Sur la conjecture de Frobenius relative aux solutions de l'équation de Markoff (Première partie)

Serge Perrine

Sur la conjecture de Frobenius relative aux solutions de l'équation de Markoff (Première partie)

Serge Perrine
5 Rue du Bon Pasteur - 57070 Metz
serge.perrine@wanadoo.fr

September 2014

Abstract

Le texte présenté ici a pour point de départ une revue détaillée de deux articles de Norbert Riedel disponibles sur le serveur arXiv (dernière référence arXiv:1208.4032 v8 [mathNT] 12 Jan 2014). Dans le présent travail nous laissons de côté la formalisation de la théorie de Markoff par le calcul quantique, ce qui constitue l'apport le plus original des articles cités. Nous montrons comment ce formalisme peut être construit de façon directe sur un $\mathbb{Z}-$module de rang 3. Nous considérons ensuite des arguments arithmétiques. Nous les positionnons sur un arbre adapté à l'étude de la conjecture de Frobenius, en cherchant à dégager ce qui est essentiel dans les calculs. Après une nouvelle démonstration de cette conjecture pour les cas primaire ou double de primaire déjà connus, nous concluons sur ce que pourrait être la signification de cette conjecture dans le cas général.

Mots clés : Markoff equation, Frobenius conjecture, Riedel tree.
[AMS classification 2000] :
Primary :11D25, 11J06, 15A36
Secondary : 20H15, 57R56, 57R22

Contents

1. Introduction

Le présent texte a été élaboré à partir d'une revue de la prépublication [46] de Norbert Riedel, intitulée "**Markoff equation and nilpotent matrices**" et déposée dans le serveur arXiv de Los Alamos (de v1 10 Sep 2007 à v6 28 Jul 2009). Cette revue a été poursuivie sur les plus récents travaux de Reidel, jusqu'à la version v8 (12 Jan 2014) de [47] intitulée **"On the Markoff equation",** en fait une nouvelle version de l'article précédent. L'intérêt de la prépublication [46] était qu'elle annonçait conclure une conjecture de Frobenius non résolue depuis un siècle [1], et pourtant essentielle pour assurer la présentation donnée dans [25] ou [13] de la théorie de Markoff relative aux solutions en nombres entiers strictement positifs de l'équation :

$$\alpha^2 + \beta^2 + \gamma^2 = 3\alpha\beta\gamma. \tag{1.1}$$

Cette conjecture énonce que pour tout triplet solution (α, β, γ) tel que :

$$\alpha \leq \gamma,\ \beta \leq \gamma,$$

la valeur γ dominante détermine de façon unique la paire $\{\alpha, \beta\}$, ou encore si l'on impose $\alpha \leq \beta$ que le couple (α, β) est unique. Dans les travaux originaux de Markoff [36], cette question n'est pas posée, car le recours aux fractions continues donne directement tous les résultats. C'est dans la présentation de ces travaux remaniée par Frobenius [25] en 1913, et qui met en avant les formes quadratiques, que la conjecture apparait pour la première fois. La plupart des travaux modernes sur la théorie de Markoff sont basés sur la présentation de Frobenius synthétisée par J. W. S. Cassels en 1957 et mentionnent le besoin que cette conjecture soit vraie ([13] p. 33 ou [21] p. 11). L'enjeu est de savoir si l'arbre des solutions de l'équation (1.1) est un arbre binaire, comme l'indique R. K. Guy dans son ouvrage sur les problèmes non résolus en théorie des nombres [28]. Selon [59], [60], [7], le problème restait ouvert en 2008. Depuis 1913, différentes démonstrations fausses ou incomplètes en ont été données, mais au printemps 2013 aucune n'éteignait la question [1]. Des approches heuristiques ont été développées (voir [8], [49], [61]), des résultats très partiels ont été démontrés (voir [4], [11], [34], [62], [63], [54]), et même des significations géométriques profondes en ont été données (voir [52], [51], [6], [38]). L'ouvrage [1] édité pour le centenaire de la conjecture synthétise ces travaux, montre cependant pour le moment aucun argument convainquant ne semble avoir été trouvé pour conclure. Dans [47] Riedel déplace la question sur un groupe de Heisenberg ([31]) de matrices 3×3. On se démarque dans le présent article des travaux de Riedel en limitant nos réflexions à l'utilisation de

moyens classiques de théorie des nombres. Notons ici pour être complet que si l'on déforme légèrement l'équation (1.1) en :

$$\alpha^2 + \beta^2 + \gamma^2 = 3\alpha\beta\gamma + 2\gamma,$$

on peut trouver une infinité de triplets de solutions correspondant à une même valeur dominante, parmi lesquels l'exemple évident ([40] p. 76) :

$$(1, 27, 73), \qquad (3, 8, 73).$$

La conjecture de Frobenius est donc bien particulière à l'équation de Markoff.

2. Le choix de l'arbre des triplets

Le but du présent paragraphe est de préciser l'arbre sur lequel nous décidons de travailler, qui est différent de celui utilisé par Norbert Riedel dans ses articles [46] et [47].

2.1. Rappels préliminaires sur les arbres de solutions

A une multiplication par un facteur 3 près ($a = 3\alpha, b = 3\beta, c = 3\gamma$), on peut ramener la résolution de la classique équation de Markoff (1.1) à celle de la recherche de nombres entiers strictement positifs a, b, et c vérifiant :

$$a^2 + b^2 + c^2 = abc. \tag{2.1}$$

Un **triplet de Markoff** est un triplet d'entiers strictement positifs (a, b, c) solution de cette équation (2.1). Classiquement on organise ces solutions en un arbre ayant pour sommets un sous ensemble de l'ensemble des triplets de Markoff, et pour les arêtes on indique comment on passe du triplet origine d'une telle arête à son triplet extrémité. Mais il y a plusieurs façons de procéder pour mettre en évidence un tel arbre. Dans les travaux [40], on considère toutes les solutions possibles en nombres entiers strictement positifs de (2.1), c'est à dire tous les triplets de Markoff, disant que l'on considére l'**arbre complet**. Les arêtes de cet arbre sont définies au moyen de trois transformations involutives notées, bien que l'opération $(.)^*$ soit équivoque :

$$\begin{aligned} X &: (a, b, c) \longrightarrow (bc - a, b, c) = (a^*, b, c), \\ Y &: (a, b, c) \longrightarrow (a, ac - b, c) = (a, b^*, c), \\ Z &: (a, b, c) \longrightarrow (a, b, ab - c) = (a, b, c^{*)}. \end{aligned}$$

Ainsi agit naturellement le groupe $\mathbf{T}_3 = \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z}$ sur l'ensemble de tous les triplets de Markoff. Le stabilisateur de tout sommet est réduit à l'identité, et il n'existe qu'une $\mathbf{T}_3$-orbite donnant tous les triplets de Markoff :

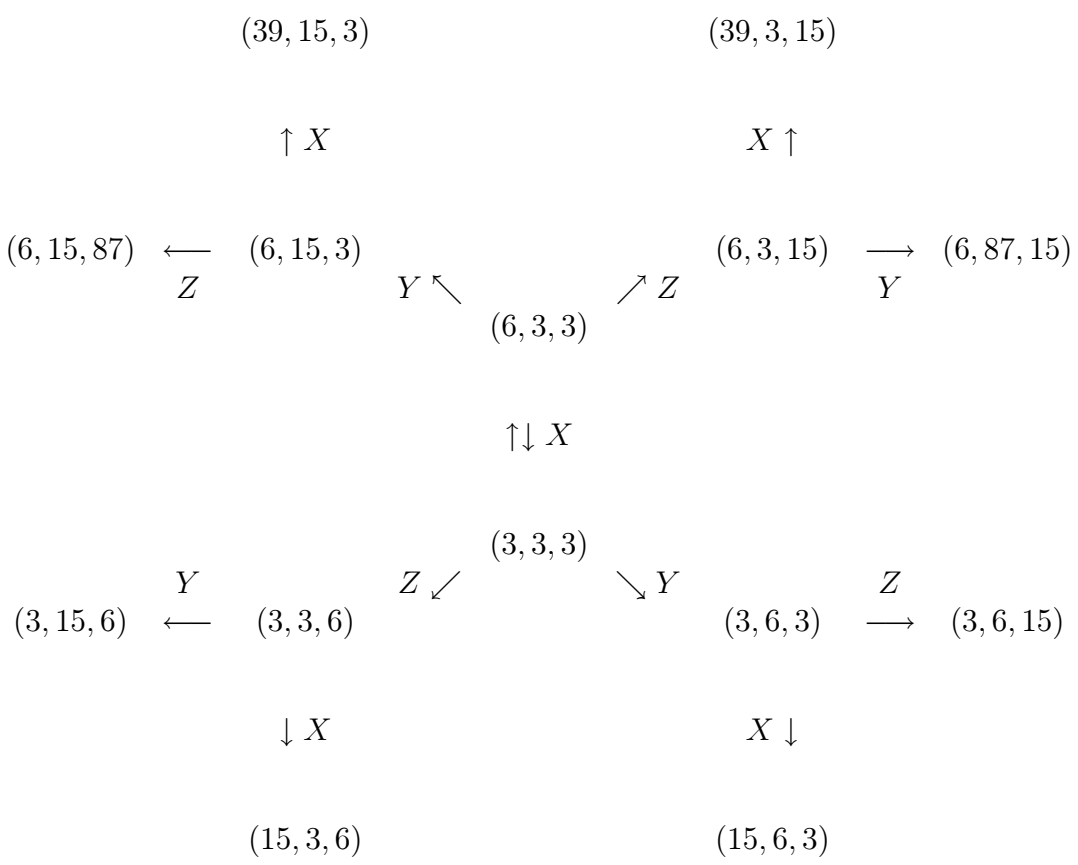


*fig.*1 : L'arbre complet de triplets de Markoff, ou T_3-orbite.

On observe que si (a, b, c) est un triplet de Markoff, tout triplet obtenu à partir de ce dernier par permutation de a, b, c en est un autre figurant dans ce même arbre. Plusieurs auteurs utilisent cette remarque pour réduire l'ensemble des triplets qu'ils considèrent. Par exemple :

- Cassels dans [13] (p. 27-28) évite des redondances en ne considérant que les **triplets de Cassels** $(\alpha, \beta, \gamma) = (a/3, b/3, c/3)$ caractérisés par le fait que α en

soit la **valeur dominante**, c'est à dire telle que :

$$\alpha = \max(\alpha, \beta, \gamma).$$

Cassels y divise en plus par deux le nombre des triplets qu'il considère en ne raisonnant que sur la partie de son arbre située sous le triplet $(15, 3, 6)$.

- Cohn dans [17] fusionne d'une certaine façon les deux opérations précédentes en ne considérant que les triplets vérifiant $a \geq b \geq c$.

- Zhang donne dans [63] une autre façon de constuire un arbre de solutions en ne considérant que les **triplets de Zhang** qui vérifient $a \leq b \leq c$. Il passe de (a, b, c) à $(a, b, ab - c)$ et $(b, c, bc - a)$. L'arbre de Zhang ([63] §1.7. figure 2) peut paraitre par sa définition bien adapté à l'étude de la conjecture de Frobenius qui se traduit simplement alors par le fait que la donnée du nombre c détermine au plus un triplet de Zhang (a, b, c). Facilement $a = b = c$ correspond à $(3, 3, 3)$ et $a = b < c$ à $(3, 3, 6)$. Hors ces cas $a < b < c$, et c est la valeur dominante du triplet (a, b, c) correspondant.

- Riedel travaille sur les triplets de Markoff (a, b, c) qui vérifient la condition :

$$\max(a, b, c) \in \{a, c\}.$$

On les appelle dans la suite les **triplets de Riedel**.

- Nous choissons dans le présent article de travailler sur les **triplets ibériques**. Ils sont caractérisés par le fait que c soit la **valeur dominante** :

$$\max(a, b, c) = c.$$

Contrairement aux triplets de Zhang nous ne posons aucune contrainte sur a et b. Notre ensemble de sommets est donc globalement deux fois plus gros que celui des triplets de Zhang, et deux fois moins gros que celui des triplets de Riedel. Néanmoins tout triplet de Markoff donne par permutation un triplet ibérique, de sorte qu'il n'y a pas de perte d'information en considérant seulement nos triplets.

Pour bien comprendre la différence entre les différents triplets, on peut observer les premiers triplets de Markoff non triviaux et déduits par permutation les uns des autres que sont $(15, 6, 3)$, $(15, 3, 6)$, $(6, 15, 3)$, $(3, 15, 6)$, $(6, 3, 15)$, $(3, 6, 15)$. Dans l'arbre complet ou la $\mathbf{T}_3$-orbite des solutions de l'équation (2.1) on considère tous ces triplets. La condition de Cassels caractérise les deux premiers divisés par 3, celle de Cohn le premier, celle de Zhang le dernier, et celle de Riedel l'ensemble à quatre éléments composé des deux premiers et des deux derniers. Le choix que nous faisons identifie les deux derniers et est donc tout à fait original. On vérifie en particulier que notre choix pour l'ensemble des sommets est plus large que celui de Zhang. Tous ses triplets apparaissent dans notre arbre des triplets ibériques.

2.1.1. L'arbre des triplets de Zhang

Exception faite des triplets $(3,3,3)$ et $(3,3,6)$ on a $a < b < c$ et on peut alors associer à tout triplet de Zhang (a,b,c) deux triplets ibériques (a,b,c) et (b,a,c). Tout triplet de Zhang (a,b,c) permet de considérer un autre triplet (a,c,b^*) où $b^* = ac - b$ reste strictement positif car b l'est aussi et que l'on a $a^2 + c^2 = b(ac-b)$.Comme cette condition donne aussi $c^2 < b(ac-b) < c(ac-b)$, il en résulte que l'on a $a < c < b^* = (ac-b)$, c'est à dire le fait que (a,c,b^*) est bien un nouveau triplet de Zhang. Un second triplet de Zhang peut se déduire de (a,b,c), il s'agit de (b,c,a^*) où $a^* = bc - a$. Il est différent du précédent $(a,c,ac-b) = (a,c,b^*)$ car $a \neq b$. C'est un triplet de Zhang car $b < c$ et $c < a^*$, avec $c^2 < a(bc-a) = b^2 + c^2 < c(bc-a) = ca^*$. Les arêtes de l'arbre de Zhang correspondantes sont données par :

$fig.\ 2:$ (a,b,c) $\nearrow$ $(b,c,bc-a) = (b,c,a^*)$

(a,b,c) $\searrow$ $(a,c,ac-b) = (a,c,b^*)$

On a $ac < bc$ et $-b < -a$, donc $a < b < c < b^* = ac - b < bc - a = a^*$. Les arêtes représentées font croitre les valeurs dominantes.

Inversement, un triplet de Zhang (a,b,c) étant donné, le nombre $c > 0$ est sa valeur dominante, et l'on peut considérer le nombre $c^* = ab - c$. Il est positif car on a $cc^* = c(ab-c) = a^2 + b^2 > 0$.Ce triplet définit l'un ou l'autre des deux triplets de Markoff (a,c^*,b) et (c^*,a,b). Supposons en effet que $b \leq c^*$, on aurait en multipliant par c :

$$bc \leq b(ab-c) = a^2 + b^2 < 2b^2, \qquad c < 2b.$$

Si (a_p,b_p,c_p) est le prédecesseur de (a,b,c), la figure 2 donne une contradiction :

$$(a,b,c) = (b_p,c_p,b_pc_p - a_p), \qquad c = b_pc_p - a_p < 2b = 2c_p \Rightarrow a = b_p < 3.$$

$$(a,b,c) = (a_p,c_p,a_pc_p - b_p), \qquad c = a_pc_p - b_p < 2b = 2c_p \Rightarrow a = a_p < 3.$$

Donc on a toujours $c^* < b$. Le cas $a = c^*$ est possible, il impose a diviseur de c avec l'expression de c^*, et donc de b avec (2.1). Ceci donne la seule possibilité ([13] p. 27) $(a,c^*,b) = (c^*,a,b) = (a,a,b) = (3,3,6)$, et $(a,b,c) = (3,6,15)$. Dans les autres cas $a \neq c^*$, et selon la position de a et c^* on trouve l'un ou l'autre des deux

triplets de Markoff indiqués, et un seul des deux est un triplet de Zhang. Les deux possibilités se présentent comme le montre la figure 2. La construction de c^* fait descendre dans l'arbre de Zhang : elle fait décroitre les valeurs dominantes. Cette descente s'arrête lorsque l'on a $(a, b, c) = (3, 6, 15)$, car on ne peut plus construire alors de triplet de Zhang avec ce triplet racine. D'où aussi la structure connexe de cet arbre (comparer à [63] p. 4). Pour illustrer la situation avec des inégalités larges et non plus strictes, on mentionne dans la représentation de l'arbre de Zhang deux triplets avant sa racine $(3, 6, 15)$:

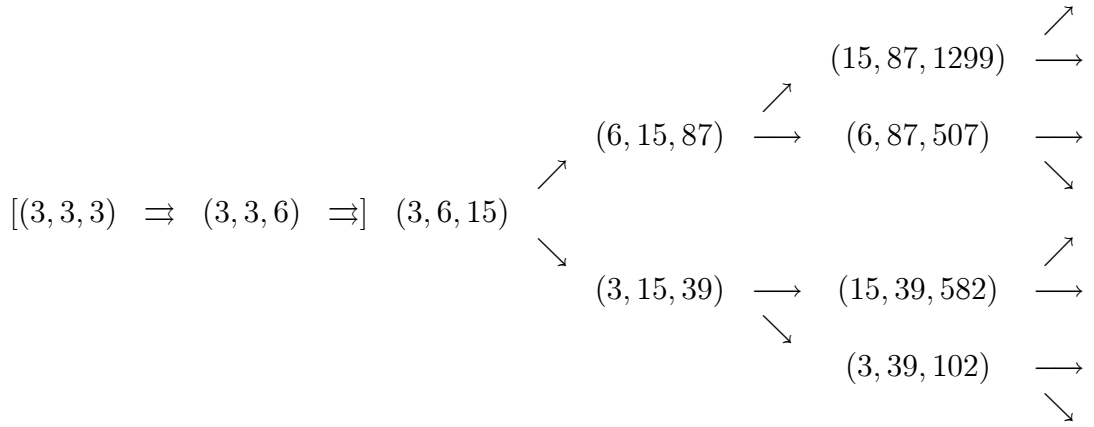


fig. 3 : L'arbre des triplets de Zhang.

2.1.2. L'arbre ibérique en matrices 3×3

Les sommets de l'**arbre ibérique** sont les triplets ibériques tels que définis avant. A chaque triplet ibérique (a, b, c) on associe bijectivement une matrice 3×3 à coefficients entiers de forme :

$$M(a, b, c) = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \in \mathbf{M}_3(\mathbb{Z}),$$

dite **M-matrice** du triplet (a, b, c) (où M signifie bien sûr Markoff). La M-matrice étant de déterminant 1, on a par construction $M(a, b, c) \in SL(3, \mathbb{Z})$. Les sommets de l'arbre ibérique peuvent donc être considérés comme étant les M-matrices $M(a, b, c)$ telles que $a < b < c$ ou $b < a < c$, ainsi que $(3, 3, 3)$ et $(3, 3, 6)$.

S'inspirant alors de ce que présente Riedel ([47] p. 3) on utilise pour définir les arêtes des matrices notées avec $x, y \in \mathbb{Z}$:

$$P^{-1}(x) = \begin{bmatrix} x & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ Q^{-1}(y) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & y \end{bmatrix}.$$

On a ainsi :

$$\begin{bmatrix} a & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & ac-b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & b \end{bmatrix} \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & b \end{bmatrix} = \begin{bmatrix} 1 & c & bc-a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}.$$

Avec la notation classique pour la transposition des matrices, on traduit ces deux égalités par :

$$^tP^{-1}(a)M(a,b,c)P^{-1}(a) = M(a,c,ac-b), \tag{2.2}$$

$$^tQ^{-1}(b)M(a,b,c)Q^{-1}(b) = M(c,b,bc-a), \tag{2.3}$$

et en permutant a et b, on a aussi :

$$^tP^{-1}(b)M(b,a,c)P^{-1}(b) = M(b,c,bc-a), \tag{2.4}$$

$$^tQ^{-1}(a)M(b,a,c)Q^{-1}(a) = M(c,a,ac-b), \tag{2.5}$$

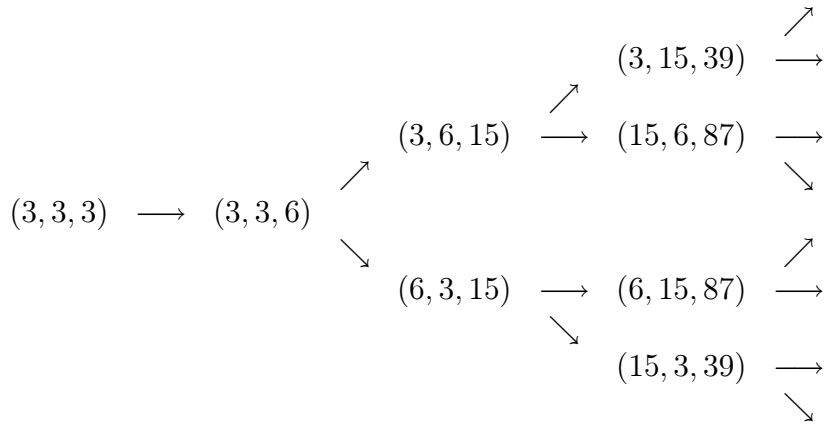
Supposant alors que (a,b,c) est un triplet de Zhang, donc ibérique, on trouve un second triplet ibérique qui est (b,a,c). Avec la figure 2 on a (a,c,b^*) triplet de Zhang issu de (a,b,c) et (c,b,a^*) triplet ibérique issu du même triplet, aussi (b,c,a^*) triplet de Zhang issu du triplet ibérique (b,a,c), et (c,a,b^*) triplet ibérique issu du même triplet. Sauf pour les plus petites valeurs dominantes on obtient quatre triplets ibériques : (a,c,b^*), (c,b,a^*), (b,c,a^*), (c,a,b^*). La M-matrice définie par le premier correspond à l'égalité (2.2), celle définie par le second correspond à l'égalité (2.3), etc.. Chacune de ces égalités donne une arête de l'arbre ibérique, ce que l'on résume par les figures suivantes (où la mention Zh : signale

que l'on a affaire à un triplet de Zhang) :

$fig.$ 4 :
$$Zh : (a, b, c) \begin{cases} \nearrow\ Zh : (a, c, ac - b) & \text{(égalité (2.2))} \\ \searrow\ (c, b, bc - a) & \text{(égalité (2.3))} \end{cases}$$

$fig.$ 5 :
$$(b, a, c) \begin{cases} \nearrow\ Zh : (b, c, bc - a) & \text{(égalité (2.4))} \\ \searrow\ (c, a, ac - b) & \text{(égalité (2.5))} \end{cases}$$

Soit en complétant la racine de l'arbre ibérique, la représentation suivante :



$fig.$ 6 : L'arbre ibérique.

