. Par la proposition 5, on peut voir $\overline{A}$ comme un ensemble de $(x_f)_{f\in F(\overline{A})}$ (vérifiant certaines conditions énoncées dans la propositions). Or $(x_f) \in \overline{A}^H$ ssi pour tout $\tau \in H$ et $f \in F(\overline{A})$, $x_{f\cdot\tau} = x_f$. Comme l'action de G commute à celle de S_n (sur $F(\overline{A})$), on a une bijection $F(\overline{A})/H \to F(\overline{A}^H)$. □

On en déduit le résulat annoncé plus haut.

Théorème 12. *Si H est un sous-groupe de S_n, alors* $\dim_{\mathbb{Q}}(\overline{A}^H) = [S_n : H]$.

Démonstration. On a $\dim_{\mathbb{Q}}(\overline{A}^H) = Card(F(\overline{A}^H)) = Card(F(\overline{A})/H) = [S_n : H]$. □

On en déduit le résultat voulu.

Corollaire 12. *Si R est un anneau de rang k et que G est un sous-groupe de S_k, alors $\overline{R}^G$ est de rang $[S_k : G]$ sur $\mathbb{Z}$.*

Démonstration. Le rang est invariant si on tensorise R par $\mathbb{Q}$. □

4.1. **Résolvante quadratique d'un anneau cubique.** Nous allons interpréter la classification de Delone-Faddeev des anneaux cubiques avec une autre méthode qui sera généralisable aux anneaux quartiques.

Faisons d'abord quelques rappels sur les corps. On se donne P un polynôme de degré 3 à coefficients rationnels dont le groupe de Galois est S_3. On peut trouver les racines de P grâce à la suite de composition $1 \subset A_3 \subset S_3$ (qui prouve que S_3 est résoluble). On note K le corps de décomposition de P. Alors $R = K^{A_3}$ est l'unique sous-extension quadratique Galoisienne. En fait, si $\Delta = \mathrm{Disc}(P)$, alors $R = \mathbb{Q}(\sqrt{\Delta})$ et R a donc même discriminant que K. On montre qu'on peut exprimer les racines de P en fonction de racines cubiques d'éléments de R. On va utiliser la même idée pour les anneaux cubiques.

Définition 27. *Si R est un anneau cubique, on définit $S^{res}(R)$ comme l'unique anneau quadratique de discriminant $D = \mathrm{Disc}(R)$. On appelle $S^{res}(R)$ l'anneau quadratique résolvant de R.*

Si $x \in R$, on note x' et x'' ses conjugués dans $\overline{R}$ (on plonge R dans $\overline{R}$ par $x \to x \otimes 1 \otimes ... \otimes 1$). On a une application naturelle $\tilde{\phi}_{3,2} : R \to \overline{R} \otimes \mathbb{Q}$ telle que

$\tilde{\phi}_{3,2}(x) = \frac{((x-x')(x'-x'')(x''-x))^2+(x-x')(x'-x'')(x''-x)}{2}$ qui est contenu dans un anneau quadratique de même discriminant que x. En effet :

Lemme 3. *Le polynôme caractéristique de x est $\chi_x = (X-x)(X-x')(X-x'')$. Donc* $\mathrm{Disc}(x) = ((x-x')(x'-x'')(x''-x))^2$.

Démonstration. La première égalité est une conséquence immédiate de la proposition concernant les fonctions symétriques élémentaires. La deuxième égalité vient du fait que le discriminant est un polynôme en les fonctions symétriques élémentaires en x, x' et x''. □

En fait, le groupe alterné A_3 laisse fixe $\tilde{\phi}_{3,2}(x)$ et donc (fait admis pour le moment) le sous anneau $S^{inv}(R) := \mathbb{Z}[\tilde{\phi}_{3,2}(x), x \in R]$ est un sous anneau quadratique de $\overline{R} \otimes \mathbb{Q}$. On appelle $S^{inv}(R)$ l'anneau quadratique invariant de R. Il est naturel de se demander le lien entre $S^{inv}(R)$ et $S^{res}(R)$.

Lemme 4. *Si $x \in R$,* $\mathrm{Disc}(x) = n^2\mathrm{Disc}(R)$ *pour un $n \in \mathbb{N}$. Donc $S^{inv}(R) \subset S^{res}(R)$.*

Démonstration. On rappelle que par définition, si $L = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_3$ est un sous réseau de R, alors $\mathrm{Disc}(L) := \mathrm{Det}(Tr(\alpha_i\alpha_j)) = \mathrm{Det}(\alpha_i^{(j)})^2$ où $\alpha_i^{(j)}$ est le j-ième conjugué de α_i (cette dernière égalité découle simplement de la définition de la trace comme somme des conjugués). Donc si $L \subset L'$ sont deux sous-réseaux de R, $\mathrm{Disc}(L') = \mathrm{Disc}(L)\cdot[L' : L]^2$. Montrons que $\mathrm{Disc}(x) = \mathrm{Disc}(L)$ où $L = \mathbb{Z}+\mathbb{Z}x+\mathbb{Z}x^2$. On sait que $\mathrm{Disc}(x) = ((x-x')(x'-x'')(x''-x))^2$ (le polynôme caractéristique P_x de x est $(X-x)(X-x')(X-x'')$, cf ci-dessus). Or :

$$\mathrm{Disc}(L) = \begin{vmatrix} 1 & 1 & 1 \\ x & x' & x'' \\ x^2 & (x')^2 & (x'')^2 \end{vmatrix}^2 = ((x-x')(x'-x'')(x''-x))^2$$

□

Nous verrons plus tard une CNS pour que $S^{inv}(R) = S^{res}(R)$.

On note que si $c \in \mathbb{Z}$, alors $\tilde{\phi}_{3,2}(x+c) = \tilde{\phi}_{3,2}(x)$ donc $\tilde{\phi}_{3,2}$ induit une application

$$\phi_{3,2} : R/\mathbb{Z} \to S/\mathbb{Z}$$

où $S := S^{res}(R)$. Si on choisit une base (ω_1, ω_2) de $R/\mathbb{Z}$ et une base de $S/\mathbb{Z} = \mathbb{Z}$, alors $\phi_{3,2}$ est une forme binaire cubique. Explicitement, si on prend $(1, \omega_1, \omega_2)$ qui est une base normale de R, i.e

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

alors on calcule : $\mathrm{Disc}(x\omega_1 + y\omega_2) = D(ax^3 + bx^2y + cxy^2 + dy^3)^2$ où $D := \mathrm{Disc}(R) = \mathrm{Disc}(S)$. On choisit pour générateur de $S/\mathbb{Z}$ $\frac{D+\sqrt{D}}{2}$ (i.e. on fait le choix d'une racine carré de $\sqrt{D}$, ce qui correspond à orienter $S = S(D)$). Alors $\phi_{3,2}(x) = \frac{\mathrm{Disc}(x\omega_1+y\omega_2)+\sqrt{\mathrm{Disc}(x\omega_1+y\omega_2)}}{2} = (ax^3 + bx^2y + cxy^2 + dy^3)(\frac{D+\sqrt{D}}{2})$ modulo $\mathbb{Z}$. Donc $\phi_{3,2}$ représente dans ces bases $ax^3 + bx^2y + cxy^2 + dy^3$. Or les $GL_2(\mathbb{Z})$-classes de formes binaires cubiques paramétrisent les classes d'isomorphie d'anneaux cubiques. Par conséquent on peut interpréter la bijection de Delone-Faddeev de la façon suivante :

Théorème 13. *Il y a une bijection entre les classes d'isomorphie de couples (R, S) où $S = S^{res}(R)$ et les classes d'isomorphie d'applications cubiques $\phi : M \to L$ où M et L sont des $\mathbb{Z}$-modules de rangs 2 et 1 respectivement.*

Démonstration. A une telle application ϕ représentant une forme binaire cubique f à $GL_2(\mathbb{Z})$-équivalence près, on associe $(R(f), S^{res}(R(f)))$ où $R(f)$ est l'anneau cubique associé à f. □

C'est ce théorème qu'on va généraliser aux anneaux quartiques. Cependant il n'y aura pas unicité de l'anneau résolvant, d'où l'intérêt d'énoncer le théorème précédent avec des couples (R, S), même si S est déterminé par R.

Avant de passer au cas quartique, nous allons répondre à la question posée ci-dessus : à quelle condition $S^{inv}(R) = S^{res}(R)$? On aura pour cela besoin d'une notion fondamentale.

Définition 28. *Soit R un anneau de rang k. Le contenu de R, noté $ct(R)$, est défini par :*

$$ct(R) = max\{n : \exists \tilde{R} \text{ de rang } k \text{ tel que } R = \mathbb{Z} + n\tilde{R}\}$$

(si le maximum n'existe pas, on pose $ct(R) = \infty$).

L'anneau R est dit primitif si $ct(R) = 1$.

Dans le cas quadratique, le contenu est habituellement appelé le « conducteur ». Mis à part le cas de l'anneau quadratique dégénéré $\mathbb{Z}[X]/(X^2)$ pour lequel le contenu est infini (écrire $\mathbb{Z}[X]/(X^2) = \mathbb{Z} + n\mathbb{Z}[X_n]/(X_n^2)$ avec $X = nX_n$, pour tout $n \geq 0$), le contenu est fini. En effet, par exemple si le discriminant D n'est pas un carré parfait, $S(D)$ est un sous-anneau de l'ordre quadratique maximal

$S(D')$ où D' est l'entier obtenu à partir de D en enlevant les exposants dans les facteurs premiers (i.e. le radical de D). En d'autres termes, $S(D')$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ (qui est le sous-anneau quadratique maximal de $\mathbb{Q}(\sqrt{D})$ car tout élément d'un anneau quadratique est un entier algébrique). Donc nécessairement $ct(S(D)) = [S(D') : S(D)] < \infty$.