Les triplets de Zhang apparaissent donc dans l'arbre ibérique, mais les arêtes ne sont plus les mêmes que dans l'arbre de Zhang. La connectivité que l'on a établie pour l'arbre de Zhang reste valide pour l'arbre ibérique. Sur ce dernier la conjecture de Frobenius se traduit, du fait que l'on a pour tous ses triplets (a, b, c) la valeur dominante :

$$\max(a, b, c) = c,$$

par la condition que toute valeur dominante c détermine exactement deux triplets différents dits **duaux** (a, b, c) et (b, a, c), hors les cas où $c = 3$ ou $c = 6$, où il n'en existe qu'un. On trouve alors les **triplets singuliers** $(3, 3, 3)$ et $(3, 3, 6)$ de la racine de l'arbre. En pratique on pourra les laisser de côté.

▷ **Notations 1 :** On a dans ce qui précède rencontré $\mathbf{M}_n(\mathbb{Z})$ l'anneau unitaire des matrices $n \times n$ à coefficients entiers. Il s'agit d'un sous anneau de $\mathbf{M}_n(\mathbb{Q})$ l'anneau unitaire des matrices $n \times n$ à coefficients rationnels. Dans ces anneaux apparaissent des groupes multiplicatifs comme $GL(n, \mathbb{Q})$ qui est composé des matrices de $\mathbf{M}_n(\mathbb{Q})$ de déterminant non nul, et $SL(n, \mathbb{Q})$ qui est composé des matrices de $GL(n, \mathbb{Q})$ de déterminant égal à 1. On y trouve aussi $GL(n, \mathbb{Z})$ qui est composé des matrices de $\mathbf{M}_n(\mathbb{Z})$ de déterminant égal à ± 1, et $SL(n, \mathbb{Z})$ qui est composé des matrices de $GL(n, \mathbb{Z})$ de déterminant égal à 1. La différence dans les définitions de $GL(n, \mathbb{Z})$ et $GL(n, \mathbb{Q})$ vient du fait que seuls 1 et -1 ont un inverse pour la multiplication dans $\mathbb{Z}$, alors que dans $\mathbb{Q}$ tout élément non nul est inversible. On note aussi parfois $S^*L(2, \mathbb{Z})$ pour $GL(2, \mathbb{Z})$.

2.1.3. Une première proposition pour l'arbre ibérique

Les matrices 3×3 définies précédemment sont inversibles, et l'on a :

$$M(a, b, c)^{-1} = \begin{bmatrix} 1 & -a & ab - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix} = M(-a, -b, ab - c),$$

$$P(x) = P^{-1}(x)^{-1} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & x & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; Q(y) = Q^{-1}(y)^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & y & 1 \\ 0 & -1 & 0 \end{bmatrix}.$$

Mieux, elles sont dans $SL(3, \mathbb{Z})$, groupe des matrices 3×3 à coefficients entiers et de déterminant égal à 1. Avec les compléments que l'on vient d'expliciter sur l'arbre ibérique, la proposition suivante est assurée :

Proposition 2.1. *Pour des M-matrices quelconques $M(a_1, b_1, c_1)$ et $M(a_2, b_2, c_2)$ correspondant à des sommets de l'arbre ibérique on peut trouver une matrice $N_{(2,1)}$ dans $SL(3, \mathbb{Z})$ telle que l'on ait :*

$$ {}^tN_{(1,2)} M(a_1, b_1, c_1) N_{(1,2)} = M(a_2, b_2, c_2). \tag{2.6}$$

Pour la démonstration, il suffit de suivre un chemin de l'arbre ibérique allant de (a_2, b_2, c_2) à $(3, 3, 3)$ puis de ce dernier à (a_1, b_1, c_1), et de composer les matrices $P^{-1}(x)$ et $Q^{-1}(y)$ données pas à pas par les arêtes de l'arbre selon les relations associées (2.2) à (2.5). Le produit de ces matrices, ou de leurs inverses si l'on prend une arête en sens inverse, donne une matrice $N_{(2,1)} \in SL(3, \mathbb{Z})$ vérifiant (2.6).

▷ **Notations 2 :** On peut écrire la condition (2.6) sous la forme :

$$ {}^tN_{(2,1)} M(a_2, b_2, c_2) N_{(2,1)} = M(a_1, b_1, c_1).$$

On se démarque donc des notations de [47] et [46]. Une matrice $N_{(2,1)}$ vérifiant (2.6) peut aussi être notée $N(a_2, b_2, c_2, a_1, b_1, c_1)$ lorsque l'on a besoin de précision. Avec un troisième triplet on a :

$$ {}^tN_{(3,2)} M(a_3, b_3, c_3) N_{(3,2)} = M(a_2, b_2, c_2),$$

$$ {}^tN_{(2,1)}\, {}^tN_{(3,2)} M(a_3, b_3, c_3) N_{(3,2)} N_{(2,1)} = M(a_1, b_1, c_1) = {}^tN_{(3,1)} M(a_3, b_3, c_3) N_{(3,1)}.$$

Le raisonnement sur les chemins que l'on vient de faire donne donc :

$$ N_{(3,1)} = N_{(3,2)} N_{(2,1)}. \tag{2.7}$$

Toute matrice $N_{(i,i)}$ obtenue avec (a_i, b_i, c_i) se reduit à l'identité, d'où aussi :

$$ \forall i,\ N_{(i,i)} = \mathbf{1}_3,\ \ N_{(2,1)}^{-1} = N_{(1,2)}. \tag{2.8}$$

En fait, pour obtenir ces dernières expressions, on a inversé la notation indicielle utilisée dans [47], cette dernière étant particulièrement malcommode. On convient aussi de noter $(a_0, b_0, c_0) = (3, 3, 3)$ le triplet singulier de la racine de l'arbre. Avec celui-ci on a l'égalité :

$$ N_{(2,1)} = N_{(2,0)} N_{(0,1)} = N_{(0,2)}^{-1} N_{(0,1)} = N_{(2,0)} N_{(1,0)}^{-1}. \tag{2.9}$$

2.2. Une explication de l'apparition des matrices 3×3

Les travaux de Cohn [17] ont montré que la théorie de Markoff est liée au groupe libre à deux générateurs. Ils disent essentiellement que dans $SL(2,\mathbb{Z})$ le sous-groupe des commutateurs, dit groupe dérivé $[SL(2,\mathbb{Z}), SL(2,\mathbb{Z})] = \mathbf{F}_2$, est un tel groupe libre engendré par les deux matrices 2×2 ([40] p. 170, [37] pp. 97-98) :

$$A_0 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = L^{-1}K^{-1}LK, \qquad B_0 = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = K^{-1}L^{-2}KL^2,$$

où

$$K = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = S, \qquad L = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = TS,$$

sont tels que l'on ait la présentation de groupe ([40] p. 167) :

$$SL(2,\mathbb{Z}) =< S, T \mid S^4 = \mathbf{1}_3, S^2 = (ST)^3 > .$$

On vérifie directement la propriété suivante du commutateur de A_0 et B_0 :

$$tr([A_0, B_0]) = tr(A_0 B_0 A_0^{-1} B_0^{-1}) = tr(\begin{bmatrix} -1 & 0 \\ -6 & -1 \end{bmatrix}) = -2.$$

Cette dernière simplifie en l'équation de Markoff (2.1) la classique égalité de Fricke [16], valable pour toutes les matrices A et B :

$$tr([A,B]) = tr(ABA^{-1}B^{-1}) = tr(A)^2 + tr(B)^2 + tr(AB)^2 - tr(A)tr(B)tr(AB) - 2. \tag{2.10}$$

Remarquons que A_0 et B_0 ne commutent pas :

$$A_0 B_0 = \begin{bmatrix} 0 & 1 \\ -1 & 3 \end{bmatrix}, \qquad B_0 A_0 = \begin{bmatrix} 0 & -1 \\ 1 & 3 \end{bmatrix} = -6.\mathbf{1}_2 + 3A_0 + 3B_0 - A_0 B_0.$$

Les travaux de Cohn ([16] à [19]) étendent l'observation que l'on vient de présenter pour (A_0, B_0) aux autres couples de générateurs (A, B) du groupe $\mathbf{F}_2$ en les liant aux solutions de l'équation (2.1). Le chapitre 6 de [40] approfondit cette question et donne ([40] p.174 prop. 4.3.) l'équivalence de trois énoncés suivants :

1/ Le couple (A, B) engendre le groupe $\mathbf{F}_2$.

2/ Le triplet $((tr(A)/3), (tr(B)/3), (tr(AB)/3))$ est une solution de l'équation de Markoff (1.1).

3/ On a l'égalité : $tr([A,B]) = tr(ABA^{-1}B^{-1}) = -2$.

En particulier l'action d'un automorphisme intérieur sur A et B est telle que, si $A' = NAN^{-1}$et $B' = NBN^{-1}$, on ait :

$$((tr(A')/3), (tr(B')/3), (tr(A'B')/3)) = ((tr(A)/3), (tr(B)/3), (tr(AB)/3)).$$

Et on a établit dans [40] (p.183 prop 5.3.) une réciproque qui énonce que lorsque cette dernière égalité est assurée, il existe une et une seule matrice $N \in GL(2, \mathbb{Z})$ telle que l'on ait :

$$A' = NAN^{-1}, \qquad B' = NBN^{-1}.$$

On en a déduit différents résultats sur le groupe des automorphismes $Aut(\mathbf{F}_2)$ et sur $GL(2, \mathbb{Z})$. Une autre perspective de cette approche est liée à l'application de la théorie des espaces de Teichmüller aux tores percés ([38]). Ces résultats sont évoqués dans [39].

2.2.1. Lien avec des quaternions

Avec les matrices A_0 et B_0 que l'on vient d'introduire, il est possible de considérer le $\mathbb{Z}$-module $\mathbb{Z} < A_0, B_0 >$ des combinaisons linéaires à coefficients dans $\mathbb{Z}$ de forme :

$$\boldsymbol{\alpha}\mathbf{1}_2 + \boldsymbol{\beta}A_0 + \boldsymbol{\gamma}B_0 + \boldsymbol{\delta}A_0B_0 = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathbf{M}_2(\mathbb{Z}), \tag{2.11}$$

où :

$$\mathbf{1}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ A_0 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix},\ B_0 = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix},\ A_0B_0 = \begin{bmatrix} 0 & 1 \\ -1 & 3 \end{bmatrix}. \tag{2.12}$$

Les expressions de A_0 et B_0 imposent que l'on ait p, q, r, s, dans $\mathbb{Z}$. En substituant dans (2.11), on obtient quatre égalités :

$$\boldsymbol{\alpha} + \boldsymbol{\beta} + \boldsymbol{\gamma} = p, \tag{2.13}$$

$$\boldsymbol{\beta} - \boldsymbol{\gamma} + \boldsymbol{\delta} = q, \tag{2.14}$$

$$\boldsymbol{\beta} - \boldsymbol{\gamma} - \boldsymbol{\delta} = r, \tag{2.15}$$

$$\boldsymbol{\alpha} + 2\boldsymbol{\beta} + \mathbf{2}\boldsymbol{\gamma} + 3\boldsymbol{\delta} = s. \tag{2.16}$$

Si on cherche à les inverser dans $\mathbb{Q}$, on trouve :

$$\boldsymbol{\alpha} = 2p + 3\frac{q}{2} - 3\frac{r}{2} - s, \tag{2.17}$$

$$\boldsymbol{\beta} = -\frac{p}{2} - \frac{q}{2} + r + \frac{s}{2}, \tag{2.18}$$

$$\boldsymbol{\gamma} = -\frac{p}{2} - q + \frac{r}{2} + \frac{s}{2}, \tag{2.19}$$

$$\boldsymbol{\delta} = \frac{q}{2} - \frac{r}{2}. \tag{2.20}$$

Mais comme on considère le $\mathbb{Z}$-module $\mathbb{Z} < A_0, B_0 >$ des combinaisons linéaires à coefficients dans $\mathbb{Z}$, il est en fait nécessaire pour que ces dernières relations donnent $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\delta} \in \mathbb{Z}$ que p, q, r, s dans $\mathbb{Z}$ vérifient différentes conditions. Avec $\boldsymbol{\delta} \in \mathbb{Z}$ ou $\boldsymbol{\alpha} \in \mathbb{Z}$ on a $q \equiv r \pmod 2$, avec $\boldsymbol{\beta} \in \mathbb{Z}$ ou $\boldsymbol{\gamma} \in \mathbb{Z}$ on a $p + s \equiv q \pmod 2$, soit en résumé :

$$p + s \equiv q \equiv r \pmod 2. \tag{2.21}$$

Inversement lorsque ces congruences sont vérifiées, on peut trouver à partir de p, q, r, s dans $\mathbb{Z}$ les nombres $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\delta}$, dans $\mathbb{Z}$. On est alors certain d'être dans le $\mathbb{Z}$-module $\mathbb{Z} < A_0, B_0 >$, qui est donc par construction sous $\mathbb{Z}$-module de $\mathbf{M}_2(\mathbb{Z})$. Les expressions que l'on vient de donner montrent que $\boldsymbol{\alpha} 1_2 + \boldsymbol{\beta} A_0 + \boldsymbol{\gamma} B_0 + \boldsymbol{\delta} A_0 B_0 = 0$ si et seulement si $\boldsymbol{\alpha} = \boldsymbol{\beta} = \boldsymbol{\gamma} = \boldsymbol{\delta} = 0$. En d'autres termes les quatre matrices $\mathbf{1}_2$, A_0, B_0, $A_0 B_0$, forment un système libre du $\mathbb{Z}$-module $\mathbb{Z} < A_0, B_0 >$ qui est de rang 4. Ces matrices sont d'ailleurs $\mathbb{Q}$-indépendantes dans $\mathbf{M}_2(\mathbb{Q})$. On peut construire à partir des expressions précédentes une table de multiplication :

$(A_0)^2$	$A_0 B_0$	$A_0(A_0 B_0)$
$= -\mathbf{1}_2 + 3A_0$	$= A_0 B_0$	$= -B_0 + 3A_0 B_0$
$B_0 A_0$	$(B_0)^2$	$B_0(A_0 B_0)$
$= -6.\mathbf{1}_2 + 3A_0 + 3B_0 - A_0 B_0$	$= -\mathbf{1}_2 + 3B_0$	$= -3.\mathbf{1}_2 + A_0 + 3B_0$
$(A_0 B_0)A_0$	$(A_0 B_0)B_0$	$(A_0 B_0)^2$
$= -3.\mathbf{1}_2 + 3A_0 + B_0$	$= -A_0 + 3A_0 B_0$	$= -\mathbf{1}_2 + 3A_0 B_0$

Cette table montre que $\mathbb{Z} < A_0, B_0 >$ est aussi muni d'une structure d'anneau, un sous-anneau de $\mathbf{M}_2(\mathbb{Q})$. Ceci permet, en utilisant le langage des quaternions [58], d'observer que dans la $\mathbb{Q}$-algèbre $\mathbf{M}_2(\mathbb{Q})$ des matrices 2×2 à coefficients rationnels considérée comme $\mathbb{Q}$-algèbre de quaternions, le sous $\mathbb{Z}$-module $\mathbb{Z} < A_0, B_0 >$ est un **ordre**. Il contient les matrices

$$A_0^{-1} = 3.\mathbf{1}_2 - A_0, \qquad B_0^{-1} = 3.\mathbf{1}_2 - B_0, \qquad A_0 B_0 A_0^{-1} B_0^{-1} = 8.\mathbf{1}_2 - 6A_0 - 3B_0 + 3A_0 B_0.$$

Le fait que $\mathbb{Z} < A_0, B_0 >$ est strictement contenu dans l'ordre $\mathbf{M}_2(\mathbb{Z})$ se voit aisément avec la condition :

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \notin \mathbb{Z} < A_0, B_0 > .$$

On peut aussi considérer dans $\mathbb{Z} < A_0, B_0 >$ la matrice :

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = -\mathbf{1}_2 + A_0.$$

Celle-ci est de déterminant -1, elle est donc inversible, et située dans le groupe de toutes les unités $\mathbb{Z} < A_0, B_0 >^*$. Elle n'est pas dans $SL(2, \mathbb{Z})$ qui ne contient que des matrices de déterminant 1. Dans $\mathbf{M}_2(\mathbb{Q})$ s'introduisent classiquement d'autres notions. Ainsi pour tout :

$$A = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathbf{M}_2(\mathbb{Q}),$$

on note :

$$\overline{A} = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix},$$

$$t(A) = p + s = tr(A), \qquad n(A) = ps - qr = \det(A),$$

$$< A, A' >= t(A\overline{A'}) = ps' - qr' + sp' - rq'.$$

Ces expressions induisent des notions analogues sur $\mathbb{Z} < A_0, B_0 >$, avec le fait que pour $A \in \mathbb{Z} < A_0, B_0 >$, la trace $tr(A)$ et le déterminant $\det(A)$ sont dans $\mathbb{Z}$, la trace étant d'ailleurs toujours paire.

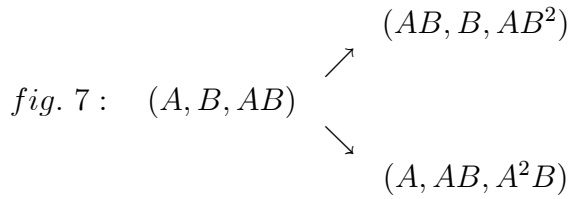
Evidemment on peut étendre le développement que l'on vient de présenter en considérant pour tout autre couple de générateurs (A, B) du groupe $\mathbf{F}_2$ le $\mathbb{Z}$-module $\mathbb{Z} < A, B >$ des combinaisons linéaires à coefficients dans $\mathbb{Z}$ de forme $\boldsymbol{\alpha}\mathbf{1}_2 + \boldsymbol{\beta}A + \boldsymbol{\gamma}B + \boldsymbol{\delta}AB$.

2.2.2. Sur les bases d'un $\mathbb{Z}$-module de rang 3

Dans ce qui précède on a rappelé que selon les travaux de Cohn [17] la théorie de Markoff est présentable avec des couples de matrices 2×2. Grâce aux travaux de Riedel [46] [47], une autre présentation de cette théorie a été trouvée avec des matrices 3×3. L'idée de ce qui suit est d'établir un lien entre ces matrices 3×3 et un sous-module libre de rang 3 du $\mathbb{Z}$-module $\mathbb{Z} < A_0, B_0 >$ mis

en évidence précédemment. Pour cela on considère le $\mathbb{Z}$-module $\mathbf{H}$ engendré par la base (A_0, B_0, A_0B_0). Il est aussi engendré par $(A_0, A_0B_0, A_0^2B_0)$ ou par $(A_0B_0, B_0, A_0B_0^2)$ qui sont d'autres bases de $\mathbf{H}$, ceci résulte directement de la table de multiplication donnée ci-dessus. Il y a bien d'autres bases dans $\mathbf{H}$, comme par exemple celles que l'on vient de citer transformées par une permutation des trois matrices les composant. On peut en contruire d'autres par récurrence en partant de (A_0, B_0, A_0B_0) et en passant de base en base en suivant pour chaque base (A, B, AB) obtenue les flèches du schéma suivant :

$fig.\ 7 :$



Si l'on suppose par récurrence que (A, B, AB) est une base engendrant $\mathbf{H}$, on peut trouver pour A, B, AB une combinaison linéaire des matrices A_0, B_0, A_0B_0, avec des coefficients entiers. Montrons qu'il en est de même pour la matrice A^2B. La matrice A est racine de son polynôme caractéristique :

$$A^2 - tr(A)A + \mathbf{1}_2 = 0,$$

de sorte que l'on a :

$$A^2B = tr(A)AB - B. \tag{2.22}$$

On conclut avec le fait vu ci-dessus que $tr(A)$ est un entier, et que A et AB sont aussi par hypothèse de récurrence combinaisons linéaires des matrices A_0, B_0, A_0B_0, avec des coefficients entiers. Il en est donc de même de A^2B. (A, AB, A^2B) engendre donc un sous module de $\mathbf{H}$. Par hypothèse de récurrence, (A, B, AB) est libre. Supposons alors que pour (A, AB, A^2B) il existe des coefficients entiers u_1, u_2, u_3, tels que :

$$0 = u_1A + u_2A^2B + u_3AB = u_1A + (u_2tr(A) + u_3)AB - u_2B.$$

On en déduit facilement :

$$0 = u_1 = u_2 = u_2tr(A) + u_3 = u_3.$$

Ainsi (A, AB, A^2B) est aussi libre. C'est une base qui engendre le même module $\mathbf{H}$ que (A, B, AB) comme le montre l'égalité déduite de (2.22) :

$$B = tr(A)AB - A^2B.$$

Le même raisonnement est faisable pour (AB, B, AB^2). De sorte que tous les triplets fabriqués avec notre figure 7 à partir de (A_0, B_0, A_0B_0) constituent une base du $\mathbb{Z}$-module $\mathbf{H}$ libre de rang 3. On ne fait cependant pas apparaitre avec ces seuls triplets toutes les bases possibles du module $\mathbf{H}$ considéré. Il suffit pour le voir de s'assurer que (A_0, A_0B_0, B_0) ne peut être obtenu par la figure 7. Dans l'esprit de [17] on peut introduire la notion de **triplet admissible**, définie par les deux règles de récurrence :

$$(A_0, B_0, A_0B_0) \text{ triplet admissible.}$$

Si (A, B, AB) triplet admissible, (A, AB, A^2B) et (AB, B, AB^2) admissibles.