Dans le cas cubique, si $R = R(f)$ où $f(x,y) = ax^2 + bx^2y + cxy^2 + dy^3$, alors $ct(R) = pgcd(a,b,c,d)$. En effet, si $R = \mathbb{Z} + n\tilde{R}$, on écrit $\tilde{R} = R(\tilde{f})$. Alors si $(1, w_1, w_2)$ est une base normale de $\tilde{R}$ avec la table de multiplication associée à $\tilde{f}$, alors $(1, n\omega_1, n\omega_2)$ est une base normale de R associée à $f' := n\tilde{f}$. Donc n divise $pgcd(a,b,c,d)$ (f' et f sont $GL_2(\mathbb{Z})$-équivalents et le pgcd des coefficients est invariant par équivalence). Réciproquement si n divise $pgcd(a,b,c,d)$, on peut diviser la base normale associée par n et écrire comme ci-dessus $R = \mathbb{Z} + n\tilde{R}$.

Proposition 24. *Soit R un anneau cubique et $S = S^{res}(R)$. Alors $[S : S^{inv}(R)] = \epsilon(R) \cdot ct(R)$, où $\epsilon(R) = 2$ si $R = \mathbb{Z} + ct(R) \cdot R_1$ avec $R_1 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2^3$ et $\epsilon(R) = 1$ sinon. En particulier, $S^{inv}(R) = S$ ssi R est primitif et $R_1 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \ncong \mathbb{Z}_2^3$ (en tant qu'anneau).*

Démonstration. On sait que $S^{inv}(R) \subset S$. Or tout sous-anneau de S est de la forme $\mathbb{Z} + rS$ pour un $r \geq 0$. En effet, un sous anneau de $S/\mathbb{Z}$ est de la forme $r \cdot S/\mathbb{Z}$ car en tant que $\mathbb{Z}$-module $S/\mathbb{Z} = \mathbb{Z}$. Donc $S^{inv}(R) = \mathbb{Z} + rS$ où r est le plus petit entier positif tel que $\phi_{3,2}(x)$ soit un multiple de r dans $S/\mathbb{Z}$, pour tout $x \in R/\mathbb{Z}$. Soit f une forme binaire cubique associée à $\phi_{3,2}$ (qu'on peut choisir à $GL_2(\mathbb{Z})$-équivalence près). On a donc vu que $[S : S^{inv}(R)]$ est le pgcd des valeurs prises par f. On pose $ct(f) := ct(R) = pgcd$(coefficients de f) On conclut avec le lemme suivant.

Lemme 5. *Le pgcd des valeurs prises par f est $\epsilon(R) \cdot ct(R)$.*

Démonstration. Soit d le pgcd de l'énoncé. On écrit $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$. Soit $G = d\mathbb{Z}$ le groupe engendré par les $f(u,v)$, $u, v \in \mathbb{Z}$. On a $G \subset ct(f)\mathbb{Z}$ donc $ct(f)$ divise d. De plus G contient a, d, $b+c$, $b-c$, donc a, d, $2b$, $2c$ et par conséquent d divise $2ct(f)$. On peut donc écrire $d = \epsilon(f) \cdot ct(f)$ avec $\epsilon(f) \in \{1,2\}$ et $\epsilon(f)$ vaut 1 ssi $f/ct(f)$ prend une valeur impaire et 2 sinon. Quitte à tout diviser par $ct(f)$, on suppose $ct(f) = 1$, i.e. $pgcd(a,b,c,d) = 1$. Alors clairement $\epsilon(f) = 2$ ssi $a, d \equiv 0 \bmod 2$ et $b, c \equiv 1 \bmod 2$. En utilisant la table de multiplication de la base normale associée, si $\epsilon(f) = 2$ il existe une base normale $(1, \omega_1, \omega_2)$ de R telle que $\overline{w_1}^2 = \overline{w_1}$, $\overline{w_2}^2 = \overline{w_2}$ et $\overline{w_1 w_2} = 0$ modulo 2, donc $R_1 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2^3$. Réciproque admise, basée sur le lemme de Hensel. □

□

4.2. **Résolvantes cubiques d'un anneau quartique.** On se donne Q un anneau quartique. On considère $\tilde{\phi}_{4,3} : Q \to \overline{Q}\ x \to xx' + x''x'''$ où x', x'' et x''' sont les conjugués de x dans $\overline{Q}$.
On reconnaît ici l'expression classique intervenant dans la résolvante de Lagrange pour la résolution de l'équation de degré 4. Plus précisément,

Définition 29. *Soit $P(X) = X^4 + pX^3 + qX^2 + rX + s$ un polynôme. On appelle résolvante de Lagrange le polynôme $Q(X) = X^3 - qX^2 + (pr - 4s)X - (p^2s - 4qs - r^2)$. Si $P(X) = (X-\alpha)(X-\alpha')(X-\alpha'')(X-\alpha''')$, alors $Q(X) = (X - (\alpha\alpha' + \alpha''\alpha'''))(X - (\alpha\alpha'' + \alpha'\alpha'''))(X - (\alpha\alpha''' + \alpha'\alpha''))$.*

Définition 30. *On pose $R^{inv}(Q) = \mathbb{Z}[\tilde{\phi}_{4,3}(x) : x \in Q]$.*

Proposition 25. *On a $R^{inv}(Q) \subset \overline{Q}^{D_4}$ où $D_4 = \{\mathrm{Id}, (2413), (34), (12), (13)(24), (21)(43), (23)(41), (2314)\}$.*

L'anneau $R^{inv}(Q)$ est de rang 3.

Démonstration. La première assertion est évidente.
Pour prouver la deuxième, il y a deux choses à voir : d'une part que sur $\mathbb{Q}$, R^{inv} (qui est défini de la même manière sur $\mathbb{Q}$ avec les $\phi_{4,3}$, ou bien en tensorisant par $\mathbb{Q}$ l'anneau $R^{\mathrm{inv}}(Q)$) est exactement l'anneau des invariants par D_4 et d'autre part que cette $\mathbb{Q}$-algèbre étale est de dimension 3 sur $\mathbb{Q}$. Il est clair que le point sur la dimension découle du théorème 12 à condition d'avoir prouvé le premier point.

Comme pour le calcul des invariants par S_4, on considère la projection $\pi(e_1 \otimes e_2 \otimes e_3 \otimes e_4) = e_1 \otimes e_2 \otimes e_3 \otimes e_4 + e_2 \otimes e_1 \otimes e_3 \otimes e_4 + e_1 \otimes e_2 \otimes e_4 \otimes e_3 + e_3 \otimes e_4 \otimes e_1 \otimes e_2 + e_3 \otimes e_4 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_4 \otimes e_3 + e_4 \otimes e_3 \otimes e_2 \otimes e_1 + e_4 \otimes e_3 \otimes e_1 \otimes e_2$.

En développant $\tilde{\phi}_{4,3}(e_1 + e_2)\tilde{\phi}_{4,3}(e_3 + e_4)$ on obtient une combinaison linéaire de $\pi(e_1 \otimes e_2 \otimes e_3 \otimes e_4)$ et d'éléments de la forme $\tilde{\phi}_{4,3}(x)$, donc $\pi(e_1 \otimes e_2 \otimes e_3 \otimes e_4) \in \mathbb{Q}[\tilde{\phi}_{4,3}(x), x \in R] = R^{\mathrm{inv}}$. □

Avant de continuer, on aura besoin d'identifier $\overline{R}$ et un anneau du type $\overline{Q}^G$ où G est un sous-groupe de S_4 contenu dans D_4 et $R = R^{\mathrm{inv}}$. Comme d'habitude on va travailler sur $\mathbb{Q}$.

Soit Q une algèbre étale de dimension 4 et $R = \overline{Q}^{D_4}$ sa résolvante cubique, où D_4 est le groupe diédral d'ordre 8 défini dans la proposition précédente. Plus précisément, il y a trois 2-sylow dans S_4 (en effet le nombre de 2-sylow divise 3 et est congru à 1 mod 2, mais D_4 n'est pas distingué dans S_4), tous les trois conjugués et isomorphes à D_4. Le groupe S_4 agit sur les 2-sylow par conjugaison, ce qui donne une suite exacte $1 \to V_4 \to S_4 \to S_3 \to 1$ où V_4 est un sous-groupe distingué d'ordre 4. De plus le normalisateur de D_4 dans S_4 est d'indice 3 et contient D_4, donc c'est D_4 (i.e. si $gD_4g^{-1} = D_4$, alors $g \in D_4$). On fixe des représentants de S_4/D_4 notés σ_1, σ_2 et σ_3, avec $\sigma_1 = \mathrm{Id}$. On note $G_i = \sigma_i D_4 \sigma_i^{-1}$. Les G_i ($i = 1, 2, 3$) sont distincts car si $G_i = G_j$, $\sigma_i\sigma_j^{-1} \in D_4$ (par la remarque précédente), donc $i = j$. On a aussi $V_4 = G_1 \cap G_2 \cap G_3$ (évident).

Théorème 14. *Il y a un isomorphisme de $\mathbb{Q}$-algèbre S_3-équivariant entre $\overline{R}$ et $\overline{Q}^{V_4}$ (où S_3 agit sur $\overline{Q}^{V_4}$ par $p(g) \cdot x := g \cdot x$ où $p : S_4 \to S_3$ est la surjection précédente, et ceci ne dépend pas du choix de g car x est invariant par $Ker(p) = V_4$).*

Démonstration. On considère l'application $\tilde{\phi} : R^{\otimes n} \to \overline{Q}^{V_4}$ telle que $\tilde{\phi}(r_1 \otimes r_2 \otimes r_3) = \sigma_1(r_1)\sigma_2(r_2)\sigma_3(r_3)$ (et ϕ ne dépend pas du choix des représentants de S_4/D_4 car $R = \overline{Q}^{D_4}$). L'application $\tilde{\phi}$ est bien définie car $V_4 = \cap_{i=1}^3 \sigma_i D_4 \sigma_i^{-1}$ stabilise $\sigma_i(r)$ si r est invariant par D_4. De plus $\tilde{\phi}$ se factorise par J' (idéal engendré par les $r \otimes 1 \otimes 1 + 1 \otimes r \otimes 1 + 1 \otimes 1 \otimes r - \mathrm{Tr}(r)$ où $r \in R$) car $\phi(r \otimes 1 \otimes 1 + 1 \otimes r \otimes 1 + 1 \otimes 1 \otimes r) = \sigma_1(r) + \sigma_2(r) + \sigma_3(r) = \mathrm{Tr}(r)$. On note $\phi : \overline{R} \to \overline{Q}^{V_4}$ l'application induite par $\tilde{\phi}$. On a vu que $dim_{\mathbb{Q}}(\overline{R}) = dim_{\mathbb{Q}}(\overline{Q}^{V_4}) = 3! = 6$. Pour montrer que ϕ est bijective, il suffit donc de montrer qu'elle est surjective. On considère $V = \overline{Q}^{G_1} \oplus \overline{Q}^{G_2}$ et $f : V \to \overline{Q}^{V_4}$ telle que $f((x, y)) = x + y$ (f est bien définie car $V_4 = G_1 \cap G_2 \cap G_3 \subset G_1 \cap G_2$). Si $f((x, y)) = 0$, alors $x = -y$ est fixé par G_1 et G_2, donc est fixé par le sous-groupe de S_4 engendré par G_1 et G_2, c'est à dire S_4 (D_4 est d'indice 3 donc si $g \notin D_4$, le sous-groupe engendré par D_4 et g est S_4). Donc x, $y \in \mathbb{Q}$. Comme $\dim(\overline{Q}^{G_i}) = [S_4 : G_i] = 3$, $\mathrm{Im}(f) = 3 + 3 - 1 = 5$. Donc $\dim(\overline{Q}^{G_1} + \overline{Q}^{G_2}) = 5$. Montrons que $\overline{Q}^{G_1} + \overline{Q}^{G_2} + \overline{Q}^{G_3} = \overline{Q}^{V_4}$ (ce dernier étant de dimension 6). Par dimension, il suffit de montrer qu'on a $\overline{Q}^{G_3} \not\subset \overline{Q}^{G_1} + \overline{Q}^{G_2}$. Soit $x + y \in (\overline{Q}^{G_1} + \overline{Q}^{G_2}) \cap \overline{Q}^{G_3}$. Alors $\sigma_3 \cdot (x + y) = x + y$, donc $y - \sigma_3 \cdot x = \sigma_3 \cdot y - x \in \overline{Q}^{G_1} \cap \overline{Q}^{G_2} = \mathbb{Q}$. Donc $y = \sigma_3 \cdot x + t$ où $t \in \mathbb{Q}$. Donc $\dim((\overline{Q}^{G_1} + \overline{Q}^{G_2}) \cap \overline{Q}^{G_3}) \leq \dim(\overline{Q}^{G_1}) + \dim(\mathbb{Q}) = 3 + 1 = 4$. Comme $\dim(\overline{Q}^{G_1} + \overline{Q}^{G_2}) = 5$, on ne peut pas avoir $\overline{Q}^{G_3} \subset \overline{Q}^{G_1} + \overline{Q}^{G_2}$.

Pour conclure, il suffit de remarquer que $\mathrm{Im}(\phi)$ contient $\overline{Q}^{G_1} + \overline{Q}^{G_2} + \overline{Q}^{G_3}$. C'est évident car $\phi(r_1 \otimes 1 \otimes 1 + 1 \otimes r_2 \otimes 1 + 1 \otimes 1 \otimes r_3) = \sigma_1(r_1) + \sigma_2(r_2) + \sigma_3(r_3)$ et que $\sigma_i(R) = \sigma_i(R^{D_4}) = R^{\sigma_i D_4 \sigma_i^{-1}} = R^{G_i}$.

□

Proposition 26. *L'application $\phi_{4,3}$ préserve le discriminant.*

Démonstration. On raisonne sur $\mathbb{Q}$. Par la proposition précédente, on peut identifier les S_3 conjugués de $\alpha\alpha' + \alpha''\alpha''' \in \overline{R}$ aux S_3-conjugués de $\alpha\alpha' + \alpha''\alpha''' \in \overline{Q}^{V_4}$, qui sont $\alpha\alpha' + \alpha''\alpha'''$, $\alpha\alpha'' + \alpha'\alpha'''$ et $\alpha\alpha''' + \alpha'\alpha''$. On a alors immédiatement : $\chi_{\phi_{4,3}(\alpha)} = (X - (\alpha\alpha' + \alpha''\alpha'''))(X - (\alpha\alpha'' + \alpha'\alpha'''))(X - (\alpha\alpha''' + \alpha'\alpha''))$. C'est bien la résolvante cubique de χ_α (cf définition 29). □

Définition 31. *Soit Q un anneau quartique. Un anneau résolvant de Q est un anneau cubique R tel que* $\mathrm{Disc}(R) = \mathrm{Disc}(Q)$ *et* $R^{inv}(Q) \subset R$.

A priori, on ne sait pas s'il existe un anneau résolvant de Q et s'il existe il n'est pas forcément unique. Nous donnerons plus tard le nombre exact d'anneaux résolvants.

On remarque que si $c \in \mathbb{Z}$ alors $\tilde{\phi}_{4,3}(x+c) = \tilde{\phi}_{4,3}(x) + d$ pour un certain $d \in \mathbb{Z}$. Donc $\tilde{\phi}_{4,3}$ induit une application :

$$\phi_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$$

Cette application est une application quadratique de $\mathbb{Z}^3$ dans $\mathbb{Z}^2$. Si on fixe des bases de $Q/\mathbb{Z}$ et de $R/\mathbb{Z}$, on obtient donc une paire de formes quadratiques ternaires qu'on représente par une paire de matrices symétriques $(A, B) \in (Sym^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ (les coefficients de A et B peuvent être demi-entiers). Changer de base revient à agir sur (A, B) par l'action naturelle de $G_{\mathbb{Z}} = GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$. Explicitement,

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

où $g_2 = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$.

Définition 32. *On pose* $\mathrm{Disc}(A, B) = \mathrm{Disc}(4 \cdot \mathrm{Det}(Ax + By)) \in \mathbb{Z}$*, qui est invariant sous l'action de* $G_{\mathbb{Z}}$ *(on a noté abusivement* $\mathrm{Det}(Ax + By)$ *pour dire la forme* $(x, y) \to \mathrm{Det}(Ax + By)$*).*

En fait on va voir que ces couples de formes paramétrisent les couples (Q, R). La stratégie va être de partir du couple (A, B) et d'en déduire la structure possible de Q et R (l'inverse semble difficile car on ne sait pas décrire (A, B) facilement).

4.3. **Structure de Q.** Si M est un $\mathbb{Z}$ module libre orienté de rang k, et si v_1, v_2, ..., v_k sont dans M, on définit $Ind_M(v_1, ..., v_k)$ comme le déterminant de $(v_1, ..., v_k)$ dans une base orientée quelconque de M.

Le lemme suivant jouera un rôle important dans la suite.

Lemme 6. *Soit Q un anneau quartique non dégénéré. Si R est une résolvante de Q, alors pour tous x, $y \in Q$,*

$$Ind_Q(1, x, y, xy) = \pm Ind_R(1, \phi_{4,3}(x), \phi_{4,3}(y))$$

Démonstration. On note choisit $(1, \alpha_1, \alpha_2, \alpha_3)$ une $\mathbb{Z}$ base de Q et $(1, \beta_1, \beta_2)$ une $\mathbb{Z}$ base de R. On pose A la matrice de $(1, x, y, xy)$ dans $(1, \alpha_1, \alpha_2, \alpha_3)$ et B celle de $(1, \phi_{4,3}(x), \phi_{4,3}(y))$ dans $(1, \beta_1, \beta_2)$. On doit montrer que $\mathrm{Det}(A) = \pm\mathrm{Det}(B)$. Cela résulte de l'identité suivante :

$$\mathrm{Disc}(Q)\mathrm{Det}(A)^2 = \begin{vmatrix} 1 & 1 & 1 & 1 \\ x & x' & x'' & x''' \\ y & y' & y'' & y''' \\ xy & x'y' & x''y'' & x'''y''' \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 & 1 \\ xx' + x''x''' & xx'' + x'x''' & xx''' + x'x'' \\ yy' + y''y''' & yy'' + y'y''' & yy''' + y'y'' \end{vmatrix}^2 = \mathrm{Disc}(R)\mathrm{Det}(B)^2.$$

Pour prouver la dernière égalité, il suffit de dire qu'on peut identifier (cf théorème 14) les S_3 conjugués de $xx' + x''x''' \in \overline{R}$ aux S_3-conjugués de $xx' + x''x''' \in \overline{Q}^{V_4}$, qui sont $xx' + x''x'''$, $xx'' + x'x'''$ et $xx''' + x'x''$. □

On choisit des bases $(1, \alpha_1, \alpha_2, \alpha_3)$ et $(1, \omega_1, \omega_2)$ telles que le signe dans l'énoncé du lemme soit positif (i.e. telles que $Ind_Q(1, x, y, xy) = Ind_R(1, \phi_{4,3}(x), \phi_{4,3}(y))$). On dit que deux telles bases sont compatibles.

En translatant les éléments de ces bases par des entiers, on peut supposer que ces bases sont normales au sens suivant : $\alpha_1\alpha_2 \in \mathbb{Z} + \alpha_3\mathbb{Z}$ et $\alpha_1\alpha_3 = \mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z}$, $\omega_1\omega_2 \in \mathbb{Z}$.

Théorème 15. *Soit $(A,B) \in (Sym^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$. Si (A,B) provient de l'application $\phi_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$ alors Q est entièrement déterminé par (A,B) et $\mathrm{Disc}(Q) = \mathrm{Disc}(A,B)$.*

Démonstration. On peut écrire :

$$\phi_{4,3}(t_1\overline{\alpha_1} + t_2\overline{\alpha_2} + t_3\overline{\alpha_3}) = B(t_1,t_2,t_3)\overline{\omega}_1 + A(t_1,t_2,t_3)\overline{\omega}_2$$

$$\alpha_i\alpha_j = c_{ij}^0 + \sum_{k=1}^{3} c_{ij}^k \alpha_k$$

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

où $c_{ij}^k \in \mathbb{Z}$, $c_{12}^1 = c_{12}^2 = c_{13}^1 = 0$ et a, b, c, $d \in \mathbb{Z}$.
Considérons $x = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3$ et $y = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3$ des éléments de Q.
On a $xy = c + t_1\alpha_1 + t_2\alpha_2 + t_3\alpha_3$ avec

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

On en déduit

$$Ind_Q(1,x,y,xy) = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & r_1 & r_2 & r_3 \\ 0 & s_1 & s_2 & s_3 \\ 0 & t_1 & t_2 & t_3 \end{vmatrix} = Ind_R(1,\phi_{4,3}(x),\phi_{4,3}(y)) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & B(r_1,r_2,r_3) & A(r_1,r_2,r_3) \\ 0 & B(s_1,s_2,s_3) & A(s_1,s_2,s_3) \end{vmatrix}$$

Ces deux déterminants sont des polynômes à coefficients entiers en les r_i, s_i, qui sont égaux quand ceux-ci prennent des valeurs entières, les coefficients des polynômes sont donc égaux, et fournissent un système d'équations linéaires en les c_{ij}^k.