On vient d'établir que tout triplet admissible est une base du $\mathbb{Z}$-module $\mathbf{H}$. On voit facilement que tout triplet admissible (A, B, AB) donne un couple de générateurs (A, B) du groupe $\mathbf{F}_2$, et donc aussi un automorphisme ϕ de ce groupe défini avec $\phi(A_0) = A$ et $\phi(B_0) = B$. La relation de Fricke (2.10) donne la trace du commutateur $[A, B] = ABA^{-1}B^{-1}$:

$$tr([A, B]) = tr(A)^2 + tr(B)^2 + tr(AB)^2 - tr(A)tr(B)tr(AB) - 2.$$

Par récurrence, il en résulte que tout couple (A, B) donné par un triplet admissible est tel que l'on ait :

$$tr([A, B]) = -2. \tag{2.23}$$

On a vérifié cette condition pour (A_0, B_0). Si elle est vraie pour (A, B), elle l'est pour (A, AB) avec :

$$\begin{aligned} tr([A, AB]) &= tr(A)^2 + tr(AB)^2 + tr(A^2B)^2 - tr(A)tr(AB)tr(A^2B) - 2 \\ &= tr(A)^2 + tr(AB)^2 + (tr(A)tr(AB) - tr(B))^2 \\ &\quad -tr(A)tr(AB)(tr(A)tr(AB) - tr(B)) - 2 \\ &= tr(A)^2 + tr(B)^2 + tr(AB)^2 - tr(A)tr(AB)tr(B) - 2 \\ &= tr([A, B]) = -2. \end{aligned}$$

Et de même pour (AB, B) en échangeant le rôle de A et B . La récurrence fonctionne et permet de conclure. En fait la condition $tr([A, B]) = -2$ caractérise plus généralement le fait que le couple (A, B) est un couple de générateurs (A, B) du groupe $\mathbf{F}_2$. Il s'agit d'un résultat du à J. Nielsen ([37] pp. 97-98). On en déduit que tous les couples de générateurs (A, B) du groupe $\mathbf{F}_2$ ne sont pas donnés par des triplets admissibles tels que l'on vient de les définir. Cependant pour tout triplet

admissible (A, B, AB), on trouve en comparant (2.10) et (2.23) une solution de l'équation (2.1) :

$$tr(A)^2 + tr(B)^2 + tr(AB)^2 = tr(A)tr(B)tr(AB).$$

2.2.3. L'arbre de Zhang en matrices 3×3

On visualise ici sur les traces ce que donnent les règles de récurrence avec lesquelles on a défini les triplets admissibles. On pose pour cela :

$$tr(A) = a,\ tr(B) = b,\ tr(AB) = c.$$

On vient de voir que tout triplet admissible (A, B, AB) donne un triplet de Markoff (a, b, c).

• Le triplet (A, AB, A^2B) donne avec l'expression (2.22) pour A^2B et la fonction matricielle Q^{-1} introduite précédemment :

$$(A, AB, A^2B) = (A, B, AB) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & tr(A) \end{bmatrix} = (A, B, AB)Q^{-1}(tr(A)).$$

Soit pour les traces :

$$(a, c, ac - b) = (a, b, c) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & a \end{bmatrix} = (a, b, c)Q^{-1}(a).$$

On trouve une relation ressemblant à (2.2), mais qui s'écrit sous la forme :

$$(a, b, c) \longrightarrow (a, c, ac - b) = (a, b, c)Q^{-1}(a). \tag{2.24}$$

• Le triplet (AB, B, AB^2) permet d'écrire de même avec (2.22), en introduisant une matrice ad'hoc :

$$\left(AB, B, AB^2\right) = (A, B, AB) \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & tr(B) \end{bmatrix} = (A, B, AB)R^{-1}(tr(B)).$$

Ceci donne pour les traces :

$$(c, b, bc - a) = (a, b, c)R^{-1}(b), \text{ où } R^{-1}(b) = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & b \end{bmatrix}.$$

On trouve une relation ressemblant à (2.3), et aussi comparable à (2.4) sous la forme :

$$(b,a,c) \longrightarrow (b,c,bc-a) = (b,a,c)Q^{-1}(b). \tag{2.25}$$

La comparaison des deux dernières égalités conduit à vérifier directement que l'on a avec une matrice de permutation $\Sigma(2,1,3)$:

$$R^{-1}(b) = {}^t\Sigma(2,1,3)Q^{-1}(b)\Sigma(2,1,3), \text{ où } \Sigma(2,1,3) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Cette matrice permutation correspond à une transposition et vérifie :

$${}^t\Sigma(2,1,3) = \Sigma(2,1,3)^{-1} = \Sigma(2,1,3).$$

• N'ayant pas vu intervenir de matrice de forme $P^{-1}(b)$ dans les deux points précédents, on fait appel à l'autre matrice permutation qui permet de représenter avec $\Sigma(2,1,3)$ tout le groupe des permutations de trois éléments :

$$\Sigma(3,1,2) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \qquad (3,1,2) = (1,2,3)\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Elle vérifie :

$${}^t\Sigma(3,1,2) = \Sigma(3,1,2)^{-1} = \Sigma(3,1,2)^2 = \Sigma(2,3,1),$$

et elle fait apparaitre $P^{-1}(b)$ avec :

$$R^{-1}(b) = {}^t\Sigma(2,3,1)P^{-1}(b)\Sigma(2,3,1),$$

$$Q^{-1}(b) = {}^t\Sigma(3,2,1)P^{-1}(b)\Sigma(3,2,1) = \Sigma(3,2,1)P^{-1}(b)\Sigma(3,2,1).$$

• Partant de $(tr(A_0), tr(B_0), tr(A_0B_0)) = (3,3,3)$, avec les expressions obtenues on peut alors traduire la figure 7 sur les triplets de traces :

fig. 8 :

$$(a,b,c) \begin{cases} \nearrow & (c,b,bc-a) = (a,b,c)R^{-1}(b) \\ \searrow & (a,c,ac-b) = (a,b,c)Q^{-1}(a) \end{cases}$$

En notant $Q_+^{-1}(a) = Q^{-1}(a)$ et remarquant que :

$$(b, c, bc - a) = (c, b, bc - a)\,\Sigma(2, 1, 3) = (a, b, c)Q_-^{-1}(b),$$

où :

$$Q_-^{-1}(b) = R^{-1}(b)\Sigma(2, 1, 3) = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & b \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & b \end{bmatrix},$$

on retrouve la figure 2 construisant l'arbre de Zhang, avec ici l'intervention de deux matrices $Q_+^{-1}(a)$ et $Q_-^{-1}(b)$ qui s'introduisent naturellement et sont de déterminants respectifs $+1$ et -1 :

$$fig.\ 2bis : \quad (a, b, c) \begin{cases} \nearrow & (b, c, bc - a) = (a, b, c)Q_-^{-1}(b) \\ \searrow & (a, c, ac - b) = (a, b, c)Q_+^{-1}(a) \end{cases}$$

On doit alors introduire deux nouvelles matrices :

$$P_+^{-1}(a) = P^{-1}(a), \qquad P_-^{-1}(b) = \Sigma(3, 2, 1)P^{-1}(b) = \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ b & 1 & 0 \end{bmatrix}.$$

Et l'on obtient ainsi des expressions qui construisent à partir de $M(3, 3, 3)$ un modèle matriciel de l'arbre de Zhang :

$$\begin{aligned} (a, b, c) &\xrightarrow{Q_-^{-1}(b)} (b, c, bc - a) \quad {}^tP_-^{-1}(b)\,{}^tM(a, b, c)P_-^{-1}(b) = M(b, c, bc - a) \\ (a, b, c) &\xrightarrow{Q_+^{-1}(a)} (a, c, ac - b) \quad {}^tP_+^{-1}(a)M(a, b, c)P_+^{-1}(a) = M(a, c, ac - b) \end{aligned}$$

Elles correspondent respectivement dans le module **H** de rang 3 aux transformations :

$$\begin{aligned} (A, B, AB) &\xrightarrow{Q_-^{-1}(b)} (B, AB, AB^2) = (A, B, AB)Q_-^{-1}(b) \\ (A, B, AB) &\xrightarrow{Q_+^{-1}(a)} (A, AB, A^2B) = (A, B, AB)Q_+^{-1}(a) \end{aligned}$$

L'apparition de la matrice ${}^tM(a, b, c)$ dans l'une de ces expressions est surprenante, mais peut être comprise avec :

$$\begin{aligned} {}^t\Sigma(3, 2, 1)\,{}^tM(a, b, c)\Sigma(3, 2, 1) &= M(b, a, c), \\ {}^tP^{-1}(b)\,M(b, a, c)P^{-1}(b) &= M(b, c, bc - a). \end{aligned}$$

2.3. Evocation de la conjecture de Tyurin et compléments

La théorie de Markoff telle que présentée classiquement [40] utilise de façon privilégiée la **relation de similitude** sur $\mathbf{M}_2(\mathbb{Z})$:

$$V_1 \sim V_2 \Longleftrightarrow \exists N \in GL(2,\mathbb{Z}) \qquad N^{-1}V_1N = V_2,$$

Cependant la proposition 2.1 fait plutôt appel à la **relation de congruence** sur $\mathbf{M}_3(\mathbb{Z})$:

$$W_1 \approx W_2 \Longleftrightarrow \exists N \in GL(3,\mathbb{Z}) \qquad {}^tNW_1N = W_2.$$

En s'inspirant des travaux de Reidel [47], on vient d'évoquer comment transposer la théorie de Markoff en dimension 3, et ce que l'on a présenté fait appel à de telles relations de congruence. C'est une perspective qui était affichée dans [41] (p. 8 ou p. 34), en liaison avec un théorème de Dyer et Formanek, et dont une esquisse apparait dans [27]. Associée à une matrice $M(a,b,c)$, il existe naturellement une forme quadratique dont l'égalité à 0 correspond à l'équation d'un cône. On l'a déjà mentionnée dans [40] (p. 138) :

$$\Phi_{M(a,b,c)}(x,y,z) = \begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

$$= \quad x^2 + y^2 + z^2 + axy + byz + czx.$$

Si on change de base pour (x,y,z) on voit que l'on change la matrice $M(a,b,c)$ en une matrice congruente, et ceci change la forme ternaire que l'on vient de mettre en évidence, ainsi que le cône considéré. Cette piste a été évoquée dans un article de Cohn [19]. On a indiqué dans [41] (§ 3.2.4 p. 55 et § 5 p. 63-64) comment une telle forme avait une certaine importance du point de vue de la géométrie algébrique, en particulier pour la classification des faisceaux vectoriels exceptionnels sur le plan projectif $\mathbf{P}^2$. Cette dernière question est le cadre de la conjecture de A.N. Tyurin qui affirme qu'un tel faisceau exceptionnel est déterminé de façon unique par son rang [57]. Il a été établi par A.L. Gorodentsev et A.N. Rudakov que les rangs des faisceaux exceptionnels de $\mathbf{P}^2$ sont des nombres de Markoff [26], [6]. Dans l'article de A.N. Rudakov [51], il est établi que la conjecture de Tyurin est équivalente à celle de Frobenius.

Si on regarde de plus près ce que l'on a dit avant sur l'apparition des matrices 3×3, pour modéliser la théorie de Markoff on constate que l'on n'a pas expliqué clairement d'où sortent les matrices $M(a,b,c)$. Dans [47] Reidel justifie leur introduction par un modèle quantique ([22] et [23]). On va donc rappeler d'abord

comment ces matrices sont liées au groupe de Heisenberg [31]. Puis on va montrer commen, sans faire appel à la mécanique quantique, ces matrices s'introduisent très naturellement dans le contexte que l'on a présenté avant. Enfin on va compléter la description du modèle matriciel de l'arbre ibérique.

2.3.1. Le lien avec le groupe de Heisenberg

Le **groupe de Heisenberg discret**, que les physiciens nomment plutôt groupe de Weyl, ou encore groupe de Heisenberg-Weyl (voir [31]), est défini comme l'ensemble :

$$\mathbb{H}_1(\mathbb{Z}) = \left\{ M(a,b,c) = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} ; a,b,c \in \mathbb{Z} \right\},$$

équipé de la multiplication des matrices. Ce groupe est un réseau du **groupe de Lie** réel $\mathbb{H}_1(\mathbb{R})$, groupe pour la multiplication de matrices analogues mais avec $a, b, c \in \mathbb{R}$. Ce dernier groupe définit un ensemble de vecteurs tangents à toutes les courbes de $\mathbb{H}_1(\mathbb{R})$ passant par l'unité, naturellement muni d'une structure d'**algèbre de Lie**. Il s'agit de l'algèbre de Lie de Heisenberg-Weyl $\mathfrak{h}_1$ qui est engendrée par trois opérateurs $\mathbf{Q}$, $\mathbf{P}$, $-\mathbf{I}$, et dont le crochet de Lie vérifie $[\mathbf{P}, \mathbf{Q}] = -\mathbf{I}$, $[-\mathbf{I}, *] = 0$. Cette algèbre de Lie est l'algèbre de Lie matricielle (on dit aussi linéaire) des matrices triangulaires supérieures :

$$p\mathbf{P} + q\mathbf{Q} - z\mathbf{I} = \begin{bmatrix} 0 & p & z \\ 0 & 0 & q \\ 0 & 0 & 0 \end{bmatrix},$$

avec pour crochet de Lie le simple commutateur des matrices :

$$[\begin{bmatrix} 0 & p & z \\ 0 & 0 & q \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & p' & z' \\ 0 & 0 & q' \\ 0 & 0 & 0 \end{bmatrix}] = \begin{bmatrix} 0 & 0 & pq' - pq' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Cette algèbre définit inversement $\mathbb{H}_1(\mathbb{R})$, comme groupe de Lie local matriciel dont l'opération est la multiplication des matrices, et dont tous les éléments s'écrivent tous comme une exponentielle :

$$g = \exp(p\mathbf{P} + q\mathbf{Q} - z\mathbf{I}) = \begin{bmatrix} 1 & p & z + \frac{pq}{2} \\ 0 & 1 & q \\ 0 & 0 & 1 \end{bmatrix}.$$

On retrouve l'algèbre de Lie $\mathfrak{h}_1$ associée en calculant les vecteurs tangents en 0 à une courbe de ce groupe passant par l'unité, avec en ce point la possibilité de noter :

$$\frac{\partial g}{\partial p} = \mathbf{P} = U - \mathbf{1}_3,\ \frac{\partial g}{\partial q} = \mathbf{Q} = V - \mathbf{1}_3,\ \frac{\partial g}{\partial z} = -\mathbf{I} = W - \mathbf{1}_3.$$

Par une vérification directe, on a :

$$\begin{aligned} & \exp(p\mathbf{P})\exp(q\mathbf{Q})\exp(-z\mathbf{I}) \\ = & \begin{bmatrix} 1 & p & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & q \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & p & z+pq \\ 0 & 1 & q \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Cette expression est différente de celle de $\exp(p\mathbf{P} + q\mathbf{Q} - z\mathbf{I})$. La différence entre les deux expressions s'explique par le classique théorème de Campbell-Baker-Hausdorff. Maintenant considérons les élements :

$$\begin{aligned} U &= \exp(\mathbf{P}) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\ V &= \exp(\mathbf{Q}) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \\ W &= \exp(-\mathbf{I}) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \end{aligned}$$

ils engendrent le sous groupe $\mathbb{H}_1(\mathbb{Z})$ de $GL_3(\mathbb{Z})$, qui est défini avec ces trois générateurs par les relations :

$$UVU^{-1}V^{-1} = VU^{-1}V^{-1}U = U^{-1}V^{-1}UV = V^{-1}UVU^{-1} = W.$$

On observe, en calculant le produit de deux matrices du groupe $\mathbb{H}_1(\mathbb{Z})$, que ce dernier est représentable plus simplement par l'ensemble $\mathbb{Z}^3$ des triplets d'entiers muni de l'opération non commutative :

$$(a, b, c)(a', b', c') = (a + a', b + b', c + c' + ab').$$

Avec son graphe de Cayley, on peut aussi représenter le groupe $\mathbb{H}_1(\mathbb{Z})$ comme une orbite pour l'action naturelle du groupe $\mathbf{T}_4 = \mathbf{T}_3 \star \mathbb{Z}/2\mathbb{Z}$, produit libre de quatre modèles du groupe à deux éléments $\mathbb{Z}/2\mathbb{Z}$. Avec la figure 1 la théorie de Markoff peut être vue comme une orbite pour une action du groupe $\mathbf{T}_3$, on l'a rappelé avant, elle est donc représentable dans $\mathbb{H}_1(\mathbb{Z})$ qui est aussi un réseau de $\mathbb{H}_1(\mathbb{R})$.

2.3.2. Construction directe des matrices $M(a,b,c)$

Dans ce qui précède on a mis en évidence une algèbre de quaternions munie d'une trace et d'une norme. On y a considéré un hyperplan $\mathbf{H}$ et des bases de cet hyperplan constituées de matrices de $SL(2,\mathbb{Z})$, c'est à dire de déterminant 1. Avec une base (A,B,AB) de $\mathbf{H}$ un point générique de cet hyperplan s'écrit :

$$\mathbf{m} = xA + yB + zAB \in \mathbf{H}.$$

C'est aussi une matrice 2×2 et un quaternion qui à ce titre possède une trace et une norme :

$$t(\mathbf{m}) = t(xA+yB+zAB) = ax+by+cz,$$
$$n(\mathbf{m}) = \det(xA+yB+zAB) = \Psi_{(A,B,AB)}(x,y,z).$$

La trace donne une forme linéaire, et la norme donne une forme quadratique que l'on peut calculer explicitement :

$$x^2\det A + y^2\det B + z^2\det AB + zxtr(B)\det A + yztr(A)\det B + xytr(AB^{-1})\det B.$$

Il suffit pour le voir d'expliciter A et B. Cette expression se simplifie avec $\det A = \det B = 1$. On retrouve alors simplement une forme ternaire Φ, telle que définie précèdemment ainsi qu'une matrice $M(tr(AB^{-1}),tr(B),tr(A))$:

$$\begin{aligned} n(\mathbf{m}) &= \Psi_{(A,B,AB)}(x,y,z) = \det(xA+yB+zAB) \\ &= x^2+y^2+z^2+tr(AB^{-1})xy+tr(B)zx+tr(A)yz \\ &= \begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 1 & tr(BA^{-1}) & tr(B) \\ 0 & 1 & tr(A) \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \\ &= \Phi_{M(tr(BA^{-1}),tr(A),tr(B))}(x,y,z). \end{aligned}$$

Sortant de $\mathbf{H}$ on peut plus simplement faire apparaitre directement $M(a,b,c)$:

$$\begin{aligned} \det(x\mathbf{1}_2+yA+zBA) &= \begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \\ &= x^2+y^2+z^2+axy+byz+czx. \end{aligned}$$

2.3.3. Retour sur la construction de l'arbre ibérique

La question se pose de comprendre comment s'étend ce que l'on a vu pour l'arbre de Zhang à l'arbre des triplets ibériques. On pourait vouloir élargir la définition des triplets admissibles, et par exemple à partir de (A, B, AB) triplet admissible, vouloir introduire un triplet admissible contenant BA. Mais avec les égalités :

$$A^{-1} = tr(A)\mathbf{1}_2 - A, \qquad B^{-1} = tr(B)\mathbf{1}_2 - B, \qquad tr(AB^{-1}) = tr(B)tr(A) - tr(AB),$$

$$(BA)^{-1} = A^{-1}B^{-1} = tr(A)tr(B)\mathbf{1}_2 - tr(B)A - tr(A)B + AB = tr(AB)\mathbf{1}_2 - BA,$$

$$BA = (tr(AB) - tr(A)tr(B))\mathbf{1}_2 + tr(B)A + tr(A)B - AB, \tag{2.26}$$

considérer la matrice BA oblige à sortir du $\mathbb{Z}$-module $\mathbf{H}$ engendré par A, B, AB, c'est à dire aussi par A_0, B_0, A_0B_0. On ne peut donc pas retenir une telle option si l'on privilégie le rang 3 de $\mathbf{H}$. Par contre en restant dans $\mathbf{H}$ on peut utiliser une matrice permutation de trois éléments. Le passage de (A, B, AB) à (AB, A, B) est ainsi réalisé avec :

$$(AB, A, B) = (A, B, AB) \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = (A, B, AB)\Sigma(3, 1, 2).$$

Cette matrice permutation $\Sigma(3, 1, 2) \in SL(3, \mathbb{Z})$ donne sur les traces :

$$(c, a, b) = (a, b, c)\Sigma(3, 1, 2).$$

Il semble étrange de faire intervenir une telle transformation car elle ne respecte pas la propriété d'être ibérique de nos triplets. Cependant la suite va montrer comment cela est possible.