On écrit $A(x_1,x_2,x_3) = \sum_{1\le i\le j\le 3} a_{ij}x_ix_j$, de même pour B.
Définissons alors les constantes

$$\lambda_{kl}^{ij} = \lambda_{kl}^{ij}(A,B) = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{kl} & b_{kl} \end{vmatrix}$$

Etant donné que $a_{ij} = a_{ji}$, les λ_{kl}^{ij} ne peuvent prendre que 15 valeurs différentes. On trouve alors que le système d'équation a l'unique solution suivante :

$$(*)\begin{cases} c_{ii}^i = \pm\lambda_{ij}^{ik} + C_i \\ c_{ii}^j = \pm\lambda_{ik}^{ii} \\ c_{ij}^i = \pm\frac{1}{2}\lambda_{jj}^{ik} + c_{ii}^i = \pm\lambda_{kl}^{ij} + C_j \\ c_{ij}^k = \pm\lambda_{ii}^{jj} \end{cases}$$

où (i,j,k) est une permutation de $(1,2,3)$, $\pm$ dénote son signe, $C_1 = \lambda_{11}^{23}$, $C_2 = -\lambda_{22}^{13}$, et $C_3 = \lambda_{33}^{12}$.
Pour déterminer les c_{ij}^0, on utilise la loi d'associativité pour Q : l'égalité $(\alpha_i\alpha_j)\alpha_k = \alpha_i(\alpha_j\alpha_k)$ fournit l'équation

$$\forall k \neq 0, j \quad c_{ij}^0 = \sum_{r=1}^{3}(c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k)$$

On vérifie que la valeur du membre de droite ne dépend pas de k, et que ces équations sont équivalentes aux lois d'associativités.
Finalement, tous les c_{ij}^k sont entiers et déterminent bien la structure de $Q = Q(A,B)$.
La table de multiplication de Q dans une base non normalisée en découle, il suffit de remarquer que si α_i est translaté d'un entier c, la constante C_i l'est de $2c$. Dans une base quelconque, seuls les C_i changent, avec $C_i \equiv \lambda_{ii}^{jk}[2]$.

L'égalité $\mathrm{Disc}(Q) = \mathrm{Disc}(A,B)$ provient d'un calcul direct. □

Notons dès à présent que les λ_{kl}^{ij} sont invariants par l'action de $SL_2(\mathbb{Z})$, ce qui sera utilisé dans la suite.

4.4. **Structure de R.** On a le résultat suivant :

Théorème 16. *Soit $(A,B) \in (Sym^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ un couple de formes non dégénéré. Si (A,B) provient de l'application $\phi_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$ alors R est entièrement déterminé par (A,B) et $\mathrm{Disc}(R) = \mathrm{Disc}(A,B)$.*

Démonstration. A ce couple (A,B) on peut associer une forme cubique binaire naturelle (invariante par l'action de $SL_3(\mathbb{Z})$) :

$$g(x,y) = a'x^3 + b'x^2y + c'xy^2 + d'y^3 = 4 \cdot \mathrm{Det}(Ax + By)$$

Nous allons montrer que cette forme est égale à celle associée à l'anneau cubique R, $f = ax^3 + bx^2y + cxy^2 + dy^3$.
Soit $x = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3$, on a :

$$Ind_Q(1, x, x^2, x^3) = Ind_R(1, \phi_{4,3}(x), \phi_{4,3}(x)^2)$$

car $\tilde{\phi}_{4,3}(x)^2 = \tilde{\phi}_{4,3}(x^2) + 2N(x)$, d'où $\phi_{4,3}(x)^2 = \phi_{4,3}(x^2)$ et on applique l'identité du lemme précédent.

Les lois de Q étant connues, on se ramène à nouveau à 2 polynômes ayant les mêmes valeurs sur les entiers, donc égaux. Les équations obtenues en les variables a, b, c, d ont une unique solution dès lors que l'image de $\phi_{4,3}$ engendre un réseau de rang 2. Si $\mathrm{Disc}(A,B) \neq 0$, la solution est alors donnée par $a = a'$, $b = b'$,$c = c'$ et $d = d'$ et l'anneau R est déterminé. □

Il faut maintenant vérifier que R est bien une résolvante cubique de Q, c'est à dire que $R^{\mathrm{inv}} \hookrightarrow R$. On admet ce fait.

On peut résumer ce qu'on a fait par le théorème suivant.

Théorème 17. *Il y a une bijection entre les paires de formes quadratiques ternaires non dégénérées et l'ensemble des classes d'isomorphie de couples non dégénérés (Q,R) où Q est un anneau quartique et R est un anneau cubique résolvant, munis de bases compatibles. (Une classe d'isomorphie est un couple à isomorphisme d'anneau près, tel que cet isomorphisme d'anneau envoie les deux bases compatibles sur les deux bases compatibles correspondantes).*

De plus cette bijection préserve le discriminant.

Dans ce qui suit, on va répondre aux questions suivantes : pour tout Q, existe-t-il une résolvante ? Si oui quel est le nombre de ces résolvantes et à quelles conditions y a-t-il unicité ?

4.5. **Calcul du nombre de résolvantes.** On a vu que les 15 $SL_2(\mathbb{Z})$ invariants $\lambda_{kl}^{ij} = \lambda_{kl}^{ij}(A,B)$ déterminent entièrement la structure de Q et pour déterminer les résolvantes de Q, on va donc étudier l'action de SL_2 sur les paires de formes. On va maintenant se placer dans $\mathbb{C}$ et étudier de plus près les orbites de $G_{\mathbb{C}} := SL_2(\mathbb{C})$ sur l'espace $V_{\mathbb{C}} := (Sym^2\mathbb{C}^3 \otimes \mathbb{C}^2)^*$ (on note en indice l'anneau utilisé).

Remarquons que les $\lambda_{kl}^{ij}(A,B)$ sont liées par les 15 relations :

$$(**)\lambda_{kl}^{gh}(A,B)\lambda_{mn}^{ij}(A,B) = \lambda_{ij}^{gh}(A,B)\lambda_{mn}^{kl}(A,B) + \lambda_{mn}^{gh}(A,B)\lambda_{kl}^{ij}(A,B)$$

Lemme 7. *Si on se donne 15 constantes $\lambda_{kl}^{ij} \in \mathbb{C}$ vérifiant $(**)$, alors il existe une $SL_2(\mathbb{C})$-orbite $W \subset V_{\mathbb{C}}$ telle que*

$$\lambda_{kl}^{ij}(W) = \lambda_{kl}^{ij}$$

Si de plus les λ_{kl}^{ij} sont non tous nuls, alors W est unique et si les $\lambda_{kl}^{ij} \in \mathbb{Z}$, alors W contient un point entier $(A,B) \in V_{\mathbb{Z}}$.

Démonstration. Dans le cas où les λ_{kl}^{ij} sont tous nuls, alors (A,B) vérifie $\lambda_{kl}^{ij}(A,B)=0$ ssi la famille (A,B) est liée sur $\mathbb{C}$. Il existe donc une infinité d'orbites W et on peut bien sûr trouver un point entier.

Supposons donc qu'il existe $\lambda_{kl}^{ij}\neq 0$. Si (A,B) vérifie $\lambda_{kl}^{ij}(A,B)=\lambda_{kl}^{ij}$, alors sans perte de généralité, on suppose $\lambda_{12}^{11}\neq 0$ et quitte à agir via $SL_2(\mathbb{C})$ que $a_{11}=1$, $b_{11}=0$, $a_{12}=0$, $b_{12}=\lambda_{12}^{11}\neq 0$.
Pour tous k et l : $\lambda_{kl}^{11}=\begin{vmatrix} a_{11} & b_{11}\\ a_{kl} & b_{kl}\end{vmatrix}=\begin{vmatrix} 1 & 0\\ a_{kl} & b_{kl}\end{vmatrix}=b_{kl}$ et de même pour $(k,l)\neq(1,1)$ $a_{kl}=\frac{\lambda_{kl}^{12}}{b_{12}}$. On remarque alors que les relations restantes pour avoir $\lambda_{kl}^{ij}(A,B)=\lambda_{kl}^{ij}$ sont équivalentes à $(**)$. Donc on a bien une unique orbite W telle que $\lambda_{kl}^{ij}(W)=\lambda_{kl}^{ij}$.

Supposons maintenant que $\lambda_{kl}^{ij}\in\mathbb{Z}$. Alors par ce qui précède, $b_{ij}=\lambda_{12}^{11}\in\mathbb{Z}$ et $a_{ij}=\frac{\lambda_{ij}^{12}}{b_{12}}\in\frac{1}{b_{12}}\mathbb{Z}$. Donc $(b_{12}A,B)\in V_{\mathbb{Z}}$ les facteurs $\mu_{kl}^{ij}=\lambda_{kl}^{ij}(b_{12}A,B)$ sont mutliples de b_{12}. Soit $L=(b_{12}A)\mathbb{Z}+B\mathbb{Z}$ qui est un sous-réseau de $V_{\mathbb{Z}}=\mathbb{Z}^6$. Par le théorème de classification de $\mathbb{Z}$-modules, il existe des entiers n_1 et n_2 ainsi qu'une $\mathbb{Z}$-base $(e_1,e_2,...,e_6)$ de $V_{\mathbb{Z}}$ telle que (n_1e_1,n_2e_2) soit une $\mathbb{Z}$-base de L. Donc $(b_{12}A,B)$ est dans la $G_{\mathbb{Z}}$-orbite de (n_1e_1,n_2e_2), et b_{12} divise le pgcd des μ_{kl}^{ij}. Montrons que $d:=\text{pgcd}(\lambda_{kl}^{ij}(e_1,e_2))=1$. Soit $1\leq i,j\leq 3$. Notons x_{kl} et y_{kl} les coefficients en position (k,l) respectifs de e_1 et e_2. Soit M_{ij} la matrice de $V_{\mathbb{Z}}$ donc le coefficient en (k,l) est $m_{kl}=\frac{x_{ij}y_{kl}-x_{kl}y_{ij}}{d}$. Alors $M_{ij}=u_1e_1+u_2e_2+...+u_6e_6$, $u_k\in\mathbb{Z}$. Donc les coefficients de dM_{ij} dans la base $(e_1,....,e_6)$ sont divisibles par d. Le coefficient en e_1 de dM_ij est $-y_{ij}$ et celui en e_2 est x_{ij}. Donc d divise y_{ij} et x_{ij}. Comme ceci est vrai pour tout i j, cela veut dire que e_1/d et e_2/d sont à coefficients entiers, mais alors c'est une contradiction car e_1 et e_2 sont les deux premiers vecteurs d'une base de $V_{\mathbb{Z}}$.

On a donc l'existence de $(A'/n_1,B'/n_2)\in V_{\mathbb{Z}}$ qui est $SL_2(\mathbb{Q})$-équivalente à (A,B) (car si $\begin{pmatrix} r & s\\ t & u\end{pmatrix}\cdot(A',B')=(b_{12}A,B)$, alors $\begin{pmatrix} r/n_2 & s/n_1\\ n_1t & n_2u\end{pmatrix}\cdot(A',B')=(A,B)$). Donc W contient un point à coordonnées entières. □

On remarque que ce lemme permet de montrer l'existence d'une résolvante cubique pour un anneau quartique non dégénéré Q. En effet, par $(*)$, si on se donne la table de multiplication d'une base normale, on peut définir des λ_{kl}^{ij}. On vérifie que l'associativité de la loi de Q implique les 15 relations $(**)$ et donc par le lemme précédent, Q provient d'un couple (A,B) et l'existence d'une résolvante R découle du théorème précédent.

Nous allons dénombrer les résolvantes cubiques.

Proposition 27. *Soient λ_{kl}^{ij} 15 entiers non tous nuls vérifiant $(**)$ et n leur pgcd. Alors le nombre de $G_{\mathbb{Z}}$-orbites $W_{\mathbb{Z}}$ dans $V_{\mathbb{Z}}$ telles que $\lambda_{kl}^{ij}(W_{\mathbb{Z}})=\lambda_{kl}^{ij}$ est $\sum_{d|n}d$.*

Démonstration. Considérons $\mu_{kl}^{ij}=\frac{\lambda_{kl}^{ij}}{n}\in\mathbb{Z}$. Par le lemme précédent, il existe une unique $SL_2(\mathbb{C})$-orbite W telle que $\lambda_{kl}^{ij}(W)=\lambda_{kl}^{ij}$ et W contient un point entier (A,B). Soit X le $\mathbb{C}$-espace vectoriel engendré par (A,B) et $X_{\mathbb{Z}}$ l'ensemble des points à coordonnées entières de X : c'est un réseau. Alors $V:=\mathbb{Z}A+\mathbb{Z}B$ est un sous-réseau de $X_{\mathbb{Z}}$. En fait $V=X_{\mathbb{Z}}$. En effet, soit (U,V) une $\mathbb{Z}$-base de V et $M\in M_2(\mathbb{Z})$ la matrice de passage de (A,B) à (U,V). Alors $\lambda_{kl}^{ij}(A,B)=\text{Det}(M)\lambda_{kl}^{ij}(U,V)=\lambda_{kl}^{ij}(U,V)\neq 0$ donc $\text{Det}(M)=\pm1$ et $V=X_{\mathbb{Z}}$.

Si (A',B') a pour λ-invariants les λ_{kl}^{ij}, on pose $L=\mathbb{Z}A'+\mathbb{Z}B'$, qui ne dépend que de la $SL_2(\mathbb{Z})$-orbite de (A',B'). C'est un sous-réseau de $X_{\mathbb{Z}}$ car $(A',B')\in X$ (diviser les coefficients de A et B par $\sqrt{n}$). De plus L est d'indice n dans X : si P est la matrice de passage de (A',B') à (A,B), $\lambda_{kl}^{ij}(A',B')=\text{Det}(M)\lambda_{kl}^{ij}(A,B)$, d'où $n=pgcd(\lambda_{kl}^{ij}(A',B'))=\text{Det}(M)pgcd(\lambda_{kl}^{ij}(A,B))=\text{Det}(M)$.
Réciproquement, si on se donne un sous-réseau L d'indice n de $X_{\mathbb{Z}}$, on définit $W'_{\mathbb{Z}}$ comme l'ensemble des (M,N) qui engendrent L : c'est aussi la $SL_2(\mathbb{Z})$-orbite d'un point $(A',B')\in W'_{\mathbb{Z}}$. Le même calcul que précédemment implique que $\text{pgcd}(\lambda_{kl}^{ij}(A',B'))=n$.

On a ainsi une bijection entre les sous-réseaux d'indice n de $\mathbb{Z}^2$ et les orbites vérifiant $\lambda_{kl}^{ij}(W_{\mathbb{Z}}) = \lambda_{kl}^{ij}$.

Pour obtenir le résultat, il suffit de dénombrer ceux-ci selon le plus petit vecteur du réseau colinéaire à $(1,0)$. □

Comme dans le cas cubique, on va donner une CNS pour que $R^{inv}(Q) = R$.

Lemme 8. *On a $ct(Q) = pgcd(\lambda_{kl}^{ij})$ (qui ne dépend pas de la base de Q choisie pour définir (A,B)). On pose $ct(A,B) := ct(Q)$.*

Démonstration. Cela découle immédiatement de la table de multiplication (*). □

Corollaire 13. *Soit Q un anneau quartique non dégénéré, $R^{inv}(Q)$ l'anneau cubique invariant et R un anneau cubique résolvant. On a $[R : R^{inv}(Q)] = ct(Q)$. En particulier, $R^{inv}(Q) = R$ si et seulement si Q est pimitif.*

Démonstration. Soit (A,B) une paire de forme quadratique ternaire correspondant à (Q,R). Si le contenu vaut 1, les vecteurs (a_{ij}, b_{ij}) engendrent $\mathbb{Z}^2$ et comme les (a_{ij}, b_{ij}) sont dans le module engendré par l'image de $\phi_{4,3}$, on a bien $R^{inv}(Q) = R$.
Si maintenant $ct(A,B) = n$, soit Q' tel que $Q = \mathbb{Z} + nQ'$. On a $R^{inv}(Q') = R'$ qui est l'unique résolvante cubique de Q'. Comme le discriminant de Q est égal à celui de R, $[R' : R] = [Q' : Q] = n^3$ (en effet $\mathrm{Disc}(Q) = [Q' : Q]^2 \cdot \mathrm{Disc}(Q')$). En utilisant le fait que $\phi_{4,3}$ est quadratique et $R/\mathbb{Z} = \phi_{4,3}(Q/\mathbb{Z})$, on obtient $R^{inv}(Q) = \mathbb{Z} + n^2R'$, puis $[R' : R^{inv}(Q)] = n^4$. On en déduit $[R : R^{inv}(Q)] = [R' : R^{inv}(Q)]/[R' : R] = n$. □

On peut énoncer un théorème de classification qui ne fait pas intervenir de résolvante cubique.

Définition 33. *On dit que (A,B) et (A',B') (dans $(Sym^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$) sont équivalentes s'il existe $g \in SL_3(\mathbb{Z})$ et $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Q})^{\pm 1}$ (discriminant ± 1) tels que $(A,B) = (r \cdot gAg^t + s \cdot gBg^t, t \cdot gAg^t u \cdot gBg^t)$.*

Corollaire 14. *Il y a une bijection entre les classes d'isomorphisme d'anneaux quartiques non triviaux et non dégénérés (i.e. $Q \neq \mathbb{Z}^4$ en tant qu'anneau et $\mathrm{Disc}(Q) \neq 0$) et les classes d'équivalence de couples (A,B) où A et B sont linéairement indépendantes sur $\mathbb{Q}$.*

Démonstration. On a vu que Q (orienté) était déterminé par les λ_{kl}^{ij} et que réciproquement en définissant les λ_{kl}^{ij} par (*), en utilisant le lemme 8 on peut trouver un couple (A,B) tel que $\lambda_{kl}^{ij}(A,B) = \lambda_{kl}^{ij}$. Il suffit de vérifier que les λ_{kl}^{ij} déterminent entièrement (A,B) à $GL_2^{\pm 1}(\mathbb{Q})$-équivalence près. Cela découle de la même démonstration que le lemme 7 (mais sur $\mathbb{Q}$ et pas sur $\mathbb{C}$). Si on ne tient plus compte de l'orientation de Q et R, on a bien la bijection voulue. □

5. Appendice

On suppose connu les notions de bases sur les anneaux noethériens (en particulier la décomposition primaire) et sur la localisation.

5.1. **Anneaux d'entiers.**

Un anneau d'entier est un exemple important d'anneau de rang k (cf au début du mémoire).