• Le triplet (A, B, AB) admissible donne par $\Sigma(3, 1, 2)$ l'autre triplet (AB, A, B), qui se transforme en (AB^2, AB, B) par la matrice $P^{-1}(tr(B))$, et donne à son tour l'autre triplet (AB, B, AB^2) par $\Sigma(3, 1, 2)^{-1}$ et (2.22) :

$$\begin{aligned}
(AB, B, AB^2) &= (A, B, AB)\Sigma(3, 1, 2)P^{-1}(b)\Sigma(3, 1, 2)^{-1} \\
&= (A, B, AB) \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} b & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \\
&= (A, B, AB) \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & b \end{bmatrix} \\
&= (A, B, AB)R^{-1}(b).
\end{aligned}$$

On retrouve ainsi l'égalité avec laquelle on a défini ci-dessus $R^{-1}(b) \in SL(3,\mathbb{Z})$. Ceci donne pour les traces l'équivalent de la relation (2.3) écrite ici :

$$(a,b,c) \stackrel{R^{-1}(b)}{\longrightarrow} (c,b,bc-a) = (a,b,c)R^{-1}(b). \tag{2.27}$$

• La transformation de (B,A,AB) en (AB,A,A^2B) s'explicite de même en utilisant (2.22). On trouve :

$$\begin{aligned}
& (AB,A,A^2B) \\
= \; & (A^2B,AB,A)\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \\
= \; & (AB,B,A)\begin{bmatrix} a & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \\
= \; & (B,A,AB)\Sigma(3,1,2)P^{-1}(a)\Sigma(3,1,2)^{-1},
\end{aligned}$$

On fait apparaitre ainsi $R^{-1}(a) \in SL(3,\mathbb{Z})$ qui donne aussi pour les traces :

$$(c,a,ac-b) = (b,a,c)R^{-1}(a) = (b,a,c)\begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & a \end{bmatrix}.$$

On retrouve cette fois la relation (2.5) écrite sous la forme :

$$(b,a,c) \stackrel{R^{-1}(a)}{\longrightarrow} (c,a,ac-b) = (b,a,c)R^{-1}(a). \tag{2.28}$$

• Dans ce que l'on vient de voir se sont introduites naturellement les deux matrices $R^{-1}(a)$ et $R^{-1}(b)$. Pour cela on est parti des bases (A,B,AB) et (B,A,AB) du $\mathbb{Z}$-module $\mathbf{H}$ libre et de rang 3. On complète aisément en choisissant la bonne matrice permutation pour transformer (2.3) en (2.4), et respectivement (2.5) en (2.2). Ceci donne un tableau global qui résume ce que l'on vient de voir sur les matrices 3×3 pour les relations (2.2) à (2.5) :

$$\begin{array}{lll}
(a,b,c) \stackrel{Q^{-1}(a)}{\longrightarrow} (a,c,ac-b) & {}^tP^{-1}(a)M(a,b,c)P^{-1}(a) = M(a,c,ac-b) & (2.2) \\
(a,b,c) \stackrel{R^{-1}(b)}{\longrightarrow} (c,b,bc-a) & {}^tQ^{-1}(b)M(a,b,c)Q^{-1}(b) = M(c,b,bc-a) & (2.3) \\
(b,a,c) \stackrel{Q^{-1}(b)}{\longrightarrow} (b,c,bc-a) & {}^tP^{-1}(b)M(b,a,c)P^{-1}(b) = M(b,c,bc-a) & (2.4) \\
(b,a,c) \stackrel{R^{-1}(a)}{\longrightarrow} (c,a,ac-b) & {}^tQ^{-1}(a)M(b,a,c)Q^{-1}(a) = M(c,a,ac-b) & (2.5)
\end{array}$$

Tableau n°1.

Ces expressions correspondent respectivement dans le module **H** de rang 3 aux transformations :

$$(A,B,AB) \overset{Q^{-1}(a)}{\longrightarrow} (A,AB,A^2B) = (A,B,AB)Q^{-1}(a)$$
$$(A,B,AB) \overset{R^{-1}(b)}{\longrightarrow} (AB,B,AB^2) = (A,B,AB)R^{-1}(b)$$
$$(B,A,AB) \overset{Q^{-1}(b)}{\longrightarrow} (B,AB,AB^2) = (B,A,AB)Q^{-1}(b)$$
$$(B,A,AB) \overset{R^{-1}(a)}{\longrightarrow} (AB,A,A^2B) = (B,A,AB)R^{-1}(a)$$

3. Préambule à l'étude de la conjecture

On s'inspire de l'article [47] de Riedel que l'on débarrasse désormais de tout décor quantique. On cherche d'abord à identifier tout argument de ce texte qui pourrait être décisif pour une démonstration arithmétique de la conjecture. On concentre l'attention sur l'étude du paragraphe 5 - Proof of the Theorem - de cet article. Une lecture attentive montre que l'auteur n'y cite qu'en trois endroits importants pour sa démonstration des énoncés issus de ses paragraphes antérieurs. On les examine en détail pour voir en quoi ils pourraient être déterminants. Le constat est le suivant sur la version 3 de [47] datée du 15 mai 2013 :

• (1) : Riedel évoque sa relation (4.1) dans la première démonstration de son lemme 5.7. Or cette relation (4.1) n'intervient pas réellement dans sa démonstration de ce lemme. On peut donc la laisser de côté.

• (2) : Il mentionne une matrice $\mathcal{A}$ dans sa proposition 4.6, et cette matrice semble assez essentielle pour sa nouvelle démonstration de la conjecture. En fait on peut s'en passer en ne considérant que les relations issues de $\mathcal{A}$.

• (3) : Il fait usage de sa relation (4.28) entre deux matrices $\mathcal{A}_1$ et $\mathcal{A}_2$. Comme on peut laisser de côté les matrices $\mathcal{A}$ on peut se passer de ces matrices, en considérant seulement toutes les relations traduisant (4.28).

• (4) : Seul reste son lemme 4.2 qui intervient de façon déterminante dans la vérification de son lemme 5.1 puis de ses relations (5.4) et (5.8). Le lemme 4.2 semble être l'argument essentiel à retenir ici de la tentative de démonstration que développe Riedel.

Pour le présent chapitre on se fixe comme objectif de démontrer ce lemme (cf. nos propositions (3.9) et (3.10)), puis de préciser comment l'appliquer. On verra ultérieurement ce qui reste à considérer par rapport à la dernière version de [47].

3.1. Quelques résultats arithmétiques préalables

3.1.1. Décomposition en facteurs pour les triplets de Markoff

Pour tout triplet (a, b, c) de Markoff on a posé $b^* = ac - b$, et ceci définit un autre triplet de Markoff (a, b^*, c). On peut en toute généralité considérer la factorisation $b^* = 2^e 3\mathfrak{b}^*$ où $\mathfrak{b}^*$ premier à 6 et $e \in \{0, 1\}$. Vérifions le ici. Le nombre b^* définit de façon unique son plus grand facteur $\mathfrak{b}^*$ premier à 6.

• Pour les puissances de 3 divisant b^*, on part de :

$$a^2 + b^{*2} + c^2 = ab^*c.$$

On raisonne modulo 3 en remarquant que b^{*2} est congru à 0 si b^* est divisible par 3, et à 1 dans le cas contraire.

∗ Si b^* est divisible par 3, on a :

$$a^2 + c^2 \equiv 0 \pmod 3.$$

Ceci n'est possible que si :

$$a = 3\alpha \equiv c = 3\gamma \equiv 0 \pmod 3,$$

et ceci nous ramène à l'équation de Markoff sous la forme classique (1.1) :

$$\alpha^2 + \beta^{*2} + \gamma^2 = 3\alpha\beta^*\gamma.$$

Si $b^* = 3\beta^*$ est divisible par 9, c'est à dire β^* divisible par 3, il vient :

$$\alpha^2 + \gamma^2 \equiv 0 \pmod 3.$$

A nouveau, par le même raisonnement, ceci n'est possible que si :

$$\alpha \equiv \gamma \equiv 0 \pmod 3.$$

Mais comme on sait avec ([13] p. 28) que les nombres α, γ, β^*, sont premiers entre eux, ce cas est impossible. Dans le cas étudié on est donc certain que b^* est divisible par 3, mais pas par 9.

∗ Le cas qui reste à examiner est celui où b^{*2} est congru à 1 modulo 3. Si a ou c multiple de 3, alors ab^*c également multiple de 3, et on trouve une contradiction car $a^2 + b^{*2} + c^2$ congru à 1 ou 2 modulo 3. Le dernier cas possible est celui où a et c non multiples de 3, alors $a^2 + b^{*2} + c^2$ est un multiple de 3 alors

que ab^*c ne l'est pas. On trouve encore une contradiction. Ainsi a-t-on vérifié que la factorisation de b^* est bien de forme $b^* = 2^e 3\mathfrak{b}^{*\maltese}$ où $\mathfrak{b}^*$ premier à 6.

• On s'intéresse alors au cas où $e \geq 2$. Modulo 4 on doit avoir :

$$a^2 + c^2 \equiv 0 \pmod 4.$$

Si a ou c impair, le nombre $a^2 + c^2$ est congru à 1 ou 2 modulo 4. On trouve une contradiction. Si $a = 2\alpha_1$ et $c = 2\gamma_1$ pairs, on se ramène à la situation suivante où $b^* = 4\beta_1^*$:

$$\alpha_1^2 + 4\beta_1^{*2} + \gamma_1^2 = 4\alpha_1\beta_1^*\gamma_1.$$

Ceci impose $\alpha_1 = 2\alpha_2$ et $\gamma_1 = 2\gamma_2$ pairs. Et l'on se ramène en posant $b^* = 4\beta_2^*$ à une équation s'écrivant :

$$\alpha_2^2 + \beta_2^{*2} + \gamma_2^2 = 4\alpha_2\beta_2^*\gamma_2.$$

Elle n'est possible que si $\alpha_2 \equiv \gamma_2 \equiv \beta_2^* \pmod 4$. Ceci impose $\alpha_1 = 4\alpha_3$, $\gamma_1 = 4\gamma_3$ et $\beta_1^* = 4\beta_3^*$ et conduit à :

$$\alpha_3^2 + \beta_3^{*2} + \gamma_3^2 = 16\alpha_3\beta_3^*\gamma_3.$$

De fil en aiguille, en renouvelant le même raisonnement, on passe par des équations s'écrivant avec t entier de plus en plus grand :

$$\alpha_t^2 + \beta_t^{*2} + \gamma_t^2 = 4^{t+1}\alpha_t\beta_t^*\gamma_t.$$

Au final, on trouve une contradiction avec le fait que l'on a $a_1 = 4^{t+1}\alpha_{t+1}$ avec t augmentant indéfiniment. Le cas $e \geq 2$ est donc impossible, et les seuls cas envisageables sont $e \in \{0, 1\}$.

• Le raisonnement que l'on vient de faire est en réalité applicable à tout triplet de Markoff, et donc il donne aussi les factorisations possibles pour a, b et c. Fixons ici les notations associées.

▷ **Notations 3** : On note désormais pour tout triplet de Markoff :

$$b^* = ac - b = 3\beta^* = 2^e 3\mathfrak{b}^*,\ e = e_{b^*} \in \{0, 1\},\ \mathfrak{b}^* \text{ premier à } 6. \tag{3.1}$$

Pour les triplets de Markoff les plus généraux (a, b, c) de l'arbre ibérique, on pose de même :

$$a = 3\alpha = 2^{e_a} 3\mathfrak{a},\ e_a \in \{0, 1\},\ \mathfrak{a} \text{ premier à } 6. \tag{3.2}$$

$$b = 3\beta = 2^{e_b} 3\mathfrak{b},\ e_b \in \{0, 1\},\ \mathfrak{b} \text{ premier à } 6, \tag{3.3}$$

$$c = 3\gamma = 2^{e_c} 3\mathfrak{c},\ e_c \in \{0, 1\},\ \mathfrak{c} \text{ premier à } 6, \tag{3.4}$$

3.1.2. Une hypothèse de départ possible

Pour démontrer la conjecture, on se place dans l'arbre ibérique. On suppose $c \neq 3$ et $c \neq 6$, les vérifications à la racine de l'arbre étant faciles. On suppose qu'il existe au moins deux triplets différents correspondant à une même valeur dominante c. En utilisant le fait que si (a, b, c) est dans l'arbre ibérique, (b, a, c) s'y trouve aussi, on peut prendre la **précaution** de ne considérer que deux d'entre eux $(a_1, b_1, c) \neq (a_2, b_2, c)$ qui sont des triplets de Zhang avec c dominant, c'est à dire tels que :

$$a_1 < b_1 < c, \qquad a_2 < b_2 < c. \tag{3.5}$$

On montre d'abord que l'on a :

$$\{a_1, b_1\} \cap \{a_2, b_2\} = \varnothing.$$

En effet, si $a_1 \in \{a_2, b_2\}$ on a $a_1 = a_2$ et $(a_1, b_1, c) = (a_2, b_2, c)$ non distincts, ou $a_1 = b_2$ et $(a_1, b_1, c) = (b_2, a_2, c)$ contradictoire par $a_2 = b_1 < b_2 = a_1 < b_1$ avec la précaution (3.5). Et si $b_1 \in \{a_2, b_2\}$ on a $b_1 = b_2$ et $(a_1, b_1, c) = (a_2, b_2, c)$ non distincts, ou $b_1 = a_2$ et $(a_1, b_1, c) = (b_2, a_2, c)$ contradictoire par $a_1 = b_2 < b_1 = a_2 < b_2$ avec la précaution (3.5). Dans les deux cas on trouve une contradiction, d'où nécessairement le fait que $\{a_1, b_1\}$ et $\{a_2, b_2\}$ sont disjoints. On peut donc, en choisissant correctement les indices, supposer que l'on a l'inégalité :

$$a_1 < a_2. \tag{3.6}$$

Ceci constitue l'**hypothèse Z** qui est la conjonction de la précaution (3.5) et de l'inégalité (3.6), et qui pourrait être prise comme hypothèse de départ pour l'étude de la conjecture.

• Pour de tels triplets, avec $b_1^* = a_1 c - b_1$ et $b_2^* = a_2 c - b_2$ on a les deux équations :

$$a_1^2 + b_1^{*2} + c^2 = a_1 b_1^{\maltese} c, \qquad a_2^2 + b_2^{*2} + c^2 = a_2 b_2^* c.$$

Si $b_1^* = b_2^*$, en soustrayant on obtient :

$$a_1^2 - a_2^2 = b_1^* c(a_1 - a_2).$$

Ou bien $a_2 = a_1$, dans ce cas $(a_2, b_2, c) = (a_1, b_1, c)$ contredit l'hypothèse Z, ou bien $a_2 = b_1^* c - a_1$ et dans ce cas $b_2 = a_2 c - b_2^* = (b_1^* c - a_1)c - b_1^*$. On trouve alors le triplet :

$$(a_2, b_2, c) = (b_1^* c - a_1, (b_1^* c - a_1)c - b_1^*, c).$$

On vérifie facilement qu'il satisfait l'équation (2.1), mais aussi que l'on a :

$$a_1 < b_1 < c < b_1^* < b_1^* c - a_1 = a_2 < (b_1^* c - a_1)c - b_1^* = b_2.$$

On obtient aussi une contradiction car ce triplet devrait être un triplet de Zhang. Ce second cas est donc aussi impossible, de sorte que l'on a toujours $b_1^* \neq b_2^*$. En fait on peut en dire plus sur la comparaison des nombres b_1^* et b_2^*. Avec :

$$a_1 c + b_2 < (a_1 + 1)c \leq a_2 c < a_2 c + b_1,$$

on obtient :

$$b_1^* = a_1 c - b_1 < b_2^* = a_2 c - b_2.$$

On peut compléter avec :

$$c + b_1 < 2c < a_1 c.$$

Ceci donne :

$$c < b_1^* = a_1 c - b_1 < b_2^* = a_2 c - b_2. \tag{3.7}$$

- La précaution (3.5) sur l'ordre donne facilement :

$$a_1 a_2 < c^2. \tag{3.8}$$

On peut alors chercher à refaire le calcul donnant la relation qui a été démontrée dans [54] pour le cas où $b_1^* = b_2^* = b^*$. Le calcul est facile, et donne :

$$\begin{aligned}(a_2 c - c a_1)(c^2 - a_1 a_2) &= (a_1^2 + c^2)a_2 c - (a_2^2 + c^2)a_1 c \\ &= (a_1 c b_1^* - b_1^{*2})a_2 c - (a_2 c b_2^* - b_2^{*2})a_1 c \\ &= b_1^* b_1 a_2 c - b_2^* b_2 a_1 c,\end{aligned}$$

d'où en simplifiant par c :

$$(a_2 - a_1)(c^2 - a_1 a_2) = b_1^* b_1 a_2 - b_2^* b_2 a_1.$$

Comme on a supposé $a_1 < a_2$, on a :

$$b_2^* b_2 a_1 < b_1^* b_1 a_2,$$

et en croisant avec (3.7), il vient :

$$a_1 b_2 < b_1 a_2. \tag{3.9}$$

• Egalement on a :

$$\begin{aligned}(b_1a_2 - a_1b_2)(b_1b_2 - a_1a_2) &= (a_1^2 + b_1^2)a_2b_2 - (a_2^2 + b_2^2)a_1b_1 \\ &= (a_1cb_1 - c^2)a_2b_2 - (a_2cb_2 - c^2)a_1b_1 \\ &= c^2(a_1b_1 - a_2b_2).\end{aligned}$$

Mais avec (3.9) on a $(b_1a_2 - a_1b_2) > 0$, et avec (3.5) on trouve aussi $(b_1b_2 - a_1a_2) > 0$. Il en resulte que le produit est positif, et avec la dernière égalité :

$$a_2b_2 < a_1b_1. \tag{3.10}$$

Mais comme par l'hypothèse Z on a aussi $a_1 < a_2$, il reste :

$$b_2 < b_1. \tag{3.11}$$

Egalement :

$$a_2c - b_2 = b_2^* < a_2^* = b_2c - a_2 < a_1^* = b_1c - a_1,$$

Avec (3.5), (3.6) et (3.11), (3.7), on obtient alors une condition dont on vérifie faciliement en sens inverse qu'elle est équivalente à l'hypothèse Z :

$$a_1 < a_2 < b_2 < b_1 < c = c_1 = c_2 < b_1^* < b_2^* < a_2^* < a_1^*. \tag{3.12}$$

3.1.3. Six lemmes techniques

Soient deux triplets ibériques différents de même valeur dominante, on énonce ici divers lemmes techniques découlant de la condition $c = c_1 = c_2$.

Proposition 3.1. *Si $q \notin \{2, 3\}$ est un facteur premier de c, alors l'un au moins des deux nombres $a_1a_2 + b_1b_2$ et $a_1a_2 - b_1b_2$ n'est pas divisible par q. Il en est de même de l'un des deux nombres $a_1b_2 + b_1a_2$ et $a_1b_2 - b_1a_2$.*

Supposons qu'au contraire q divise $a_1a_2 + b_1b_2$ et $a_1a_2 - b_1b_2$, il divise $2a_1a_2$, et donc aussi a_1a_2, c'est à dire a_1 ou a_2, et donc respectivement b_1 ou b_2 puisqu'il divise également c. Mais avec l'équation de Markoff (2.1) on aurait alors $q = 3$, c'est à dire une contradiction avec l'hypothèse du lemme. Ce dernier est donc établi, sachant que le même raisonnement vaut pour l'autre paire de nombres $a_1b_2 + b_1a_2$ et $a_1b_2 - b_1a_2$.

Proposition 3.2. *Si $q \notin \{3\}$ est un facteur premier de c, alors :*
a/ q divise $a_1b_2 - b_1a_2$ si et seulement s'il divise $a_1a_2 + b_1b_2$,
b/ q divise $a_1a_2 - b_1b_2$ si et seulement s'il divise $a_1b_2 + b_1a_2$.