Définition 34. *Soit A un anneau et B une A-algèbre. On dit qu'un élément $x \in B$ est entier sur A s'il existe un polynôme unitaire $P \in A[X]$ tel que $P(x) = 0$.*

Proposition 28. *Soit S un anneau de rang k (cf début du mémoire). Alors tout élément x de S est entier sur $\mathbb{Z}$.*

Démonstration. Soit m_x l'endomorphisme de multiplication par x et M_x sa matrice dans une $\mathbb{Z}$-base de S. Alors par le théorème de Cayley-Hamilton le polynôme caractéristique de M_x annule x et c'est un polynôme unitaire à coefficients dans $\mathbb{Z}$. □

Définition 35. *Soit A un anneau. On dit que A est intégralement clos si A est intègre et que $\{x \in Frac(A), x$ entier sur $A\} = A$.*

Proposition 29. *Un anneau factoriel est intégralement clos.*

Démonstration. Soit A un anneau factoriel et $K = Frac(A)$. Soit $x = \frac{a}{b} \in K$, où $a, b, \in A$ et $pgcd(a, b) = 1$. Si x entier sur A, il existe a_0, ..., a_{n-1} dans A tels que $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$. Alors $a^n + ba_{n-1}a^{n-1} + ... + b^n a_0 = 0$ et b divise a^n, impossible car $pgcd(a, b) = 1$. □

Définition 36. *Soit $x \in \mathbb{C}$. On dit que x est un entier algébrique si c'est un entier sur $\mathbb{Z}$.*

Proposition 30. *Si x et y sont des entiers algébriques, alors $x - y$ et xy sont des entiers algébriques.*

Démonstration. Cf [10] Chap. II, Cor. 1. □

Proposition 31. *Un élément $x \in \mathbb{C}$ est un entier algébrique ssi son polynôme minimal sur $\mathbb{Q}$ est à coefficients entiers.*

Démonstration. Si x est un entier algébrique, il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$. Soit $P_x \in \mathbb{Q}[X]$ le polynôme minimal de x sur $\mathbb{Q}$. Alors P_x divise P dans $\mathbb{Q}$, donc les racines de P_x sont des entiers algébriques, et par conséquent les coefficients de P_x sont des entiers algébriques (par la proposition précédente). Or un entier algébrique rationnel est un entier relatif (car $\mathbb{Z}$ est factoriel donc intégralement clos). □

Définition 37. *Soit K une extension finie de $\mathbb{Q}$ (on dit que K est un corps de nombres). On appelle anneau des entiers de K, noté $\mathcal{O}_K$, l'ensemble des entiers algébriques de K. Un sous anneau de $\mathcal{O}_K$ contenant une $\mathbb{Q}$-base de K est appelé un ordre de K.*

On utilisera dans la suite les notions de trace, polynôme caractéristique et discriminant qui ont déjà été définies et étudiées au début du mémoire.

Proposition 32. *Soit K un corps de nombre. Il existe $x \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(x)$.*

Démonstration. Par la théorème de l'élément primitif, on peut trouver $x \in K$ tel que $K = \mathbb{Q}(x)$. On écrit $a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$ pour $a_i \in \mathbb{Z}$ et $n = [K : \mathbb{Q}]$. On multiplie cette égalité par a_n^{n-1} pour obtenir que $y := a_n x$ est un entier algébrique, avec $K = \mathbb{Q}(y)$. □

Théorème 18. *Structure additive de $\mathcal{O}_K$ Soit $n = [K : \mathbb{Q}]$. Il existe $(e_1, ..., e_n)$ une $\mathbb{Q}$-base de K tel que $\mathcal{O}_K = \mathbb{Z}e_1 + ... + \mathbb{Z}e_n$.*

Démonstration. Soit $x \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(x)$. On notre $Tr(.)$ la trace sur $\mathbb{Z}[x]$. On peut étendre $Tr(.)$ à K de manière évidente.
Si $y \in \mathcal{O}_K$, il existe des rationnels a_0, ..., a_{n-1} tels que $y = a_0 + a_1 x + ... + a_{n-1}x^{n-1}$. Alors si $0 \leq i \leq n-1$, $Tr(yx^i) = \sum_{j=0}^{n-1} a_j Tr(x^j x^i)$. Or la matrice $(Tr(x^i x^j))$ est de déterminant $\mathrm{Disc}(1, x, ..., x^{n-1}) \neq 0$ (cf les calculs de discriminants au début du mémoire). Donc en inversant le système de n équations linéaires en les a_i, on voit que $da_i \in \mathbb{Z}$ et par conséquent $\mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[x]$. Donc $\mathcal{O}_K$ est contenu dans un $\mathbb{Z}$-module de rang n et est donc un $\mathbb{Z}$-module libre de rang n (le rang est n car par exemple $\mathbb{Z}[x] \subset \mathcal{O}_K$). □

Corollaire 15. *Soit A un ordre de K et I un idéal non nul de A. Alors I est un $\mathbb{Z}$-module libre de rang n.*

Démonstration. La seule chose à voir est que I contient une $\mathbb{Q}$-base de K. C'est évident car si $x \in I - \{0\}$, alors $x \cdot A \subset I$ et A contient une $\mathbb{Q}$-base de K par définition. □

Corollaire 16. *Si I est un idéal d'un ordre A de K, alors $Card(A/I)$ est fini (et est au signe près $N(I)$ par définition).*

Démonstration. Il suffit d'utiliser le théorème de la base adaptée pour les $\mathbb{Z}$-modules : si $(d_1e_1, ..., d_ne_n)$ et $(e_1, ..., e_n)$ sont des $\mathbb{Z}$-bases respectives de I et A (avec d_1, ..., d_n entiers naturels non nuls), alors $Card(A/I) = d_1...d_n$. □

Une autre propriété important de $\mathcal{O}_K$ est que c'est un anneau de Dedekind, comme nous le verrons dans la section suivante.

5.2. **Anneaux de Dedekind.** On va définir et donner quelques propriétés importantes des anneaux de Dedekind.

Définition 38. *Un anneau de Dedekind est un anneau noethérien, intégralement clos, et de dimension 1 (i.e. tout idéal premier non nul est maximal).*

Nous allons voir que la propriété d'être un anneau de Dedekind est une propriété locale. Pour cela nous allons introduire les anneaux de valuation discrète qui vont s'avérer être les anneaux de Dedekind locaux.

Définition 39. *Un anneau de valuation discrète est un anneau local (i.e. avec un unique idéal maximal) principal qui n'est pas un corps.*

Soit A un anneau de valuation discrète. Notons $\mathfrak{m}$ l'unique idéal maximal. Comme A est principal, il existe un élément irréductible π (unique à association près) tel que $\mathfrak{m} = \pi$. De plus tout élément irréductible est associé à π car l'anneau est principal et n'a qu'un idéal maximal. Comme A est factoriel, tout élément $x \neq 0$ est associé à π^n, pour un unique n (et tout idéal non nul est de la forme $\mathfrak{m}^n$ pour un unique n). On pose alors $v(x) = n$, appelée valuation de x. On vérifie immédiatement les propriétés suivantes :

$$v(xy) = v(x) + v(y) \tag{4}$$

$$v(x + y) \geq v(x) + v(y) \tag{5}$$

Si $\frac{x}{y} \in K := Frac(A)$, on pose $v(\frac{x}{y}) = v(x) - v(y)$, ce qui ne dépend pas de l'écriture choisie pour $\frac{x}{y}$, par (1). On a une sorte de réciproque à ceci.

Proposition 33. *Soit K un corps et $v : K^* \to \mathbb{Z}$ est surjective vérifiant les propriétés (1) et (2) ci-dessus, alors $A := \{0\} \cap \{x \in K^*, v(x) \geq 0\}$ est un anneau de valuation discrète, dont l'idéal maximal est $\mathfrak{m} = \{0\} \cup \{x \in K^*, v(x) > 0\}$.*

Démonstration. Le fait que A est un anneau découle immédiatement des propriétés (1) et (2).

Soit I un idéal de A. Soit $a \in I$ tel que $v(a)$ est minimal et $b \in I$. Alors $v(b/a) = v(b) - v(a) \geq 0$ et donc $b/a \in A$ et $b = (b/a) \cdot a \in I$. Donc $I = (a)$ est bien principal. Si $x \in A$ n'est pas inversible, alors $-v(x) = v(1/x) < 0$ et par conséquent $v(x) \geq 1$. Comme v est surjective, on peut trouver $\pi \in A$ tel que $v(\pi) = 1$. Si $x \in A$ n'est pas inversible, on a $v(x/\pi) \geq 0$ et par conséquent $x \in (\pi)$: (π) est l'unique idéal maximal. □

Proposition 34. *A est un anneau de valuation discrète ssi A est un anneau de Dedekind local.*

Démonstration. Si A est un anneau de valuation discrète, alors A est clairement de dimension 1 et noethérien. Il est intégralement clos car A est intègre et factoriel (car principal).

Réciproquement, soit A un anneau de Dedekind local. Soit $\mathfrak{m}$ sont unique idéal maximal et $\pi \in \mathfrak{m} - \mathfrak{m}^2$. Comme A est de dimension 1 et est noethérien, le seul idéal premier contenant π est $\mathfrak{m}$ et on sait que (cf décomposition primaire dans un anneau noethérien) $\mathfrak{m}$ est associé à (π) : $\exists a \in A$, $\mathfrak{m} = \{x \in A, ax \in (\pi)\}$.

Alors $\frac{a}{\pi}\mathfrak{m} \subset A$ (et $\frac{a}{\pi} \in Frac(A)$). Si $\frac{a}{\pi}\mathfrak{m} \subset A$, comme A est noethérien, $\mathfrak{m}$ est de type fini et par une proposition de la section « Anneaux d'entiers », $\frac{a}{\pi}$ est entier sur A. Comme A est intégralement clos, $\frac{a}{\pi} \in A$, absurde car alors $\mathfrak{m} = A$. L'anneau A étant local, tout idéal strict de A est contenu dans $\mathfrak{m}$ et par conséquent $\frac{a}{\pi}\mathfrak{m} = A$. On a alors que $\mathfrak{m} = (\frac{\pi}{a})$ est principal. L'anneau A est local, donc par le théorème d'intersection de Krull, $\cap_{n\geq 1}\mathfrak{m}^n = 0$. Pour tout $x \in A - \{0\}$, on peut alors poser $v(x) = max\{n \geq 0, x \in \mathfrak{m}^n\}$, qui vérifie trivialement (1) et (2). De plus v se prolonge sur $Frac(A) - \{0\}$ et par la proposition précédente, A est un anneau de valuation discrète. □

On va maintenant prouver que la propriété « être de Dedekind » est une propriété locale. Rappelons que si A est un anneau, que $\mathfrak{p}$ est un idéal premier et I est un idéal de A, on pose $I_\mathfrak{p} := I \otimes_A A_\mathfrak{p}$ (appelé I localisé $\mathfrak{p}$), où $A_\mathfrak{p}$ est le localisé de A en $S = A - \mathfrak{p}$ (pour plus de détails sur la localisation, cf [5], Chap II, Localization).