Supposons en effet que l'on ait $a_1b_2 - b_1a_2 \equiv 0 \pmod{q}$. On peut alors écrire modulo q, avec $q \neq 3$ diviseur de c, et donc pas de a_1 :

$$\begin{aligned} 0 &\equiv a_1a_2cb_1 \equiv a_2(a_1^2 + b_1^2) \equiv a_2(a_1^2) + b_1(a_2b_1) \\ &\equiv a_2(a_1^2) + b_1(a_1b_2) \equiv a_1(a_1a_2 + b_1b_2) \pmod{q}. \end{aligned}$$

Ceci impose que q soit un diviseur de $a_1a_2 + b_1b_2$ et démontre une partie l'énoncé a/ de la dernière proposition. Si inversement $a_1a_2 + b_1b_2 \equiv 0 \pmod{q}$, on peut écrire, avec $q \neq 3$ diviseur de c, et donc pas de b_1 :

$$\begin{aligned} 0 &\equiv a_1a_2cb_1 \equiv a_2(a_1^2 + b_1^2) \equiv a_1(a_1a_2) + a_2(b_1^2) \\ &\equiv -a_1(b_1b_2) + a_2(b_1^2) \equiv b_1(a_2b_1 - a_1b_2) \pmod{q}. \end{aligned}$$

Ceci impose que q soit un diviseur de $a_1b_2 - b_1a_2$ et termine la démonstration de l'énoncé a/ de la dernière proposition. L'énoncé b/ se vérifie de même à partir de $a_1a_2 - b_1b_2 \equiv 0 \pmod{q}$ avec :

$$\begin{aligned} 0 &\equiv a_1a_2cb_1 \equiv a_2(a_1^2 + b_1^2) \equiv a_1(a_1a_2) + b_1(a_2b_1) \\ &\equiv a_1(b_1b_2) + b_1(a_2b_1) \equiv b_1(a_1b_2 + a_2b_1) \pmod{q}. \end{aligned}$$

et à partir de $a_1b_2 + b_1a_2 \equiv 0 \pmod{q}$ avec :

$$\begin{aligned} 0 &\equiv a_1a_2cb_1 \equiv a_2(a_1^2 + b_1^2) \equiv a_1(a_1a_2) + b_1(a_2b_1) \\ &\equiv a_1(a_1a_2) - b_1(b_2a_1) \equiv a_1(a_1a_2 - b_1b_2) \pmod{q}. \end{aligned}$$

Proposition 3.3. *Supposons que l'on ait $c = c'q^e$ avec $q \notin \{2, 3\}$ facteur premier de c ne divisant pas c', alors ou bien q^{2e} divise $b_1a_2 - a_1b_2$, ou bien q^{2e} divise $b_1b_2 - a_1a_2$, mais on n'a pas simultanément ces deux propriétés.*

Cet énoncé résulte de l'égalité que l'on a démontrée ci-dessus :

$$(b_1a_2 - a_1b_2)(b_1b_2 - a_1a_2) = c^2(a_1b_1 - a_2b_2). \tag{3.13}$$

Le cas où q divise à la fois $b_1a_2 - a_1b_2$ et $b_1b_2 - a_1a_2$ est impossible. Si tel était le cas, par la proposition 3.2, q diviserait aussi $a_1a_2 + b_1b_2$ et $b_1b_2 - a_1a_2$,

et avec la proposition 3.1 on aurait une contradiction. Finalement q^{2e} qui divise c^2 divise soit $b_1a_2 - a_1b_2$, soit $b_1b_2 - a_1a_2$, mais pas les deux. La proposition est établie. L'application répétée de cette dernière permet en décomposant c en facteurs premiers $c = 2^{e_c}3\prod q_i^{e_i}$ de répartir les nombres premiers q_i en deux ensembles, ceux divisant $b_1a_2 - a_1b_2$ et ceux divisant $b_1b_2 - a_1a_2$. Ceci constuit un diviseur f de c et de $b_1a_2 - a_1b_2$ et un diviseur g de c et de $b_1b_2 - a_1a_2$. Ils sont définis de façon unique et sont premiers entre eux et à 2 ou 3. Les vérifications complémentaires étant évidentes, on a :

Proposition 3.4. *On peut factoriser c de façon unique sous la forme $c = 2^{e_c}3fg$, où f et g sont deux entiers premiers entre eux et premiers à 6 tels que f^2 divise $b_1a_2 - a_1b_2$ et g^2 divise $b_1b_2 - a_1a_2$. De plus f n'a aucun facteur commun avec $b_1b_2 - a_1a_2$, ni avec $a_1b_2 + b_1a_2$, et g n'a aucun facteur premier commun avec $b_1a_2 - a_1b_2$, ni avec $a_1a_2 + b_1b_2$.*

▷ **Notations 4** : Deux triplets ibériques différents (a_1, b_1, c) et (a_2, b_2, c) étant donnés de même valeur dominante c, on note avec la proposition 3.4 :

$$c = 3\gamma = 2^{e_c}3\mathfrak{c} = 2^{e_c}3fg,\ e_c \in \{0,1\},\ \mathfrak{c} \text{ premier à } 6,\ f \text{ et } g \text{ premiers entre eux.}$$

Si on prolonge les conditions de la proposition 3.4 pour $(a_1, b_1, c) = (a_2, b_2, c)$, on a :

$$f^2 \mid a_1b_1 - b_1a_1 = 0, \qquad g^2 \mid a_1^2 - b_1^2.$$

Ces deux conditions de divisibilité sont assurées avec $(f, g) = (\mathfrak{c}, 1)$. Dans le cas où $(b_1, a_1, c) = (a_2, b_2, c)$ on a de même :

$$f^2 \mid a_1^2 - b_1^2, \qquad g^2 \mid a_1b_1 - b_1a_1 = 0.$$

Ces conditions de divisibilité sont assurées avec $(f, g) = (1, \mathfrak{c})$. Ces deux cas sont dits être les **cas limites pour le couple** (f, g). Ils peuvent être vérifiés de façon plus précise. Considérons par exemple $(a_1, b_1, c) = (a_2, b_2, c)$. On y factorise c sous la forme $c = 2^{e_c}3\mathfrak{c}$, l'équation de Markoff impose que $\mathfrak{c}$ divise $a_1^2 + b_1^2$. Mais alors $\mathfrak{c}$ n'a aucun facteur commun avec $b_1^2 - a_1^2 = b_1b_2 - a_1a_2$. Ceci impose $g = 1$

et $f = \mathfrak{c}$, c'est à dire $(f, g) = (\mathfrak{c}, 1)$. Dans l'autre cas où $(a_2, b_2, c_2) = (b_1, a_1, c)$, on utilise encore la décomposition $c = 2^{e_c}3\mathfrak{c}$, par contre on a cette fois $\mathfrak{c}$ sans facteur commun avec $b_1^2 - a_1^2 = a_2b_1 - b_2a_1$, soit $f = 1$ et $g = \mathfrak{c}$, c'est à dire $(f, g) = (1, \mathfrak{c})$.

Inversement, il s'agit de s'assurer que les deux cas limites pour (f, g) correspondent aux seuls cas que l'on vient de voir pour les triplets. On veut donc démontrer que si $(f, g) = (1, \mathfrak{c})$, alors $(b_1, a_1, c) = (a_2, b_2, c)$, et que si $(f, g) = (\mathfrak{c}, 1)$, alors $(a_1, b_1, c) = (a_2, b_2, c)$. Le premier cas n'est jamais rencontré si l'on suppose avoir affaire à deux triplets de Zhang, comme le prévoit par exemple l'hypothèse Z.

Supposons ici $(b_1, a_1, c) \neq (a_2, b_2, c)$ et $(f, g) = (1, \mathfrak{c})$. La décomposition de c en facteurs premiers $c = 2^{e_c}3\prod q_i^{e_i}$ a permis par la proposition 3.4 de répartir les nombres premiers q_i pour construire les deux nombres f et g qui n'ont pas de facteur premier égal à 2 ou 3. Comme on a $g = \mathfrak{c}$, en revenant à l'égalité 3.13 et se souvenant que g^2 divise $b_1b_2 - a_1a_2$, il vient :

$$(\frac{b_1b_2 - a_1a_2}{3g^2})(b_1a_2 - a_1b_2) = 2^{2e_c}(a_1b_1 - a_2b_2).$$

Ceci montre que $(3\mathfrak{c})^2$, c'est à dire c^2 ou $(c/2)^2$, divise $(b_1b_2 - a_1a_2) > 0$. On a donc :

$$(3\mathfrak{c})^2 \leq (b_1b_2 - a_1a_2) < b_2b_1 < b_1^2.$$

De là on conclut facilement que $3\mathfrak{c}$ est moindre que le nombre b_1. Le premier cas où $c = 3\mathfrak{c}$ impose alors $c < b_1$. On trouve une contradiction avec le fait que c est le terme dominant du triplet (b_1, a_1, c). Reste le second cas où $e_c = 1$, et où avec des termes positifs on a :

$$(\frac{b_1b_2 - a_1a_2}{3\mathfrak{c}^2})(b_1a_2 - a_1b_2) = 2^2(a_1b_1 - a_2b_2).$$

Le nombre c étant pair, puisque :

$$\text{pgcd}(a_1, c) = \text{pgcd}(b_1, c) = \text{pgcd}(a_2, c) = \text{pgcd}(b_2, c) = 3,$$

on a a_1, b_1, a_2, b_2 impairs. Ceci donne :

$$2 \mid (a_1b_1 - a_2b_2), \qquad 8 \mid (b_1b_2 - a_1a_2)(b_1a_2 - a_1b_2).$$

Si $4 \mid (b_1b_2 - a_1a_2)$ on trouve comme précédemment $c < b_1$ et donc une contradiction. Le seul cas restant à regarder est celui où 4 n'est pas un diviseur de

$\mathbf{B} = (b_1b_2 - a_1a_2)$, mais divise $\mathbf{A} = (b_1a_2 - a_1b_2)$. Or on peut faire le tableau suivant décrivant toutes les possibilités de résidus modulo 4 suivant :

a_1	a_2	b_1	b_2	$\mathbf{B} = (b_1b_2 - a_1a_2)$	$4 \nmid \mathbf{B}$	$\mathbf{A} = (b_1a_2 - a_1b_2)$	$4 \mid \mathbf{A}$
1	1	1	1	0		0	ok
1	1	1	3	2	ok	2	
1	1	3	1	2	ok	2	
1	1	3	3	0		0	ok
1	3	1	1	2	ok	2	
1	3	1	3	0		0	ok
1	3	3	1	0		0	ok
1	3	3	3	2	ok	2	
3	1	1	1	2	ok	2	
3	1	1	3	0		0	ok
3	1	3	1	0		0	ok
3	1	3	3	2	ok	2	
3	3	1	1	0		0	ok
3	3	1	3	2	ok	2	
3	3	3	1	2	ok	2	
3	3	3	3	0		0	ok

Tableau n°2.

Ce tableau montre que le cas restant ne se produit jamais et que l'on a donc une contradiction. Ainsi la condition $(f, g) = (1, \mathfrak{c})$ impose-t-elle $(b_1, a_1, c) = (a_2, b_2, c)$.

Supposons maintenant $(a_1, b_1, c) \neq (a_2, b_2, c)$ et $(f, g) = (\mathfrak{c}, 1)$. La décomposition de c en facteurs premiers $c = 2^{e_c} 3 \prod q_i^{e_i}$ a permis par la proposition 3.4 de répartir les nombres premiers q_i pour construire les deux nombres f et g qui n'ont pas de facteur premier égal à 2 ou 3. Comme on a $f = \mathfrak{c}$, en revenant à l'égalité (3.13) et se souvenant que f^2 divise $b_1a_2 - a_1b_2$, il vient :

$$(b_1b_2 - a_1a_2)(\frac{b_1a_2 - a_1b_2}{3f^2}) = 2^{2e_c}(a_1b_1 - a_2b_2).$$

Ceci montre que $(3\mathfrak{c})^2$, c'est à dire c^2 ou $(c/2)^2$, divise $(b_1a_2 - a_1b_2) > 0$. On a donc :

$$(3\mathfrak{c})^2 \leq (b_1a_2 - a_1b_2) < a_2b_1 < b_1^2.$$

De là on conclut facilement que $3\mathfrak{c}$ est moindre que le nombre b_1. Le cas où $c = 3\mathfrak{c}$ impose alors $c < b_1$. On trouve une contradiction avec le fait que (a_1, b_1, c) est

un triplet de Zhang. Reste le cas où $e_c = 1$, où avec des termes positifs on a :

$$(b_1b_2 - a_1a_2)(\frac{b_1a_2 - a_1b_2}{3\mathfrak{c}^2}) = 2^2(a_1b_1 - a_2b_2).$$

Le nombre c étant alors pair, et puisque :

$$\text{pgcd}(a_1, c) = \text{pgcd}(b_1, c) = \text{pgcd}(a_2, c) = \text{pgcd}(b_2, c) = 3,$$

on a encore a_1, b_1, a_2, b_2 impairs. Ceci donne :

$$2 \mid (a_1b_1 - a_2b_2), \qquad 8 \mid (b_1b_2 - a_1a_2)(b_1a_2 - a_1b_2).$$

Si $4 \mid (b_1a_2 - a_1b_2)$ on trouve comme précédemment $c < b_1$ et donc une contradiction. Le seul cas restant à regarder est celui où 4 n'est pas un diviseur de $\mathbf{A} = (b_1a_2 - a_1b_2)$, mais divise $\mathbf{B} = (b_1b_2 - a_1a_2)$. On peut alors considérer le tableau précédent des résidus modulo 4. Il montre que cas ne se produit jamais et que l'on a encore une contradiction. Ainsi la condition $(f, g) = (\mathfrak{c}, 1)$ donne-t-elle $(a_1, b_1, c) = (a_2, b_2, c)$. On peut donc énoncer :

Proposition 3.5. *Dans la factorisation unique de* $c = 2^{e_c}3\mathfrak{c} = 2^{e_c}3fg \notin \{3, 6\}$, *donnée par la proposition 3.4, avec* f *et* g *deux entiers premiers entre eux et premiers à* 6 *tels que* f^2 *divise* $b_1a_2 - a_1b_2$ *et* g^2 *divise* $b_1b_2 - a_1a_2$, *on est certain de pouvoir trouver des facteurs premiers* q_i *différents dans* f *et dans* g, *et différénts de* 2 *et* 3 *dès que l'on a* $\{f, g\} \neq \{1, \mathfrak{c}\}$. *Si au contraire* $\{f, g\} \neq \{1, \mathfrak{c}\}$ *on a* $(f, g) = (\mathfrak{c}, 1)$ *dans le cas où* $(a_1, b_1, c) = (a_2, b_2, c)$, *et* $(f, g) = (1, \mathfrak{c})$ *dans le cas où* $(b_1, a_1, c) = (a_2, b_2, c)$. *Ce dernier cas ne se rencontre jamais lorsque est assurée l'hypothèse Z.*

On a un dernier résultat qui généralise la proposition 3.2 :

Proposition 3.6. *Si* f *et* g *nombres impairs premiers à* 6 *sont des diviseurs de* c, *alors :*

a/ f *divise* $b_1a_2 - a_1b_2$ *si et seulement s'il divise* $a_1a_2 + b_1b_2$,

b/ g *divise* $b_1b_2 - a_1a_2$ *si et seulement s'il divise* $a_1b_2 + b_1a_2$.

Supposons en effet que l'on ait avec h entier $b_1a_2 - a_1b_2 = fh$. On peut alors écrire, avec f diviseur de c et premier à 3, donc premier à a_1 :

$$\begin{aligned} 0 &\equiv a_1a_2cb_1 \equiv a_2(a_1^2 + b_1^2) \equiv a_2(a_1^2) + b_1(a_2b_1) \\ &\equiv a_2(a_1^2) + b_1(a_1b_2) \equiv a_1(a_1a_2 + b_1b_2) \pmod{f}. \end{aligned}$$

Ceci impose que f soit un diviseur de $a_1a_2 + b_1b_2$ et démontre une partie de l'énoncé a/ de la dernière proposition. Supposons inversement qu'avec h entier, on ait $a_1a_2 + b_1b_2 = fh$. On peut alors écrire, avec f diviseur de c et premier à 3, donc premier à b_1 :

$$\begin{aligned} 0 &\equiv a_1a_2cb_1 \equiv a_2(a_1^2 + b_1^2) \equiv a_1(a_1a_2) + a_2(b_1^2) \\ &\equiv -a_1(b_1b_2) + a_2(b_1^2) \equiv b_1(a_2b_1 - a_1b_2) \pmod{f}. \end{aligned}$$

Ceci impose que f soit un diviseur de $b_1a_2 - a_1b_2$ et démontre complètement l'énoncé a/ de la proposition. L'énoncé b/ se vérifie de même en transposant avec g les deux suites de congruences qui ont été utilisées pour démontrer la proposition 3.2.

3.2. Adaptation aux triplets ibériques des résultats de Cassels

3.2.1. Rappels sur la présentation de Cassels

On considère ici un triplet ibérique (a, b, c) que l'on suppose **non singulier**, c'est à dire différent de $(3, 3, 3)$ et $(3, 3, 6)$. On remarque qu'il est équivalent de dire que $(c/3, b/3, a/3)$ est un triplet de Cassels non singulier, c'est à dire différent de $(1, 1, 1)$ et $(2, 1, 1)$. On peut alors traduire les résultats de [13] (p. 27-30) sur nos triplets ibériques en remplaçant les notations de Cassels, c'est à dire m par γ, m_1 par β, et m_2 par α. On note de plus, en cohérence avec les notations a^*, b^*, c^*, utilisées avant :

$$\alpha^* = 3\beta\gamma - \alpha,\ \beta^* = 3\gamma\alpha - \beta,\ \gamma^* = 3\alpha\beta - \gamma.$$

Et l'on a ainsi (avec les notations de Cassels $m' = \gamma^*$, $m'_1 = \beta^*$, et $m'_2 = \alpha^*$) :

$$\gamma = \max(\gamma, \beta, \alpha),$$

$$\gamma^* < \max(\beta, \alpha) < \gamma,$$

$$\beta^* > \max(\gamma, \alpha) = \gamma, \qquad \alpha^* > \gamma.$$

En notant comme Cassels avec x, y, z entiers :

$$x \equiv \frac{y}{z} \pmod{m} \Longleftrightarrow m \mid xz - y,$$

on peut identifier trois nombres k, k_1, k_2 vérifiant :

$$k \equiv \frac{\alpha}{\beta} \equiv \frac{-\beta}{\alpha} \pmod{\gamma}, \qquad 0 \leq k < \gamma, \tag{3.14}$$

$$k_1 \equiv \frac{\gamma}{\alpha} \equiv \frac{-\alpha}{\gamma} \pmod{\beta}, \qquad 0 \leq k_1 < \beta, \tag{3.15}$$

$$k_2 \equiv \frac{\beta}{\gamma} \equiv \frac{-\gamma}{\beta} \pmod{\alpha}, \qquad 0 < k_2 \leq \alpha. \tag{3.16}$$

Le nombre k est construit par le théorème de Bezout, avec puisque $\text{pgcd}(\beta, \gamma) = 1$, l'existence de deux entiers u_β et u_γ tels que :

$$\beta u_\beta - \gamma u_\gamma = 1,$$

soit en multipliant par α et posant $k = u_\beta \alpha$:

$$\beta k - \gamma u_\gamma \alpha \equiv \beta k \equiv \alpha \pmod{\gamma},$$

en multipliant par β et utilisant l'équation (1.1) :

$$\beta^2 k \equiv -\alpha^2 k \equiv \alpha\beta \pmod{\gamma},$$

soit en simplifiant par β qui est premier à γ :

$$\alpha k \equiv -\beta \pmod{\gamma}.$$

On vient donc d'établir (3.14). Les conditions (3.15) et (3.16) s'établissent de même. Cassels indique que les inégalités strictes $<$ dans ces trois conditions doivent être considérées comme des inégalités larges $\leq$ si α, β, γ valent 1. Le cas où $\gamma = 1$ donnerait une contradiction puisqu'on a supposé que le triplet (a, b, c) est ibérique ($\max(a, b, c) = c$) et non singulier. Il n'a pas à être considéré ici. Cassels déduit l'existence d'entiers l, l_1, l_2 tels que l'on puisse écrire :

$$k^2 + 1 = l\gamma, \qquad k_1^2 + 1 = l_1\beta, \qquad k_2^2 + 1 = l_2\alpha. \tag{3.17}$$

On a en effet une congruence qu'il suffit de simplifier par β premier à γ :

$$\beta k^2 \equiv \alpha k \equiv -\beta \pmod{\gamma}.$$

En montrant alors que $\gamma k_2 - \alpha k - \beta$ est congru à 0 modulo $\alpha\gamma$, et strictement compris entre $-\alpha\gamma$ et $\alpha\gamma$, Cassels en déduit que l'on a :

$$\gamma k_2 - \alpha k = \beta. \tag{3.18}$$

De même :

$$\beta k - \gamma k_1 = \alpha. \tag{3.19}$$

$$\beta k_2 - \alpha k_1 = \gamma^* = 3\alpha\beta - \gamma. \tag{3.20}$$

Remarquons ici que l'on ne peut avoir $k = 0$, sans quoi on trouverait $\gamma = 1$. Ce cas est exclus par l'hypothèse faite que (a, b, c) est ibérique et non singulier. Pour la suite l'inégalité large apparaissant dans la condition (3.14) doit être remplacée par une inégalté stricte.

• Sur les formes quadratiques, Cassels considère dans [13] l'expression :

$$\gamma x^2 + (3\gamma - 2k)xy + (l - 3k)y^2.$$

C'est à ce niveau (p. 33) qu'il se pose la question de la conjecture de Frobenius car il voudrait noter une telle forme $\gamma F_\gamma(x, y)$. Mais il faudrait, pour qu'il n'y ait pas de problème, que γ détermine une valeur k (donc l) de façon unique, c'est à dire que la correspondance $\gamma \longrightarrow F_\gamma(x, y)$ soit injective. Or il montre d'abord que pour $k' = \gamma - k$ on a $l' = \gamma - 2k + l$ on trouve une seconde forme qui devrait également être notée $\gamma F_\gamma(x, y)$. Elle vérifie :

$$\begin{aligned} & \gamma x^2 + (3\gamma - 2k')xy + (l' - 3k')y^2 \\ = \ & \gamma(x + 2y)^2 + (3\gamma - 2k)(x + 2y)(-y) + (l - 3k)(-y)^2. \end{aligned}$$

Elle est déductible de la précédente par la transformation :

$$\begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \in GL(2, \mathbb{Z}).$$

On pourrait raisonner à une équivalence près pour l'action de $GL(2, \mathbb{Z})$ sur les formes quadratiques afin que la notation $\gamma F_\gamma(x, y)$ désigne un unique objet. Mais même ce faisant il reste une ambigüité sur la notation tant que la conjecture de Frobenius n'est pas établie. C'est la raison pour laquelle dans [40] (p. 18) on a plutôt noté cette forme γF_θ, où $\theta = \theta_2(S)$ est un nombre algébrique de degré 2 et positif dont le développement en fraction continue est périodique :

$$\theta_2(S) = [0, \underline{S^*, 2}] = \frac{2k - 3\gamma + \sqrt{9\gamma^2 - 4}}{2\gamma}.$$

Avec le conjugué de $\theta_2(S)$ que l'on écrit $\overline{\theta} = \overline{\theta_2(S)}$ et qui est négatif, on a :

$$\begin{aligned} F_\theta(x, y) &= (x - \theta_2(S)y)(x - \overline{\theta_2(S)}y) = x^2 + (\frac{3\gamma - 2k}{\gamma})xy + (\frac{l - 3k}{\gamma})y^2 \\ &= (x - \frac{2k - 3\gamma + \sqrt{9\gamma^2 - 4}}{2\gamma}y)(x - \frac{2k - 3\gamma - \sqrt{9\gamma^2 - 4}}{2\gamma}y). \end{aligned}$$

$$\gamma F_\theta(x, y) = \gamma x^2 + (3\gamma - 2k)xy + (l - 3k)y^2 \in \mathbb{Z}[x, y].$$

3.2.2. Des relations nouvelles non mentionnées par Cassels

En combinant les relations (3.14) à (3.20) que l'on vient de voir, on en découvre de nouvelles que Cassels ne cite pas dans [13]. Par exemple en éliminant α entre (3.18) et (3.19) :

$$k_1 k + k_2 = \beta l, \tag{3.21}$$

en faisant disparaitre β entre (3.18) et (3.19) :

$$k_2 k - k_1 = \alpha l. \tag{3.22}$$

Eliminant β entre (3.18) et (3.20), et traitant le reste avec les relations connues :

$$(\gamma k_2 - \alpha k)k_2 - \alpha k_1 = 3\alpha(\gamma k_2 - \alpha k) - \gamma,$$

$$\alpha l_2 \gamma - k\alpha k_2 - k_1\alpha = \gamma + \gamma k_2^2 - k\alpha k_2 - k\alpha = -3k\alpha^2 + 3\gamma k_2 \alpha,$$

$$l_2\gamma - kk_2 - k_1 = -3k\alpha + 3\gamma k_2,$$

$$k_1 = 3k\alpha - kk_2 - 3\gamma k_2 + l_2\gamma, \tag{3.23}$$

$$k_1 + kk_2 = -3\beta + l_2\gamma. \tag{3.24}$$

Comparant avec (3.22) :

$$2k_1 = -\alpha l - 3\beta + l_2\gamma. \tag{3.25}$$

En éliminant α entre (3.19) et (3.20) :

$$\beta k_2 - (\beta k - \gamma k_1)k_1 = 3(\beta k - \gamma k_1)\beta - \gamma$$

$$k_2 = 3k\beta + kk_1 - 3\gamma k_1 - l_1\gamma = 3\alpha + kk_1 - l_1\gamma,$$

$$k_2 - kk_1 = 3\alpha - l_1\gamma. \tag{3.26}$$

Comparant avec (3.21) ;

$$2k_2 = 3\alpha + \beta l - l_1\gamma, \tag{3.27}$$

également, en multipliant simplement par l la précédente égalité :

$$lk_2 - lkk_1 = 3\alpha l - l_1 k^2 - l_1,$$

$$l_1 = 3\alpha l - lk_2 - l_1 k^2 + lkk_1. \tag{3.28}$$

On va maintenant établir que :

$$-l_1 k^2 + lkk_1 = -3kk_2 + kl_2,$$

divisant par k :

$$-l_1 k + l k_1 = -3k_2 + l_2,$$
$$l_2 = 3k_2 + l k_1 - l_1 k, \tag{3.29}$$

multipliant par γ et avec (3.18) et (3.19) :

$$l_2\gamma = 3k_2\gamma + l k_1\gamma - l_1 k\gamma = 3\beta + 3\alpha k - l\alpha + l\beta k - l_1 k\gamma,$$

d'où avec (3.25) :

$$2k_1 = -\alpha l - 3\beta + l_2\gamma = 3\alpha k + l\beta k - l_1 k\gamma - 2l\alpha, \tag{3.30}$$

et en comparant avec (3.27) multipliée par k :

$$2k_1 = 2k_2 k - 2l\alpha.$$

Or cette égalité qui n'est autre que (3.22) est assurée. On a donc :

$$-l_1 k^2 + l k k_1 = -3k k_2 + k l_2. \tag{3.31}$$

En comparant alors (3.28) et (3.31) on conclut que l'on a :

$$l_1 = 3l\alpha - 3k k_2 + k l_2 - l k_2 = -3k_1 + k l_2 - l k_2. \tag{3.32}$$

3.2.3. Rappels sur le formalisme des fractions continues

On considère de façon générale des suites finies d'entiers strictement positifs :

$$S = (\omega_0, \omega_1, ..., \omega_n).$$

Suivant [40], la **fraction continue** ou **réduite d'ordre** n définie par la suite S est :

$$[S] = [\omega_0, \omega_1, ..., \omega_n] = \omega_0 + \cfrac{1}{\omega_1 + \cfrac{1}{... + \cfrac{1}{\omega_n}}} = \frac{p_n}{q_n} \in \mathbb{Q}. \tag{3.33}$$

La **suite miroir** (ou **duale**) de la suite S est notée :

$$S^* = (\omega_n, \omega_{n-1}, ..., \omega_0).$$

On dit que S est une suite **palindrome** (ou **autoduale**) si et seulement $S = S^*$. On associe à toute suite S sa **suite étendue sur la droite** avec :

$$S\triangleright = \left\{ \begin{array}{ll} (\omega_0, \omega_1, ..., \omega_n - 1, 1) & \text{si } \omega_n \neq 1 \\ (\omega_0, \omega_1, ..., \omega_{n-1} + 1) & \text{si } \omega_n = 1 \end{array} \right\},$$

Par construction, on a pour les fractions continues :

$$[S] = [S\triangleright].$$

Avec l'opération miroir, on définit la **suite étendue sur la gauche** avec :

$$\triangleleft S = (S^*\triangleright)^*.$$

La **matrice de la suite** S notée $M_S \in GL(2, \mathbb{Z})$ ou $M(S)$ est définie comme étant :

$$M_S = \left[\begin{array}{cc} \omega_0 & 1 \\ 1 & 0 \end{array} \right] ... \left[\begin{array}{cc} \omega_n & 1 \\ 1 & 0 \end{array} \right] = \left[\begin{array}{cc} m & K_1 \\ m - K_2 & K_1 - l \end{array} \right] = \left[\begin{array}{cc} p_n & p_{n-1} \\ q_n & q_{n-1} \end{array} \right] \quad (3.34)$$

son **extension** est le nombre :

$$m_S = m,$$

son **déterminant** est :

$$\varepsilon_S = \det(M_S) = K_1K_2 - ml = (-1)^{n+1} = \pm 1, \quad (3.35)$$

sa **trace** est :

$$tr(M_S) = (m + K_1 - l), \quad (3.36)$$

sa **cotrace** et son **écart de palindromie** valent respectivement :

$$co(M_S) = (m - K_2 - K_1), \qquad \rho = \rho(M_S) = \frac{co}{m}, \quad (3.37)$$

son **antitrace** et son **écart d'antidromie** sont respectivement définis par :

$$\partial K(M_S) = (K_1 - K_2), \qquad r = r(M_S) = \frac{\partial K}{m}. \quad (3.38)$$

Pour la suite vide :

$$M_\varnothing = \mathbf{1}_2 = \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right].$$

La transposition des matrices correspond à l'opération miroir pour les suites. Elle est notée :

$$^tM_S = M_{S^*}.$$

D'autre part, les deux opérateurs d'extension des suites à droite et à gauche conduisent à poser :

$$M(\triangleleft) = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = {}^tM(\triangleright) \in GL(2,\mathbb{Z}).$$

• On fait apparaitre des nombres algébriques de degré 2 dont le développement en fraction continue est périodique et s'écrit, avec ω et une suite d'entiers positifs $S^* = (\omega_n, \omega_{n-1}, ..., \omega_0)$, c'est à dire une **période** :

$$\theta_\omega(S) = [0, \underline{S^*, \omega}] = [0, S^*, \omega, S^*, \omega, S^*, \omega, ...]. \tag{3.39}$$

Plus généralement ([29] Theorem 177 p. 144) à l'action près d'une matrice de $GL(2,\mathbb{Z})$ tout algébrique de degré 2 se réduit sous cette forme avec (S^*, ω) une période d'entiers strictement positifs. Sachant que la matrice de la suite S^* est donnée par une expression déduite de (3.34), valable même si $S^* = \varnothing$, l'expression de $M_{(S^*,\omega)}$, matrice de la période du nombre $\theta_\omega(S)$, est alors :

$$M_{(S^*,\omega)} = \begin{bmatrix} (\omega+1)m - K_2 & m \\ (\omega+1)K_1 - l & K_1 \end{bmatrix}.$$

Ceci permet d'identifier une matrice $M_{(0,S^*,\omega,0)}$ non triviale qui laisse le nombre $\theta_\omega(S)$ invariant :

$$M_{(0,S^*,\omega,0)}(\theta_\omega(S)) = \begin{bmatrix} K_1 & (\omega+1)K_1 - l \\ m & (\omega+1)m - K_2 \end{bmatrix}(\theta_\omega(S)) = \theta_\omega(S). \tag{3.40}$$

Elle donne l'expression algébrique du **nombre de Markoff** $\theta_\omega(S) = [0, \underline{S^*, \omega}]$:

$$\theta_\omega(S) = \frac{K_1 + K_2 - (\omega+1)m + \sqrt{((\omega+1)m + K_1 - K_2)^2 + 4\varepsilon_S}}{2m}, \tag{3.41}$$

où apparait le **discriminant** qui n'est pas un carré d'entier :

$$\Delta_\omega(S) = ((\omega+1)m + K_1 - K_2)^2 + 4\varepsilon_S > 0. \tag{3.42}$$

Le **nombre de Markoff conjugué** s'écrit alors :

$$\overline{\theta_\omega(S)} = \frac{K_1 + K_2 - (\omega+1)m - \sqrt{((\omega+1)m + K_1 - K_2)^2 + 4\varepsilon_S}}{2m}, \qquad (3.43)$$

il a pour décomposition en fraction continue :

$$\overline{\theta_\omega(S)} = [-(\omega+1), 1, \omega_0 - 1, \underline{\omega_1, ..., \omega_n, \omega, \omega_0}] = [-(\omega+1), \lhd S, \underline{\omega, S}]. \qquad (3.44)$$

Par construction $\theta_\omega(S)$ est strictement compris entre 0 et 1, et donc positif, et $\overline{\theta_\omega(S)}$ est strictement compris entre $-(\omega+1)$ et $-\omega$, donc négatif.

• Les deux nombres $\theta = \theta_\omega(S)$ et $\overline{\theta_\omega(S)}$ définissent une **forme de Markoff** qui leur est associée :

$$F_\theta(x,y) = (x - \theta_\omega(S)y)(x - \overline{\theta_\omega(S)}y) = x^2 - \beta_0^\theta xy + \gamma_0^\theta y^2. \qquad (3.45)$$

Les expressions algébriques (3.41) et (3.43) permettent d'expliciter :

$$F_\theta(x,y) = x^2 + \left[\frac{(\omega+1)m - K_1 - K_2}{m}\right] xy + \left[\frac{l - (\omega+1)K_1}{m}\right] y^2, \qquad (3.46)$$

d'où une forme quadratique binaire entière $mF_\theta(x,y) \in \mathbb{Z}[x,y]$:

$$mF_\theta(x,y) = mx^2 + ((\omega+1)m - K_2 - K_1)xy + (l - (\omega+1)K_1)y^2. \qquad (3.47)$$

Toute forme $F_\theta(x,y)$ peut être vue comme un déterminant dans $\mathbb{Q}[x,y]$ avec :

$$\mathbf{A}_1 = \left[\frac{(\omega+1)m - K_1 - K_2}{m}\right], \ \mathbf{A}_0\mathbf{A}_2 = \left[\frac{l - (\omega+1)K_1}{m}\right],$$

on a en effet :

$$F_\theta(x,y) = \det \begin{bmatrix} x & -\mathbf{A}_0 y \\ \mathbf{A}_2 y & x + \mathbf{A}_1 y \end{bmatrix} = \det \left(x\mathbf{1}_2 - y \begin{bmatrix} 0 & \mathbf{A}_0 \\ -\mathbf{A}_2 & -\mathbf{A}_1 \end{bmatrix} \right). \qquad (3.48)$$

En calculant le polynôme caractéristique de la matrice apparaissant ainsi, et en comparant à l'expression (3.45), on est conduit à introduire naturellement un monomorphisme :

$$\pi : (x - \theta_\omega(S)y) \longrightarrow \left(x\mathbf{1}_2 - y \begin{bmatrix} 0 & \mathbf{A}_0 \\ -\mathbf{A}_2 & -\mathbf{A}_1 \end{bmatrix} \right). \qquad (3.49)$$

Ceci donne à considérer un anneau $\mathbb{Z}[\theta_\omega(S)]$ de nombres algébriques de degré 2 engendré par $\theta_\omega(S)$ (ou le corps $\mathbb{Q}[\theta_\omega(S)]$ selon la nature de x et y), et sa représentation matricielle image par π dans $\mathbf{M}_2(\mathbb{Z})$ (respectivement dans $\mathbf{M}_2(\mathbb{Q})$). Dans cet anneau $F_\theta(x,y)$ s'interprète comme une **norme**. D'où la propriété de multiplication :

$$F_\theta(x,y)F_\theta(x',y') = F_\theta((x'x - y'y\mathbf{A}_0\mathbf{A}_2),(xy + y'x + y'y\mathbf{A}_1)). \tag{3.50}$$

L'inverse $\theta_\omega(S)^{-1} = [\underline{S^*,\omega}]$ de $\theta_\omega(S)$ correspond à la matrice :

$$\pi(\theta_\omega(S)^{-1}) = \frac{1}{\mathbf{A}_0\mathbf{A}_2}\begin{bmatrix} -\mathbf{A}_1 & -\mathbf{A}_0 \\ \mathbf{A}_2 & 0 \end{bmatrix} = \left(\frac{-\mathbf{A}_1}{\mathbf{A}_0\mathbf{A}_2}\mathbf{1}_2 - \frac{1}{\mathbf{A}_0\mathbf{A}_2}\begin{bmatrix} 0 & \mathbf{A}_0 \\ -\mathbf{A}_2 & -\mathbf{A}_1 \end{bmatrix}\right),$$

et le conjugué donne quant à lui :

$$\pi(\overline{\theta_\omega(S)}) = \begin{bmatrix} -\mathbf{A}_1 & -\mathbf{A}_0 \\ \mathbf{A}_2 & 0 \end{bmatrix}.$$

Ceci permet d'écrire matriciellement la forme quadratique $F_\theta(x,y)$:

$$\pi(F_\theta(x,y)) = \begin{bmatrix} x & -\mathbf{A}_0y \\ \mathbf{A}_2y & x + \mathbf{A}_1y \end{bmatrix}\begin{bmatrix} x + \mathbf{A}_1y & \mathbf{A}_0y \\ -\mathbf{A}_2y & x \end{bmatrix} = F_\theta(x,y)\mathbf{1}_2.$$

Cette expression est invariante si l'on remplace (x,y) par $(-x,-y)$, et de même si l'on remplace y par $-y$ et x par $x + \mathbf{A}_1y$:

$$F_\theta(x + \mathbf{A}_1y, -y)\mathbf{1}_2 = \begin{bmatrix} x + \mathbf{A}_1y & \mathbf{A}_0y \\ -\mathbf{A}_2y & x \end{bmatrix}\begin{bmatrix} x & -\mathbf{A}_0y \\ \mathbf{A}_2y & x + \mathbf{A}_1y \end{bmatrix} = F_\theta(x,y)\mathbf{1}_2.$$

On vient donc d'identifier deux matrices qui permutent :

$$\pi(x - \theta_\omega(S)y) = \begin{bmatrix} x & -\mathbf{A}_0y \\ \mathbf{A}_2y & x + \mathbf{A}_1y \end{bmatrix},\ \pi(x - \overline{\theta_\omega(S)}y) = \begin{bmatrix} x + \mathbf{A}_1y & \mathbf{A}_0y \\ -\mathbf{A}_2y & x \end{bmatrix}.$$

Et l'on a dégagé l'égalité suivante (où $\mathbf{A}_1 \in \mathbb{Q}$) :

$$F_\theta(x,y) = F_\theta(x + \mathbf{A}_1y, -y).$$

- Ceci conduit pour toute forme quadratique $F(x,y)$ et toute matrice :

$$T = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix},$$

à définir une nouvelle forme $(F \circ T)$ obtenue par action de T sur F :

$$(F \circ T)(x, y) = F(v_{11}x + v_{12}y, v_{21}x + v_{22}y). \tag{3.51}$$

On peut formaliser cette opération en introduisant la **matrice de la forme** $F(x, y) = \alpha x^2 - \beta xy + \gamma y^2$:

$$\Psi_F = \begin{bmatrix} \alpha & -\frac{\beta}{2} \\ -\frac{\beta}{2} & \gamma \end{bmatrix}, \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \alpha & -\frac{\beta}{2} \\ -\frac{\beta}{2} & \gamma \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = F(x, y),$$

on a :

$$\Psi_{(F \circ T)} = \left({}^t \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} \right) \begin{bmatrix} \alpha & -\frac{\beta}{2} \\ -\frac{\beta}{2} & \gamma \end{bmatrix} \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}. \tag{3.52}$$

L'**orbite** de F pour cette action est l'ensemble des formes $(F \circ T)$ où T décrit l'ensemble considéré pour ces matrices ($GL(2, \mathbb{Z})$, $GL(2, \mathbb{Q})$, ...). Le **stabilisateur** $\Sigma(F)$ de F est l'ensemble des matrices T qui la laisse invariante. En particulier on a vu que F_θ est invariante par les deux matrices suivantes qui sont dans son stabilisateur :

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in GL(2, \mathbb{Z}), \qquad \begin{bmatrix} 1 & \mathbf{A}_1 \\ 0 & -1 \end{bmatrix} \in GL(2, \mathbb{Q}).$$

Si $F(x, y) = (x - \xi y)(x - \overline{\xi} y)$ et $(F \circ T)(x, y) = (x - \xi' y)(x - \overline{\xi}' y)$, on a :

$$F(v_{11}\xi' + v_{12}, v_{21}\xi' + v_{22}) = F(v_{11}\overline{\xi}' + v_{12}, v_{21}\overline{\xi}' + v_{22}) = 0,$$

ceci permet de conclure en choisissant bien les notations pour ξ et $\overline{\xi}$:

$$\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} (\xi') = \xi, \qquad \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} (\overline{\xi}') = \overline{\xi},$$

où cette fois la matrice T agit sur les algébriques ξ' et $\overline{\xi}'$:

$$\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} (\xi') = \frac{v_{11}\xi' + v_{12}}{v_{21}\xi' + v_{22}} = \xi, \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} (\overline{\xi}') = \frac{v_{11}\overline{\xi}' + v_{12}}{v_{21}\overline{\xi}' + v_{22}} = \overline{\xi}.$$

Par conjugaison, on a usuellement pour le stabilisateur de cette dernière action $\Sigma(\xi) = \Sigma(\overline{\xi})$, et il s'agit là d'un groupe lié à $\Sigma(F)$. Avec sa définition et (3.40),

la forme quadratique $F_\theta(x,y)$ possède un groupe de transformations de $GL(2,\mathbb{Z})$ privilégié, dont un générateur s'écrit :

$$g = \begin{bmatrix} K_1 & (\omega+1)K_1 - l \\ m & (\omega+1)m - K_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} M_{(S^*,\omega)} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{3.53}$$

En explicitant le calcul, on obtient :

$$F_\theta(K_1x + ((\omega+1)K_1 - l)y, mx + ((\omega+1)m - K_2)y) = -\varepsilon_S F_\theta(x,y). \tag{3.54}$$

En particulier, si $\varepsilon_S = 1$ la transformation g est dans $\Sigma(\theta_a(S))$ mais non dans $\Sigma(F_\theta)$. On peut écrire dans le cas général :

$$g = \begin{bmatrix} K_1 & -m\mathbf{A}_0\mathbf{A}_2 \\ m & K_1 + m\mathbf{A}_1 \end{bmatrix}, \qquad g(\theta_\omega(S)) = \theta_\omega(S), \qquad g(\overline{\theta_\omega(S)}) = \overline{\theta_\omega(S)}.$$

Si l'on a fait le choix $\mathbf{A}_2 = 1$ il en résulte :

$$\pi(K_1 - \theta_\omega(S)m) = g.$$

Le déterminant $-\varepsilon_S$ peut valoir -1 ou 1, raison pour laquelle on n'utilise pas a priori le mot de rotation pour désigner g. On dit plutôt que g est une **isométrie entière** de $GL(2,\mathbb{Z})$. Le qualificatif **hyperbolique** signifie que la valeur absolue de la trace est strictement supérieure à 2, ce qui est le cas le plus fréquent car :

$$tr(g) = (\omega+1)m + K_1 - K_2 = tr(M_{(S^*,\omega)}) \geq \omega.$$

Elle laisse une hyperbole invariante. Si le déterminant de g vaut -1, on dit aussi que l'on a affaire à une **isométrie hyperbolique non conforme** (retournant les angles). Si au contraire $\det(g) = -\varepsilon_S = 1$, on appelle g une **rotation hyperbolique (entière et conforme)**. g est dans $SL(2,\mathbb{Z})$, sous groupe du **groupe unimodulaire** $SL(2,\mathbb{R})$, et a une image $PSL(2,\mathbb{Z})$ dans le **groupe modulaire** $PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm\mathbf{1}_2\}$ (ses sous-groupes discrets sont les **groupes fuchsiens**). g est aussi une **transformation de Möbius** (matrice de g à coefficients complexe et de déterminant non nul). Ainsi (comparer à [13] (p. 33) :

Proposition 3.7. *Pour toute forme de Markoff on a :*

$$F_\theta(x,y) = F_\theta(-x,-y) = F_\theta(x + \mathbf{A}_1 y, -y), \tag{3.55}$$

$$F_\theta(\frac{l - (\omega+1)K_1}{m}y, x) = \frac{l - (\omega+1)K_1}{m} F_\theta(x,y). \tag{3.56}$$

La transformation $g \in GL(2,\mathbb{Z})$ donnée par l'expression (3.53) est une isométrie hyperbolique :

$$tr(g) \in \mathbb{R}, \qquad tr(g)^2 = ((\omega+1)m + K_1 - K_2)^2 = \Delta_\omega(S) - 4\varepsilon_S > 4,$$

une rotation hyperbolique si $\varepsilon_S = -1$, une isométrie non conforme sinon. Et :

$$(F_\theta \circ g)(x,y) = -\varepsilon_S F_\theta(x,y), \tag{3.57}$$

$$F_\theta(K_1, m) = F_\theta(K_2 - (\omega+1)m, m) = \varepsilon_1\varepsilon_2 = -\varepsilon_S. \tag{3.58}$$

• On donne un complément sur l'application de la **théorie de la réduction des formes quadratiques** à $F_\theta(x,y)$. La **forme réduite** définie par F_θ est donnée par les expressions ([40] p. 21) :

$$\begin{aligned} F_\theta(-x,y) &= x^2 - \left[\frac{(\omega+1)m - K_1 - K_2}{m}\right]xy + \left[\frac{l-(\omega+1)K_1}{m}\right]y^2 \\ &= (x - \xi_0 y)(x + \frac{1}{\eta_0}y) = x^2 + \beta_0^\theta xy + \gamma_0^\theta y^2 = f_0^\theta(x,y), \end{aligned}$$

où l'on note avec (3.39) :

$$0 < \theta_\omega(S) = [0, \underline{S^*, \omega}] = [0, S^*, \omega, S^*, \omega, ...] = \frac{1}{\eta_0} = [0, \alpha_{-1}, \alpha_{-2}, ..., \alpha_{-j}, ...] < 1,$$

$$-\overline{\theta_\omega(S)} = [\underline{\omega, S}] = [\omega, S, \omega, S, \omega, ...] = \xi_0 = [\alpha_0, \alpha_1, ..., \alpha_j, ...] > 1.$$

Et si l'on pose :

$$\theta^* = \theta_\omega(S^*) = -\omega - \overline{\theta_\omega(S)}, \tag{3.59}$$

$$M = \begin{bmatrix} 1 & \omega \\ 0 & -1 \end{bmatrix} \in GL(2,\mathbb{Z}), \qquad M^2 = \mathbf{1}_2.$$

on généralise la remarque qui a été faite ci dessus à partir de ([13] p. 33) au sujet des notations :

$$F_{\theta^*}(x,y) = (x+\omega y + \overline{\theta_\omega(S)y})(x+\omega y+\theta_\omega(S)y) = F_\theta(x+\omega y, -y) = (F_\theta \circ M)(x,y).$$

On dit que $\theta^* = \theta_\omega(S^*)$ est l'**algébrique de degré 2 dual** de $\theta = \theta_\omega(S)$, et que $F_{\theta^*}(x,y)$ est la **forme duale** de $F_\theta(x,y)$.