Proposition 35. *Soit A un anneau. Alors A est de Dedekind $\Leftrightarrow \forall \mathfrak{p} \in Spec(A)$, $A_\mathfrak{p}$ est de Dedekind $\Leftrightarrow \forall \mathfrak{p} \in Spec(A)$, $A_\mathfrak{p}$ est un anneau de valuation discrète.*

Démonstration. La deuxième équivalence est exactement la proposition précédente. Pour montrer la première équivalence, commençons par montrer un petit lemme.

Lemme 9. *Soit A un anneau intègre noethérien. Alors A est intégralement clos ssi pour tout $\mathfrak{p}$ premier, $A_\mathfrak{p}$ est intégralement clos.*

Démonstration. On a $K := Frac(A) = Frac(A_\mathfrak{p})$ pour tout $\mathfrak{p}$ premier (évident). Supposons que A est intégralement clos et que $\mathfrak{p}$ est premier. Soit $x \in K$ un entier sur $A_\mathfrak{p}$: $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$, où $a_i \in A_\mathfrak{p}$. On peut écrire $a_i = \frac{b_i}{s}$ où $b_i \in A$ et $s \in A - \mathfrak{p}$. Alors $(sx)^n + sb_{n-1}(sx)^{n-1} + ... + s^{n-1}b_0 = 0$. Comme A est intégralement clos, $sx \in A$ et $x \in A_\mathfrak{p}$. Réciproquement, supposons que pour tout $\mathfrak{p}$ premier, $A_\mathfrak{p}$ est intégralement clos. Soit $x \in K$ entier sur A. Alors x entier sur $A_\mathfrak{p}$ pour tout $\mathfrak{p} \in Spec(A)$. Donc $x \in \cap_{\mathfrak{p}\in Spec(A)}A_\mathfrak{p}$ (où les intersections sont prises dans A). Or $\cap_{\mathfrak{p}\in Spec(A)}A_\mathfrak{p} = A$ car A est intègre. □

Si A est de Dedekind, alors par le lemme, pour tout $\mathfrak{p}$, $A_\mathfrak{p}$ est intégralement clos. Si on a une chaîne d'idéaux premiers $\mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_n$ de $A_\mathfrak{p}$ alors on a une chaîne d'idéaux premiers $\mathfrak{p}_1 \cap A \subsetneq ... \subsetneq \mathfrak{p}_n \cap A$ car $\mathfrak{p}_i = A_\mathfrak{p} \cdot (\mathfrak{p}_i \cap A)$. Donc $dim(A_\mathfrak{p}) = 1$. Par le même argument $A_\mathfrak{p}$ est noethérien.

Réciproquement si pour tout $\mathfrak{p}$, $A_\mathfrak{p}$ est de Dedekind, alors par le lemme, A est intégralement clos. Si $\mathfrak{p}$ est un idéal premier de A, soit $\mathfrak{m}$ un idéal maximal de A contenant $\mathfrak{p}$. Alors $A_\mathfrak{m}$ est de Dedekind et $\mathfrak{p}\cdot A_\mathfrak{m}$ est un idéal premier (car $\mathfrak{p}\cap(A-\mathfrak{m}) = \emptyset$) donc maximal (donc égal $\mathfrak{m}$), d'où $\mathfrak{p} = (\mathfrak{p}\cdot A_\mathfrak{m})\cap A = (\mathfrak{m}\cdot A_\mathfrak{m})\cap A = \mathfrak{m}$ (rappelons que si I est un idéal premier contenu dans $\mathfrak{m}$, alors $I = (I \cdot A_\mathfrak{m}) \cap A$). □

On peut maintenant prouver un théorème important concernant l'arithmétique des anneaux de Dedekind.

Théorème 19. *Dans un anneau de Dedekind, tout idéal s'écrit de manière unique comme produit d'idéaux premiers (donc maximaux).*

Démonstration. Soit A un anneau de Dedekind. Soit $\mathfrak{q}$ un idéal $\mathfrak{m}$-primaire où $\mathfrak{m}$ est un idéal maximal de A. Par les propositions précédentes, $\mathfrak{q}A_\mathfrak{m} = \mathfrak{m}^n A_\mathfrak{m}$ pour un $n > 0$. Ces deux idéaux sont $\mathfrak{m}$-primaires et on peut donc écrire : $\mathfrak{q} = \mathfrak{q}A_\mathfrak{m} \cap A = \mathfrak{m}^n A_\mathfrak{m} \cap A = \mathfrak{m}^n$. Comme A est noethérien, si I est un idéal de A, il existe une décomposition primaire de I : $I = \cap\mathfrak{q}_i$ où q_i est $\mathfrak{m}_i$-primaire. Par ce qu'on vient de voir, $\mathfrak{q}_i = \mathfrak{m}_i^{n_i}$, donc $I = \cap\mathfrak{m}_i^{n_i} = \prod \mathfrak{m}_i^{n_i}$. La dernière égalité est le lemme chinois car si $i \neq j$, $\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j} = A$ (passer au radical).

L'unicité découle de l'unicité d'une décomposition primaire minimale dans le cas où tous les idéaux premiers au dessus de I sont minimaux (ce qui est le cas dans un Dedekind). □

Théorème 20. *Si K est un corps de nombre, $\mathcal{O}_K$ est un anneau de Dedekind. De plus $\mathcal{O}_K$ est le seul ordre de K qui est un anneau de Dedekind.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors $\mathcal{O}_K/\mathfrak{p}$ est un anneau intègre et fini (cf section « Anneaux d'entiers »). Or un anneau fini intègre est un corps (considérer $x \in A - \{0\}$ et l'endormorphisme de multiplication par x qui est injectif donc bijectif, ce qui implique que x est inversible). Donc $\mathfrak{p}$ est maximal.

Soit I un idéal de $\mathcal{O}_K$. Comme A/I est fini, il n'y a qu'un nombre fini d'idéaux contenant I et A est noethérien.

Montrons pour finir que $\mathcal{O}_K$ est intégralement clos. Soit x un entier sur $\mathcal{O}_K$ et $P \in \mathcal{O}_K[X]$ tel que $P(x) = 0$. Soit M l'anneau engendré par x et les coefficients de $\mathcal{O}_K$: c'est un $\mathbb{Z}$-module de type fini. En notant m_x l'endomorphisme de multiplication par x dans M et en utilisant le théorème de Cayley-Hamilton, il existe $Q \in \mathbb{Z}[X]$ tel que $Q(x) = 0$, d'où $x \in \mathcal{O}_K$.

Pour la dernière assertion, en fait ce qui manque à un ordre quelconque pour être de Dedekind est la propriété « intégralement clos » : on vérifie immédiatement que tout ordre est noethérien et de dimension 1. Cependant si A est un ordre strict (i.e. $A \subsetneq \mathcal{O}_K$), alors il existe $x \in \mathcal{O}_K - A$ qui est entier sur $\mathbb{Z}$, donc sur A, mais n'est pas dans A. □

Dans le mémoire, nous avons utilisé le fait que dans le cas d'un anneau de Dedekind, les idéaux fractionnaires sont inversibles et la norme est alors multiplicative. Pour mieux comprendre ce que signifie l'inversibilité des idéaux, nous allons travailler dans le cadre plus général des modules projectifs.

5.3. **Modules projectifs, idéaux inversibles.**

Définition 40. *Soit A un anneau commutatif. On dit qu'un module P est projectif si l'une des trois propriétés équivalentes suivantes est vérifiée :*
(1) Si M et N sont deux A-modules et $g : M \to N$ est un morphisme surjectif, alors pour tout morphisme $f : P \to N$, il existe un morphisme $h : P \to M$ tel que $f = gh$.
(2)Il existe un A-module M tel que $P \oplus M$ est un A-module libre.
(3)Toute suite exacte $0 \to M' \to M'' \to P \to 0$ est scindée.
(4)Le foncteur $M \to Hom_A(P, M)$ est exact (i.e. ce foncteur préserve les suites exactes).

Démonstration. Cf [9] Partie I, Chap III, Paragraphe 4. □

On a une caractérisation sympathique des modules projectifs de type fini dans le cas où A est noethérien (et c'est bien le cas dans le mémoire).

Proposition 36. *Soit A un anneau noethérien. Les propriétés suivantes sont équivalentes.*
(1) P est un A-module projectif de type fini.
(2)Pour tout idéal maximal $\mathfrak{m}$ de A, $P_\mathfrak{m}$ est un $A_\mathfrak{m}$-module libre.
(3)Pour tout idéal maximal $\mathfrak{p}$ de A, $P_\mathfrak{p}$ est un $A_\mathfrak{p}$-module libre.
(4)Il existe une famille $(f_1, ..., f_n)$ d'éléments de A telle que $Af_1 + ... + Af_n = A$ et pour tout $1 \leq i \leq n$, P_{f_i} est un A_{f_i} module libre (où l'indice f_i signifie qu'on localise par rapport à la partie $S = \{f_i^n, n \geq 0\}$). On dit que P est localement libre.

Démonstration. Cf [5] Chap. II, Paragraphe 5.3, Théorème 1. □

Autrement dit dans le cas d'un module de type fini sur un anneau noethérien, la projectivité est une propriété locale qui est équivalente localement au fait d'être libre.

Définition 41. *Si P est un module projectif de type fini sur un anneau noethérien A, pour $\mathfrak{p} \in Spec(A)$, on définit $rg_\mathfrak{p}(P)$ comme le rang du $A_\mathfrak{p}$-module libre $P_\mathfrak{p}$.*

Proposition 37. *Si A est intègre, alors $rg : \mathfrak{p} \to rg_\mathfrak{p}(P)$ est constante sur $Spec(A)$. On pose alors $rg(P) = rg_\mathfrak{p}(P)$ pour tout $\mathfrak{p}$.*

Démonstration. La fonction rg est à valeurs entière et localement constante sur l'espace topologique $Spec(A)$, car par (4) de la proposition précédente, si $\mathfrak{p} \in Spec(A)$, il existe i tel que $f_i \notin \mathfrak{p}$ (sinon $\mathfrak{p} = A$ n'est pas premier) et P_{f_i} est libre. Alors $P_{\mathfrak{p}} = P_{f_i} \otimes_{A_{f_i}} A_{\mathfrak{p}}$ est de même rang que P_{f_i}. Autrement dit rg est constante sur l'ouvert $D_{f_i} = \{\mathfrak{p} \in Spec(A), f_i \notin \mathfrak{p}\}$. Or $Spec(A)$ est connexe car A est intègre, donc rg est constante sur $Spec(A)$. □

On va voir le lien entre idéaux inversibles et modules projectifs, ce qui permettra de bien mieux comprendre l'inversibilité des idéaux. On rappelle d'abord une définition.