3.2.4. Des résultats de Cassels aux fractions continues

La comparaison du cas général que l'on vient de développer avec ce que présente [13] conduit à remplacer ω par 2, K_1 et K_2 par k, et ε_S par -1, et comme avant m par γ. La relation (3.58) n'est autre qu'une partie de son lemme 8 ([13] p. 33). L'expression (3.35) correspond à la première condition de (3.17) :

$$k^2 + 1 = l\gamma.$$

Elle conduit à associer au triplet ibérique (a, b, c) non singulier dont on est parti une réduite et une matrice qui s'écrivent :

$$M_S = \begin{bmatrix} \omega_0 & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} \omega_{2i} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \gamma & k \\ \gamma - k & k - l \end{bmatrix} = \begin{bmatrix} p_{2i} & p_{2i-1} \\ q_{2i} & q_{2i-1} \end{bmatrix},$$

$$[S] = [\omega_0, \omega_1, ..., \omega_{2i}] = \omega_0 + \cfrac{1}{\omega_1 + \cfrac{1}{... + \cfrac{1}{\omega_{2i}}}} = \frac{\gamma}{\gamma - k} = \frac{p_{2i}}{q_{2i}} \in \mathbb{Q}.$$

Pour la suite étendue à gauche construite avec S, on a :

$$M_{\lhd S} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \gamma & k \\ \gamma - k & k - l \end{bmatrix} = \begin{bmatrix} \gamma & k \\ k & l \end{bmatrix} = M^*_{\lhd S} = M_{(\lhd S)^*} = M_{S^* \rhd}.$$

La suite $(\lhd S)$ a donc la propriété d'être autoduale :

$$(\lhd S) = (\lhd S)^* = S^* \rhd .$$

On vient d'utiliser la première égalité de (3.17), on en déduit que :

$$(\lhd S) = (\lhd S)^* = S^* \rhd = (1, \omega_0 - 1, \omega_1, ..., \omega_{2i}).$$

$$M_{S^*} = \begin{bmatrix} \omega_{2i} & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} \omega_0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \gamma & \gamma - k \\ k & k - l \end{bmatrix}.$$

$$\theta_2(S) = [0, \underline{S^*, 2}], \qquad \overline{\theta_2(S)} = [-3, \lhd S, 2, \underline{S, 2}].$$

Avec β et k_1, respectivement α et k_2, on peut construire comme dans [40] deux suites X_1 et X_2. Elles ont également une propriété d'autodualité analogue, en effet la seconde et la troisième égalité de (3.17) permettent d'écrire :

$$(X_1 \rhd) = (X_1 \rhd)^* = (\omega_{1,0}, \omega_{1,1}, ..., \omega_{1,2i_1} - 1, 1),$$

$$(X_2\,\triangleright) = (X_2\,\triangleright)^* = (\omega_{2,0}, \omega_{2,1}, ..., \omega_{2,2i_2} - 1, 1),$$

$$M_{X_1} = \begin{bmatrix} \omega_{1,0} & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} \omega_{1,2i_1} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \beta & \beta - k_1 \\ k_1 & k_1 - l_1 \end{bmatrix},\ \varepsilon_1 = \det(M_{X_1}) = -1$$

$$M_{X_2} = \begin{bmatrix} \omega_{2,0} & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} \omega_{2,2i_2} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha & \alpha - k_2 \\ k_2 & k_2 - l_2 \end{bmatrix},\ \varepsilon_2 = \det(M_{X_2}) = -1.$$

$$M_{X_1\triangleright} = \begin{bmatrix} \beta & \beta - k_1 \\ k_1 & k_1 - l_1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \beta & k_1 \\ k_1 & l_1 \end{bmatrix},\ M_{X_2\triangleright} = \begin{bmatrix} \alpha & k_2 \\ k_2 & l_2 \end{bmatrix}.$$

On peut alors faire le lien avec le formalisme développé dans [40]. On a $k_{12} = k_1$ et $k_{21} = k_2$, ce qui correspond à la propriété d'autodualité des deux suites $X_1\,\triangleright$ et $X_2\,\triangleright$ que l'on vient de voir. Supposons alors que l'on ait :

$$M_2^{-1} M_{X_2}^{-1} M_{S^*\triangleright} = M_{X_1\triangleright},$$

soit :

$$\begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} l_2 - k_2 & (\alpha - k_2) \\ k_2 & -\alpha \end{bmatrix} \begin{bmatrix} \gamma & k \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} \gamma k_2 - k\alpha & kk_2 - l\alpha \\ 3k\alpha - kk_2 - 3\gamma k_2 + \gamma l_2 & 3l\alpha - 3kk_2 + kl_2 - lk_2 \end{bmatrix} = \begin{bmatrix} \beta & k_1 \\ k_1 & l_1 \end{bmatrix}.$$

On retrouve les quatre conditions équivalentes (3.18), (3.22), (3.23), (3.32) :

$$\beta = \gamma k_2 - k\alpha,$$

$$k_1 = kk_2 - l\alpha = 3k\alpha - kk_2 - 3\gamma k_2 + \gamma l_2,$$

$$l_1 = 3l\alpha - 3kk_2 + kl_2 - lk_2.$$

Comme on les a démontrées dans ce qui précède, on en déduit que l'on a avec les suites introduites la condition $S^* = (X_2, 2, X_1)$. Cette formule n'est pas celle de [40] (p. 13). En regroupant ce qui précède :

Proposition 3.8. *Pour tout triplet ibérique non singulier (a, b, c) on peut construire avec les propriétés (3.14) à (3.16) trois suites S, X_1 et X_2, ayant les propriétés d'autodualité suivantes :*

$$(\triangleleft S) = (\triangleleft S)^* = S^*\,\triangleright,$$

$$(X_1\,\triangleright) = (X_1\,\triangleright)^* = \triangleleft\, X_1^*, \qquad (X_2\,\triangleright) = (X_2\,\triangleright)^* = \triangleleft\, X_2^*.$$

Elles sont également liées par l'égalité de concaténation suivante :

$$(S^*) = (X_2, 2, X_1). \tag{3.60}$$

Remarquons que si l'on considère la suite transposée $S = (X_1^*, 2, X_2^*)$, on peut écrire :

$$M_S = \begin{bmatrix} \gamma & k \\ \gamma - k & k - l \end{bmatrix} = {}^t(M_{S^*}) = \left({}^t \begin{bmatrix} {}^t\gamma & {}^tk \\ {}^t\gamma - {}^tk & {}^tk - {}^tl \end{bmatrix} \right) = \begin{bmatrix} {}^t\gamma & {}^t\gamma - {}^tk \\ {}^tk & {}^tk - {}^tl \end{bmatrix}$$

$$ {}^t\gamma = \gamma, \qquad {}^tk = \gamma - k, \qquad {}^tl = \gamma - 2k + l, \tag{3.61}$$

On dit ainsi que la valeur duale de γ est ${}^t\gamma$, celle de k est ${}^tk = \gamma - k$, etc. Pour les traces, on note de même l'impact de la transposition sur les traces, en définissant par dualité :

$$({}^ta, {}^tb, {}^tc) = (b, a, c). \tag{3.62}$$

En fait cette notion de dualité est assez troublante du point de vue des notations, et il faut rester prudent en l'utilisant, c'est à dire revenir à sa signication en cas de doute. Elle dépend en effet du contexte.

3.3. Conséquences pour la conjecture et l'arbre ibérique

On a montré l'autodualité des suites $S^* \triangleright$, $X_1 \triangleright$, et $X_2 \triangleright$. L'égalité (3.60) recouvre d'autres décompositions plus fines de la suite $S^* \triangleright$. En fait les suites X_1 et X_2 ne sont pas indépendantes, et elles sont liées à des sommes de deux carrés.

3.3.1. Apparition des sommes de deux carrés

L'autodualité de $\triangleleft S$ est liée au résultat classique qui dit que si $k^2 + 1 = \gamma l$ et $0 < k < \gamma$ on peut écrire avec un développement en fraction continue autodual unique ([44] Satz 4 p. 33) :

$$\frac{\gamma}{k} = [\triangleleft S] = [1, \omega_0 - 1, \omega_1, ..., \omega_{2j}] = [\omega_{2j}, \omega_{2j-1}, ..., \omega_0 - 1, 1], \qquad (-1)^{2j+2} = 1.$$

On peut considérer la matrice de déterminant ± 1 (pas seulement 1 et donc pas nécessairement dans $SL(2, \mathbb{Z})$) formée avec les $j + 1$ premiers termes de ce développement :

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \omega_0 - 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \omega_1 & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} \omega_{j-1} & 1 \\ 1 & 0 \end{bmatrix}.$$

Par construction elle vérifie :

$$\frac{a_{11}}{a_{21}} = [1, \omega_0 - 1, \omega_1, ..., \omega_{j-1}],$$

$$M_{\lhd S} = A \times {}^tA = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{bmatrix} = \begin{bmatrix} \gamma & k \\ k & l \end{bmatrix}.$$

Evidemment la fraction continue de (γ/k) assure l'unicité de la matrice A. Ceci permet d'énoncer un résumé de ce que l'on vient de voir, mais qui vaut bien au delà de la théorie de Markoff, où k et γ sont des entiers positifs quelconques :

Proposition 3.9. *Pour toute solution en k de l'équation $k^2+1 \equiv 0 \pmod{\gamma}$ avec $0 < k < \gamma$ il existe une unique matrice $A \in \mathbf{M}_2(\mathbb{Z})$ à coefficients entiers positifs ou nuls et de déterminant ± 1 telle que :*

$$A \times {}^tA = \begin{bmatrix} \gamma & k \\ k & l \end{bmatrix}.$$

De plus on a alors une décomposition de γ en une somme de deux carrés premiers entre eux :

$$\gamma = a_{11}^2 + a_{12}^2.$$

La proposition que l'on vient d'énoncer est la partie c/ du lemme 4.2 de [47].

• Ce résultat détermine, γ et k étant fixés, une unique décomposition :

$$\gamma = a_{11}^2 + a_{12}^2,\ l = a_{21}^2 + a_{22}^2,\ k = (a_{11}a_{21} + a_{12}a_{22}),\ 1 = (a_{12}a_{21} - a_{11}a_{22})^2. \quad (3.63)$$

L'entier $2 = 1^2 + 1^2$ peut être un facteur de γ, mais pas 4, et tout facteur premier impair p de γ est lui-même une somme de deux carrés premiers entre eux ([20] Descent step p. 10), et est donc congru à 1 modulo 4 ([20] Theorem 1.2. p. 10). Inversement si $2^e \mid \gamma$ impose $e \leq 1$, et si tout facteur premier impair p de γ est congru à 1 modulo 4, tout p est une somme de deux carrés premiers entre eux ([48] p. 93), et ceci de façon unique au signe et à l'ordre près ([33] Corollary Theorem 7-5 p. 128). Le nombre γ se décompose en une somme de deux carrés $\gamma = a_{11}^2 + a_{12}^2$ par application répétée de la classique formule de Fibonacci :

$$(x'^2 + y'^2)(x^2 + y^2) = (x'x \pm y'y)^2 + (x'y \mp y'x)^2.$$

En fait on peut faire mieux en montrant que l'on peut ajouter la contrainte que a_{11} et a_{12} sont premiers entre eux. Pour le voir, il suffit de procéder comme suit.

$*$ On part de p premier impair tel que $p = x^2 + y^2$ avec x et y premiers entre eux, et donc aussi à p. Pour tout entier n, à partir de $p = (x + iy)(x - iy)$ élevé à la puissance n par la formule du binôme, on peut écrire :

$$\begin{aligned} p^n &= (x^n - \binom{n}{2}x^{n-2}y^2 + \binom{n}{4}x^{n-4}y^4 - ...)^2 + (\binom{n}{1}x^{n-1}y - \binom{n}{3}x^{n-3}y^3 + ...)^2 \\ &= A_n(x,y)^2 + B_n(x,y)^2. \end{aligned}$$

Par exemple pour $n = 2$:

$$p^2 = (x^2 - y^2)^2 + (2xy)^2, \qquad A_2(x,y) = x^2 - y^2, \qquad B_2(x,y) = 2xy.$$

On a $x^2 - y^2$ impair, et si d pgcd de $x^2 - y^2$ et $2xy$, alors d pgcd de $x^2 - y^2$ et xy. Si δ facteur premier de d, et si $\delta \mid x$, avec $\delta \mid x^2 - y^2$ il reste $\delta \mid y^2$ soit $\delta \mid y$, et puisque x et y premiers entre eux, $\delta = 1$, d'où une contradiction. Si $\delta \mid y$, on procède de même. La conclusion générale est que $x^2 - y^2$ et $2xy$ sont premiers entre eux. On suppose par récurrence que $A_n(x,y)$ et $B_n(x,y)$ sont premiers entre eux, ce qui est équivalent à dire que p ne divise ni $A_n(x,y)$ ni $B_n(x,y)$. On a :

$$(A_n(x,y)+iB_n(x,y))(x+iy) = (xA_n(x,y)-yB_n(x,y))+i(xB_n(x,y)+yA_n(x,y)),$$

$$A_{n+1}(x,y) = xA_n(x,y) - yB_n(x,y), \qquad B_{n+1}(x,y) = xB_n(x,y) + yA_n(x,y),$$
$$A_{n+1}(x,y)^2 + B_{n+1}(x,y)^2 = (x^2+y^2)(A_n(x,y)^2 + B_n(x,y)^2) = p^{n+1}.$$

Si δ facteur premier divise $A_{n+1}(x,y)$ et $B_{n+1}(x,y)$ on a :

$$\delta^2 \mid p^{n+1}, \qquad \delta = p.$$

Avec $p \mid \ A_{n+1}(u,v)$ on écrit :

$$p \mid (x^{n+1} - \binom{n+1}{2} x^{n-1}(p-x^2) + \binom{n+1}{4} x^{n-3}(p-x^2)^2 - ...),$$

$$p \mid (\binom{n+1}{0} + \binom{n+1}{2} + \binom{n+1}{4} + ...)x^{n+1},$$

soit puisque p est premier à u :

$$p \mid (\binom{n+1}{0} + \binom{n+1}{2} + \binom{n+1}{4} + ...).$$

Avec $p \mid \ B_{n+1}(x,y)$ on écrit :

$$p \mid \binom{n+1}{1} x^n y - \binom{n+1}{3} x^{n-2} y(p-x^2) + \binom{n+1}{5} x^{n-4} y(p-x^2)^2 + ...,$$

$$p \mid (\binom{n+1}{1} + \binom{n+1}{3} + \binom{n+1}{5} + ...)x^n y,$$

soit puisque p est premier à x et à y :

$$p \mid (\binom{n+1}{1} + \binom{n+1}{3} + \binom{n+1}{5} + ...).$$

En additionnant alors les deux conditions de divisibilité obtenues pour p :

$$p \mid \sum_{k=1,...,n+1} \binom{n+1}{k} = 2^{n+1}.$$

On tombe sur une contradiction avec le fait que p est impair, ce qui signife que l'on $A_{n+1}(x,y)$ et $B_{n+1}(x,y)$ premiers entre eux, et par récurrence que toute puissance p^n se représente pour tout $n \in \mathbb{N}^*$ comme somme de deux carrés premiers entre eux, et ceci de façon unique au signe et à l'ordre près ([33] Theorem 7-5 p. 128).

$*$ Supposons que deux sommes de carrés premiers entre eux $x'^2 + y'^2$ et $x^2 + y^2$, premières entre elles, soient alors multipliées sous la forme :

$$(x'^2 + y'^2)(x^2 + y^2) = (x'x + y'y)^2 + (x'y - y'x)^2.$$

Si δ facteur premier divise $(x'x + y'y)$ et $(x'y - y'x)$, on a :

$$\delta \mid x(x'x + y'y) + y(x'y - y'x) = x'(x^2 + y^2),$$

$$\delta \mid y(x'x + y'y) - x(x'y - y'x) = y'(x^2 + y^2),$$

d'où puisque x' et y' sont premiers entre eux :

$$\delta \mid (x^2 + y^2).$$

Mais on a aussi :

$$\delta \mid x'(x'x + y'y) - y'(x'y - y'x) = x(x'^2 + y'^2),$$

$$\delta \mid x'(x'x + y'y) + x'(x'y - y'x) = y(x'^2 + y'^2),$$

d'où puisque x et y sont premiers entre eux :

$$\delta \mid (x'^2 + y'^2).$$

On conclut en remarquant que par hypothèse $(x^2 + y^2)$ et $(x'^2 + y'^2)$ sont premiers entre eux. Ceci impose $\delta = 1$. On vient d'établir que le produit $(x'^2 + y'^2)(x^2 + y^2)$ se décompose alors comme somme de deux carrés premiers entre eux. Ce résultat

se généralise par récurrence à tout entier dont tout facteur premier est impair et congru à 1 modulo 4, qui se décompose donc comme somme de deux carrés premiers entre eux ([20] p. 10). Remarquons que l'on peut donner une autre décomposition en sommes de deux carrés premiers entre eux avec la formule :

$$(x'^2 + y'^2)(x^2 + y^2) = (x'x - y'y)^2 + (x'y + y'x)^2.$$

Par exemple, le nombre 65 est représentable par deux sommes de deux carrés premiers entre eux différentes avec :

$$65 = 5 \times 13 = (1^2 + 2^2)(3^2 + 2^2) = 7^2 + 4^2 = 8^2 + 1^2$$

$*$ On peut compléter ce qui précède en considérant $(x^2 + y^2)$ impair et somme de deux carrés premiers entre eux. Avec $2 = 1^2 + 1^2$ on a :

$$2(x^2 + y^2) = (x + y)^2 + (x - y)^2.$$

Si δ facteur premier de $(x + y)$ et $(x - y)$, alors $\delta \mid 2x$ et $\delta \mid 2y$, mais puisque x et y premiers entre eux, il reste $\delta \mid 2$. Mais si $\delta = 2$ il reste $4 \mid 2(x^2 + y^2)$ ce qui est contradictoire avec $(x^2 + y^2)$ impair. Donc en fait $\delta = 1$.

On dit qu'un nombre admet une **représentation propre** en une somme de deux carrés si ces carrés sont premiers entre eux. On vient d'établir en partie (plus précisément 3/⇒2/⇒1/⇒2/) :

Proposition 3.10. *Pour tout entier positif γ on a équivalence des propriétés :*

1/ Tout facteur premier p de γ vaut 2 et n'apparait dans γ qu'à la puissance 1, ou est impair et congru à 1 modulo 4.

2/ Le nombre γ admet au moins une représentation propre (en somme de deux carrés premiers entre eux) :

$$\gamma = a_{11}^2 + a_{12}^2.$$

3/ Le nombre -1 est un résidu quadratique modulo γ.

Partant de 2/ et décomposant en fraction continue le rationnel (a_{11}/a_{12}) on fabrique une matrice A qui montre que -1 est un résidu quadratique modulo γ. On a d'ailleurs deux fractions continues valant ce rationnel, celle que l'on vient de donner et celle qui correspond à :

$$A' = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{11} - a_{12} \\ a_{21} & a_{21} - a_{22} \end{bmatrix},$$

cependant la seconde fraction continue peut ne pas correspondre à γ mais au nombre :

$$a_{11}^2 + (a_{11} - a_{12})^2.$$

Si ce nombre valait γ on aurait $2a_{12} = a_{11}$ soit $a_{12} = 1$ et $a_{11} = 2$, ce qui donne toujours $\gamma = 5$, avec les deux possibilités $k = 3$ qui correspond à la suite $(\gamma/k) = [1, 1, 1, 1]$ ou $k = 2$ qui correspond à la suite $(\gamma/k) = [2, 2]$. Dans tous les cas la donnée de γ et k détermine de façon unique une matrice A et donc la suite S. Les nombres -1 et γ sont premiers entre eux, et la congruence $k^2 \equiv -1 \pmod{\gamma}$ a une solution en k. On obtient ainsi 3/, et ceci termine la démonstration de la proposition 3.10. On trouve aussi la partie a/ du lemme 4.2 de [47].