Définition 42. *Soit A un anneau de rank k (i.e. libre de rang k en tant que $\mathbb{Z}$-module). On pose $K = A \otimes_{\mathbb{Z}} \mathbb{Q}$ (c'est la $\mathbb{Q}$-algèbre associée à A).*

On dit qu'un A-module I est un idéal fractionnaire de A si $I \subset K$ et si I est un $\mathbb{Z}$-module de rank k. De manière équivalente, I est un idéal fractionnaire de A si il existe $d \in \mathbb{N}^*$ tel que $d \cdot I \subset A$.

On dit que I est inversible si il existe un idéal fractionnaire J tel que $I \cdot J = A$.

Proposition 38. *Soit A un anneau noethérien et I un idéal fractionnaire de A. Alors I est projectif ssi I est inversible.*

Démonstration. Supposons d'abord que I est inversible. Il existe J tel que $I \cdot J = A$. Autrement dit il existe a_1, ..., a_n dans A et b_1, ..., b_n dans B tels que $a_1b_1 + ... + a_nb_n = 1$. Montrons que I est projectif. Soit $f : M \to I$ un morphisme surjectif où M est un A-module. On doit construire $g : I \to M$ tel que $fg = Id$. Comme f est surjectif, il existe $e_k \in M$ tel que $f(e_k) = a_k$. On pose $g(x) = (xb_1)e_1 + ... + (xb_n)e_n$. On remarque que si $x \in I$, alors $xb_k \in I \cdot J = A$. Alors $f(g(x)) = xb_1f(e_1) + ... + xb_nf(e_n) = x(a_1b_1 + ... + a_nb_n) = x$.

Réciproquement, supposons que I est projectif et que $I \subset A$ (quitte à multiplier I par un entier). Comme I est de type fini, il existe $n \geq 1$ et $f : A^n \to I$ un morphisme surjectif. On note $(e_1, ..., e_n)$ une A-base de A^n. Soit g un inverse à droite de f (possible car I est projectif). On peut alors écrire de manière unique $g(x) = g_1(x)e_1 + ... + g_n(x)e_n$, pour tout $x \in I$, où $g_i : I \to A$ est un morphisme. On sait que $N(I) \in I$ car dans A/I, $\overline{N(I)} = \overline{0}$. On pose alors $a = N(I) \in I \cap \mathbb{Z}$ qui est inversible dans K. Pour tout $1 \leq i \leq n$, $g_i(ax) = ag_i(x) = xg_i(a)$, donc $g_i(x) = xb_i$ où $b_i = a^{-1}g_i(a)$. Soit $J = b_1A + ... + b_nA$. Pour tout $x \in I$, $xb_i = g_i(x) \in A$, donc $I \cdot J \subset A$. L'égalité $f(g(x)) = x$ implique $x = x(f(e_1)b_1 + ... + f(e_n)b_n)$. Donc $I \cdot J = A$. □

Corollaire 17. *Soit A un anneau commutatif intègre noethérien. Alors A est de Dedekind ssi tout idéal fractionnaire est inversible (de rang 1).*

Démonstration. Si A est de Dedekind, alors pour tout $\mathfrak{p} \in A$, $A_{\mathfrak{p}}$ est principal (car c'est un anneau de valuation discrète), donc si I est un idéal de A, $I_{\mathfrak{p}}$ est principal donc libre. Donc I est projectif donc inversible.

Réciproquement, supposons que tous les idéaux de A sont inversibles, donc projectifs. Alors si $\mathfrak{p} \in Spec(A)$ et I est un idéal non nul de A, $I_{\mathfrak{p}}$ est libre de rang 1 donc principal. Donc $A_{\mathfrak{p}}$ est un anneau local principal (qui n'est pas un corps car les éléments de $\mathfrak{p}$ ne sont pas inversibles), i.e. un anneau de Dedekind local. Donc A est de Dedekind (c'est une propriété locale). □

5.4. **Norme d'un idéal.** Soit S un anneau de rang k (i.e. isomorphe à $\mathbb{Z}^k$ en tant que $\mathbb{Z}$-module). On va simplifier un peu la définition de la norme d'un idéal $I \subset S$ en oubliant l'orientation : on pose $N(I) = Card(S/I) > 0$ (les résultats restent valables de manière évidente).

Proposition 39. *Soient I et J des idéaux fractionnaires de S. Si I est projectif, (c'est à dire inversible par la section précédente), alors $N(IJ) = N(I)N(J)$.*

Démonstration. On aura besoin de quelques propriétés sur les modules projectifs

Lemme 10. *Soit M un S-module projectif. Si $N \subset N'$ sont des S-modules alors*

$$(M \otimes_S N')/(M \otimes_S N) \simeq M \otimes_S (N'/N)$$

Démonstration. On a une suite exacte de S-modules

$$0 \to N \to N' \to N'/N \to 0$$

Comme M est projectif, M est plat et donc on peut tensoriser cette suite exacte par M pour obtenir le résultat. □

Lemme 11. *Soit M un S-module projectif et J un idéal de S. Alors :*

$$M \otimes_S J \simeq J \cdot M$$

Démonstration. On a une injection de J dans S qu'on peut tensoriel avec M et donc $M \otimes_S J$ peut être vu comme un sous-module de $M \otimes_S S$. Donc si $\phi : M \otimes_S S \to M$ est telle que $\phi(x \otimes_S 1) = x$, alors ϕ restreinte à $M \otimes_S J$ est injective car les éléments de $M \otimes_S J$ sont de la forme $x \otimes_S 1$ (dans l'espace $M \otimes_S S$). D'où le résultat : ϕ induit un isomorphisme entre $M \otimes_S J$ et son image $J \cdot M$. □

Quitte à multiplier I et J par des éléments de $K := S \otimes_{\mathbb{Z}} \mathbb{Q}$, on peut supposer que I et J sont des idéaux de S.

On a une chaîne de S-modules $J = J_1 \subset J_2 \subset ... \subset J_n = S$ tels que J_k/J_{k+1} est un S-module simple (Théorème de Jordan-Hölder), donc il existe $\mathfrak{m}_k$ idéal maximal tel que $J_k/J_{k+1} = S/\mathfrak{m}_k$. On a alors $0 = I/IS \subset I/IJ_{n-1} \subset ... \subset I/IJ_1 = I/IJ$ et les quotients sont $IJ_k/IJ_{k+1} \simeq I \otimes_S (J_k/J_{k+1}) = I \otimes_S (S/\mathfrak{m}_k)$ (car I étant projectif, $IJ_k \simeq I \otimes_S J_k$ par lemme 2 et on utilise le lemme 1). Montrons que $I \otimes_S (S/\mathfrak{m}_k)$ est un $S/\mathfrak{m}_k$ sev de dimension 1. En effet, par les propriétés des idéaux inversibles, $I_{\mathfrak{m}_k}$ est libre de rang 1, et $I \otimes_S (S/\mathfrak{m}_k)$ est isomorphe à $I_{\mathfrak{m}_k}/(\mathfrak{m}_k I_{\mathfrak{m}_k})$ qui est un $S_{\mathfrak{m}_k}/(\mathfrak{m}_k S_{\mathfrak{m}_k}) = S/\mathfrak{m}_k$ ev de dimension 1. En passant au cardinal dans les deux chaînes on a le résultat. □

Corollaire 18. *Si A est un anneau de Dedekind (en particulier si $A = \mathcal{O}_K$ où K est un corps de nombre), la norme est multiplicative.*

5.5. **Classes d'idéaux.** Soit K un corps de nombre et A un ordre de K. On note $Cl(A)$ l'ensemble des idéaux fractionnaires de A modulo la relation d'équivalence $I \sim J$ s'il existe $x \in K$ tel que $J = xI$.

Proposition 40. *La multiplication des idéaux est compatible avec la relation d'équivalence précédente et munit $Cl(A)$ d'une structure de monoide dont l'élément neutre est la classe de A (qui est celle des idéaux principaux).*

En fait $Cl(A)$ mesure le « défaut de principalité » de A car A est principal ssi $Cl(A)$ est trivial, et plus généralement un idéal est principal ssi sa classe est celle de A (l'élément neutre).

On voit que $Cl(A)$ (muni du produit des idéaux) est un groupe (abélien) ssi tous les idéaux fractionnaires de A sont inversibles ssi A est un anneau de Dedekind ssi $A = \mathcal{O}_K$. On a le résultat général suivant.

Théorème 21. *L'ensemble $Cl(A)$ est fini.*

Démonstration. Pour une preuve dans le cas où $A = \mathcal{O}_K$, cf [10] Chap. 4, paragraphe 3, Théorème 2.

□

Notons que nous n'avons pas besoin de ce résultat dans le mémoire, et qu'on le montre indirectement pour le cas quadratique et cubique.

Références

[1] Manjul Bhargava. Higher composition laws 1 : A new view on gauss compostion and quadratic generalizations.
[2] Manjul Bhargava. Higher composition laws 2 : On cubic analogues of gauss composition.
[3] Manjul Bhargava. Higher composition laws 3 : The parametrization of quartic rings.
[4] N. Bourbaki. *Algèbre, Chapitre 5*.
[5] N. Bourbaki. *Commutative Algebra*.
[6] B. N. Delone and D. K. Faddeev. The theory of irrationalities of the third degree.
[7] M. Sato et T. Kimura. A classification of irreducible prehomogeneous vector spaces and their relative invariants.
[8] C.F. Gauss. *Disquisitiones Arithmeticae*.
[9] Serge Lang. *Algebra*.
[10] Pierre Samuel. *Théorie algébrique des nombres*.
[11] Jean-Pierre Serre. Modules projectifs et espaces fibrés à fibre vectorielle.
[12] D. J. Wright and A. Yukie. Prehomogeneous vector spaces and field extensions.