Le fait que 3/⇒1/ est aussi démontrable avec [32] (Theorem 88 p. 64) et [33] (Theorem 5-1 p. 63). On peut s'intéresser au nombre de telles solutions de la congruence $k^2 \equiv -1 \pmod{\gamma}$. On trouve avec [33] (Theorem 5-2 p. 65) le fait que pour γ non divisible par 4 cette congruence a exactement $2^{\boldsymbol{\omega}(\gamma)}$ classes modulo γ de solutions différentes en k, avec $\boldsymbol{\omega}(\gamma)$ nombre de diviseurs premiers impairs distincts de γ. Tous les facteurs premiers impairs de γ sont congrus à 1 modulo 4. On obtient aussi la partie b/ du lemme 4.2 de [47]

Avec les deux propositions 3.9 et 3.10 le lemme 4.2 de [47] est complètement démontré, et ceci répond à l'objectif que l'on s'était fixé au tout début du présent chapitre.

3.3.2. Une démonstration partielle de la conjecture

On voit avec ce que l'on vient de développer que la conjecture de Frobenius a à voir avec le fait que γ (ou $c = 3\gamma$) étant donné, on ne peut pas trouver trop de valeurs convenables k vérifiant la condition $k^2 + 1 = \gamma l$ avec $0 < k < \gamma$. Ayant trouvé une telle valeur k correspondant au triplet ibérique (a, b, c), on a d'abord une autre possibilité ${}^t k = \gamma - k$ pour assurer cette condition de divisibilité. Elle apparait de façon naturelle et correspond aux conditions (3.14) à (3.16) mises sous la forme :

$$ {}^t k = \gamma - k \equiv \frac{\beta}{\alpha} \equiv \frac{-\alpha}{\beta} \pmod{\gamma}, \qquad 0 < {}^t k < \gamma, \tag{3.64}$$

$$ {}^t k_1 = \alpha - k_2 \equiv \frac{\gamma}{\beta} \equiv \frac{-\beta}{\gamma} \pmod{\alpha}, \qquad 0 \leq {}^t k_1 < \alpha, \tag{3.65}$$

$$ {}^t k_2 = \beta - k_1 \equiv \frac{\alpha}{\gamma} \equiv \frac{-\gamma}{\alpha} \pmod{\beta}, \qquad 0 < {}^t k_2 \leq \beta. \tag{3.66}$$

Ces dernières correspondent au triplet ibérique $(b,a,c) = ({}^ta, {}^tb, {}^tc)$ **dual** du précédent (a,b,c), comme défini par (3.62). La question posée par la conjecture de Frobenius est de savoir si l'on peut trouver un troisième triplet correspondant à la même valeur c, et donc à la même valeur γ. Si tel est le cas, par la proposition 3.9 il en résulte une autre valeur de k associée à la même valeur γ, qui n'est ni k ni $\gamma - k$, d'où plusieurs décompositions de γ en somme de deux carrés premiers entre eux :

$*$ La valeur k issue de $(a,b,c) = (a_1,b_1,c)$ correspond à la décomposition :

$$\begin{aligned} \gamma &= a_{11}^2 + a_{12}^2,\ k = a_{11}a_{21} + a_{12}a_{22}, \\ k^2+1 &= (a_{11}a_{21} + a_{12}a_{22})^2 + 1 = \left(a_{11}^2 + a_{12}^2\right)\left(a_{21}^2 + a_{22}^2\right) = \gamma l, \end{aligned}$$

$$l = a_{21}^2 + a_{22}^2.$$

$*$ La valeur duale ${}^tk = \gamma - k$ associée à $(b,a,c) = (b_1,a_1,c)$ donne de même :

$$\gamma = a_{11}^2 + a_{12}^2,\ \gamma - k = (a_{11} - a_{21})a_{11} + (a_{12} - a_{22})a_{12},$$

$$\begin{aligned} ({}^tk)^2 + 1 &= (\gamma - k)^2 + 1 = \left(a_{11}^2 - a_{21}a_{11} + a_{12}^2 - a_{22}a_{12}\right)^2 + 1 \\ &= \left(a_{11}^2 + a_{12}^2\right)\left((a_{11} - a_{21})^2 + (a_{12} - a_{22})^2\right) \\ &= \gamma(l - 2k + \gamma) = ({}^t\gamma)({}^tl), \end{aligned}$$

$$l - 2k + \gamma = a_{21}^2 + a_{22}^2 - 2a_{11}a_{21} - 2a_{12}a_{22} + a_{11}^2 + a_{12}^2 = (a_{11} - a_{21})^2 + (a_{12} - a_{22})^2.$$

$*$ Toute valeur k' de k différente des deux précédentes, issue d'un autre triplet ibérique non singulier (a_2,b_2,c) qui n'est ni (a_1,b_1,c) ni (b_1,a_1,c) s'il existe, est aussi donnée par la construction précédente développée avec les conditions (3.14) à (3.16). La valeur k' obtenue est nouvelle sans quoi on identifierait à partir de la bonne condition $k^2 + 1 = \gamma l$ et avec la proposition 3.9 une des deux matrices A déjà rencontrées dans les deux cas précédents, donc aussi une valeur k déjà rencontrée. De plus si k' correspondait à la même décomposition de γ en somme de deux carrés premiers entre eux, on aurait avec des notations évidentes :

$$k = (a_{11}a_{21} + a_{12}a_{22}) \neq k' = (a_{11}b_{21} + a_{12}b_{22}),$$

$$\gamma = a_{11}^2 + a_{12}^2,$$
$$l = a_{21}^2 + a_{22}^2 \neq l' = b_{21}^2 + b_{22}^2,$$
$$1 = (a_{12}a_{21} - a_{11}a_{22})^2 = (a_{12}b_{21} - a_{11}b_{22})^2.$$

La dernière égalité imposerait avec $\varepsilon = \pm 1$:

$$a_{12}(a_{21} + \varepsilon b_{21}) = a_{11}(a_{22} + \varepsilon b_{22}),$$

et avec a_{12} et a_{11} premiers entre eux, l'existence de $t \in \mathbb{Z}$ tel que :

$$\varepsilon b_{21} = ta_{11} - a_{21}, \qquad \varepsilon b_{22} = ta_{12} - a_{22}.$$

D'où :

$$k' = (a_{11}b_{21} + a_{12}b_{22}) = -\varepsilon\left(-t\gamma + k\right).$$

Mais avec $0 < k < \gamma$ et $0 < k' < \gamma$ on ne trouverait que les possibilités $\varepsilon = -1$ et $t = 0$, ou $\varepsilon = 1$ et $t = 1$, c'est à dire l'un ou l'autre des cas suivants :

$$1/\ b_{21} = a_{21},\ b_{22} = a_{22}, \qquad 2/\ b_{21} = a_{11} - a_{21},\ b_{22} = a_{12} - a_{22}.$$

Le premier cas donnerait $l = l'$ et $k = k'$ donc une contradiction avec ce que l'on a supposé sur k'. Le second cas donnerait le cas dual $l' = l - 2k + \gamma$ et $k' = (a_{11}(a_{11} - a_{21}) + a_{12}(a_{12} - a_{22})) = \gamma - k$, donc aussi une contradiction. Il en résulte que dans la présente situation, on doit considérer pour le nombre γ une décomposition en somme de deux carrés qui n'est pas celle déjà rencontrée :

$$\gamma = b_{11}^2 + b_{12}^2 = a_{11}^2 + a_{12}^2,\ (b_{11}, b_{12}) \neq (a_{11}, a_{12}),$$

$$k = (a_{11}a_{21} + a_{12}a_{22}) \neq k' = (b_{11}b_{21} + b_{12}b_{22}),$$

$$l = a_{21}^2 + a_{22}^2 \neq l' = b_{21}^2 + b_{22}^2,$$

$$1 = (a_{12}a_{21} - a_{11}a_{22})^2 = (b_{12}b_{21} - b_{11}b_{22})^2.$$

$*$ La valeur duale de $\gamma - k'$ existe si k' existe et se traite de la même façon que le cas que l'on vient de voir, elles impose la même conclusion pour γ :

$$\gamma = b_{11}^2 + b_{12}^2,$$

$$\gamma - k' = (b_{11} - b_{21})b_{11} + (b_{12} - b_{22})b_{12}$$

$$(\gamma - k')^2 + 1 = \left(b_{11}^2 + b_{12}^2\right)\left((b_{11} - b_{21})^2 + (b_{12} - b_{22})^2\right) = \gamma(l - 2k + \gamma),$$

$$l' - 2k' + \gamma = (b_{11} - b_{21})^2 + (b_{12} - b_{22})^2.$$

• Le processus pourrait éventuellement se poursuivre en permettant de trouver k" différent des valeurs k; $\gamma - k$, k', $\gamma - k'$. Mais la conjecture de Frobenius dit qu'en fait on ne peut pas même trouver un autre triplet ibérique non singulier

(a_2, b_2, c) qui n'est ni (a_1, b_1, c) ni (b_1, a_1, c). Donc en réalité il semble qu'il n'y a pas de nouvelles valeurs convenables k', $\gamma - k'$, et notre problème est de comprendre pourquoi. Le groupement par paire duale $(\gamma, k), (\gamma, \gamma - k)$ des exemples précédents permet de confirmer que dans l'étude de la conjecture on peut se limiter à supposer (a_1, b_1, c) et (a_2, b_2, c) triplets de Zhang distincts, et donc à faire l'hypothèse Z, avec $\gamma = a_{11}^2 + a_{12}^2 = b_{11}^2 + b_{12}^2$ les deux décompositions différentes associées, et avec (3.17) :

$$\gamma = a_{11}^2 + a_{12}^2 \mid k^2 + 1 = (a_{11}a_{21} + a_{12}a_{22})^2 + 1,\ 0 < k < \gamma,$$

$$\gamma = b_{11}^2 + b_{12}^2 \mid k'^2 + 1 = (b_{11}b_{21} + b_{12}b_{22})^2 + 1,\ 0 < k' < \gamma.$$

Leur connaissance ne suffit pas à décrire la structuration interne des suites S associées (cf. la proposition 3.8).

• Notons cependant que l'on évoqué précédemment un théorème ([33] Theorem 5-2 p. 65) qui implique ici, puisque γ non divisible par 4 d'après (3.4), le fait que la congruence $x^2 \equiv -1 \pmod{\gamma}$ a exactement $2^{\boldsymbol{\omega}(\gamma)}$ classes modulo γ de solutions différentes en x, avec $\boldsymbol{\omega}(\gamma)$ nombre de diviseurs premiers impairs distincts de γ (ces diviseurs premiers sont congrus à 1 modulo 4 par notre proposition 3.10). Il en résulte, si $\gamma = 2^{e_c}p^e$ est un nombre primaire ou un double de primaire, que $\boldsymbol{\omega}(\gamma) = 1$, et qu'il y a exactement $2^{\boldsymbol{\omega}(\gamma)} = 2$ possibilités pour k sachant que $0 < k < \gamma$. On ne trouve alors que les deux possibilités duales (a_1, b_1, c) et (b_1, a_1, c) pour tout triplet ibérique non singulier, avec ici $c = 2^{e_c}3p^e$. Dans ce cas particulier on vient de démontrer la conjecture de Frobenius. On obtient un résultat qui a déjà été établi de plusieurs façons différentes de la présente (pour un nombre γ primaire : [11], [52], [34], [54], pour un nombre γ primaire ou double de primaire : [63], [7] (Corollary B2 p. 211), [53] (p. 26), ce dernier cite [4] qui donne des conditions plus originales γ, $3\gamma - 2$ ou $3\gamma + 2$ premier, double ou quadruple d'un nombre premier). On a donc établi avec une méthode assez simple :

Proposition 3.11. *Si γ est puissance d'un nombre premier ou double d'une puissance d'un nombre premier, il n'existe avec $c = 3\gamma$ qu'au plus deux triplets ibériques dont c soit la valeur dominante, ils sont duaux : (a, b, c) et (b, a, c).*

La conjecture de Frobenius est donc établie dans le cas très particulier où $c = 2^{e_c}3p^e$ où $e_c \in \{0, 1\}$, p premier et $e \in \mathbb{N}^*$. Dans des cas plus généraux, γ peut possèder d'autres décompositions en une somme de deux carrés premiers entre eux permettant d'identifier plus de solutions pour la congruence $x^2 \equiv -1 \pmod{\gamma}$.

Ces cas se présentent, comme le montrent par exemple les triplets $(\alpha, \beta, \gamma) = (2, 169, 985)$ et $(\alpha, \beta, \gamma) = (13, 34, 1325)$:

$$985 = 5 \times 197 = (2^2 + 1^2)(14^2 + 1^2), \qquad 1325 = 5^2 \times 53 = (2^2 + 1^2)^2(7^2 + 2^2).$$

Pour le seul premier cas, on a $\boldsymbol{\omega}(985) = 2$, et $985 = 29^2 + 12^2 = 27^2 + 16^2$. La proposition 3.10 donne les conditions :

$$985 \mid 577^2 + 1,\ 985 \mid 408^2 + 1, \qquad 985 \mid 183^2 + 1,\ 985 \mid 802^2 + 1.$$

La dernière condition de divisibilité s'accorde mal avec la théorie de Markoff ou les fractions continues qui apparaissent ne contiennent que des valeurs 1 et 2 :

$$\begin{aligned} \frac{27}{16} &= [1, 1, 2, 4, 1], \\ [\lhd S] &= [1, \omega_0 - 1, \omega_1, ..., \omega_{2i}] = [1, 4, 2, 1, 1, 1, 1, 2, 4, 1] = \frac{985}{802}. \end{aligned}$$

Par contre, la condition $985 \mid 577^2 + 1$ s'y intègre bien avec :

$$\begin{aligned} \frac{29}{12} &= [2, 2, 2, 1, 1], \\ [\lhd S] &= [1, \omega_0 - 1, \omega_1, ..., \omega_{2i}] = [1, 1, 2, 2, 2, 2, 2, 2, 1, 1] = \frac{985}{577} = \frac{\gamma}{k}. \end{aligned}$$

Elle donne le triplet ibérique $(a, b, c) = (6, 507, 2955)$ avec dans ce cas $k_2 = 99$ et $k_1 = 1$:

$$\gamma k_2 - \alpha k = \beta = (985 \times k_2) - (169 \times 577) = 2,$$
$$\beta k - \gamma k_1 = \alpha = (2 \times 577) - (985 \times k_1) = 169.$$

On voit sur cet exemple la limite de l'argument que l'on a utilisé pour démontrer notre proposition 3.11. Pour trouver une démonstration plus générale de la conjecture de Frobenius, il semble indispensable de faire intervenir des contraintes pesant sur la suite S, par exemple le fait que des coefficients ω_j soient plus grands que 2, ou sur les paramètres qui comme α, k_2, β, k_1 sont liés à la structure interne de cette suite. On va donc chercher à en savoir plus sur les suites liées à l'arbre ibérique.

3.3.3. L'arbre ibérique en matrices 2×2

On va maintenant voir que l'on dispose d'un procédé de construction de l'arbre ibérique avec des matrices 2×2. Pour le triplet $(a, b, c) = (3, 3, 3)$ correspondant à $(\alpha, \beta, \gamma) = (1, 1, 1)$ on calcule S, X_1 et X_2, avec (3.14) à (3.20). Les inégalités imposées par Cassels donnent :

$$(k, k_1, k_2) = (0, 0, 1),\ (l, l_1, l_2) = (1, 1, 2),$$

$$M_{X_1} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = M_{(\triangleright)},\ M_{X_2} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = M_{(\triangleleft)}.$$

Mais ceci pose problème car toutes les conditions (3.18) à (3.20) ne sont pas assurées, de plus :

$$\begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = M_{S^*}.$$

On a ici un phénomène de dégénérescence propre au sommet de l'arbre. Ce triplet singulier doit être laissé de côté pour décrire la construction de l'arbre, sachant que les matrices M_{X_1} et M_{X_2} mises en évidence réapparaissent avec le cas suivant.

• Pour le triplet $(a, b, c) = (3, 3, 6)$ correspondant à $(\alpha, \beta, \gamma) = (1, 1, 2)$ on calcule S, X_1 et X_2, avec (3.14) à (3.20). Tout se passe bien avec ce triplet :

$$k \equiv 1 \equiv -1 \pmod 2, \qquad 0 \leq k < 2, k = 2k_2 - 1 = 2k_1 + 1 = 1,$$

$$k_1 \equiv 2 \equiv \frac{-1}{2} \pmod 1, \qquad 0 \leq k_1 < 1, \qquad k_1 = 0,$$

$$k_2 \equiv \frac{1}{2} \equiv -2 \pmod 1, \qquad 0 < k_2 \leq 1, \qquad k_2 = 1,$$

$$\frac{\gamma}{k} = [1, \omega_0 - 1, \omega_1, ..., \omega_{2i}] = \frac{2}{1} = [1, 1],$$

$$(l, l_1, l_2) = (1, 1, 2),$$

$$M_{X_1} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = M_{(\triangleright)},\ \varepsilon_1 = \det(M_{X_1}) = -1,$$

$$M_{X_2} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = M_{(\triangleleft)},\ \varepsilon_2 = \det(M_{X_2}) = -1,$$

$$S^* = (\omega_0) = (2) = (X_2, 2, X_1),$$

$$X_2 = (\lhd),\ X_1 = (\rhd).$$

• Pour le triplet $(a, b, c) = (3, 6, 15)$ correspondant à $(\alpha, \beta, \gamma) = (1, 2, 5)$:

$$k \equiv \frac{1}{2} \equiv \frac{-2}{1} \pmod 5, \qquad 0 \leq k = 3 < 5,$$

$$k_1 \equiv \frac{5}{1} \equiv \frac{-1}{5} \pmod 2, \qquad 0 \leq k_1 = 1 < 2,$$

$$k_2 \equiv \frac{2}{5} \equiv \frac{-5}{2} \pmod 1, \qquad 0 < k_2 = 1 \leq 1,$$

$$\frac{\gamma}{k} = [1, \omega_0 - 1, \omega_1, ..., \omega_{2i}] = \frac{5}{3} = [1, 1, 1, 1],$$

$$(l, l_1, l_2) = (2, 1, 2),$$

$$M_{X_1} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = M_{(2)},\ \varepsilon_1 = \det(M_{X_1}) = -1, \tag{3.67}$$

$$M_{X_2} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = M_{(\lhd)},\ \varepsilon_2 = \det(M_{X_2}) = -1, \tag{3.68}$$

$$S^* = (\omega_2, \omega_1, \omega_0) = (1, 1, 2) = (X_2, 2, X_1),$$

$$X_2 = (\lhd),\ X_1 = (2).$$

• Pour le triplet $(a^*, b^*, c^*) = (6, 3, 15)$ associé à $(\alpha^*, \beta^*, \gamma^*) = (2, 1, 5)$:

$$k^* \equiv \frac{2}{1} \equiv \frac{-1}{2} \pmod 5, \qquad 0 \leq k^* = 2 < 5,$$

$$k_1^* \equiv \frac{5}{2} \equiv \frac{-2}{5} \pmod 1, \qquad 0 \leq k_1^* = 0 < 1,$$

$$k_2^* \equiv \frac{1}{5} \equiv \frac{-5}{1} \pmod 2, \qquad 0 < k_2^* = 1 \leq 2,$$

$$\frac{\gamma^*}{k^*} = [1, \omega_{2j} - 1, \omega_{2j-1}, ..., \omega_0] = \frac{5}{2} = [1, 0, 1, 2],$$

$$(l^*, l_1^*, l_2^*) = (1, 1, 1),$$

$$M_{X_2^*} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = M_{(\rhd)},\ \varepsilon_2^* = \det(M_{X_2^*}) = -1,$$

$$M_{X_1^*} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = M_{(2)},\ \varepsilon_1^* = \det(M_{X_2}) = -1,$$

$$S = (\omega_0, \omega_1, \omega_2) = (2, 1, 1) = (X_1^*, 2, X_2^*),$$
$$X_1^* = (2),\ X_2^* = (\triangleright).$$

• Pour les triplets suivants, ces calculs donnent les suites S^*, X_1 et X_2 :

(α, β, γ)	(k, k_1, k_2)	(l, l_1, l_2)	X_2	X_1	$S^* = (\overrightarrow{X_2}, 2, \overleftarrow{X_1})$
$(1, 5, 13)$	$(8, 3, 1)$	$(5, 2, 2)$	$(\triangleleft)$	$(1, 1, 2)$	$(1, 1, \overleftarrow{1, 1, 2})$
$(5, 2, 29)$	$(17, 1, 3)$	$(10, 1, 2)$	$(1, 1, 2)$	(2)	$(\overrightarrow{1, 1, 2}, 2, \overleftarrow{2})$
$(2, 5, 29)$	$(12, 2, 1)$	$(5, 1, 1)$	(2)	$(2, 1, 1)$	$(\overrightarrow{2}, 2, \overleftarrow{2, 1, 1})$
$(5, 1, 13)$	$(5, 0, 2)$	$(2, 1, 1)$	$(2, 1, 1)$	$(\triangleright)$	$(\overrightarrow{2, 1, 1}, 1, 1)$

Tableau n°3.

D'où le début de l'arbre des suites $S^* = (X_2, 2, X_1)$, où $(\triangleleft, 2) = (1, 1) = (2, \triangleright)$:

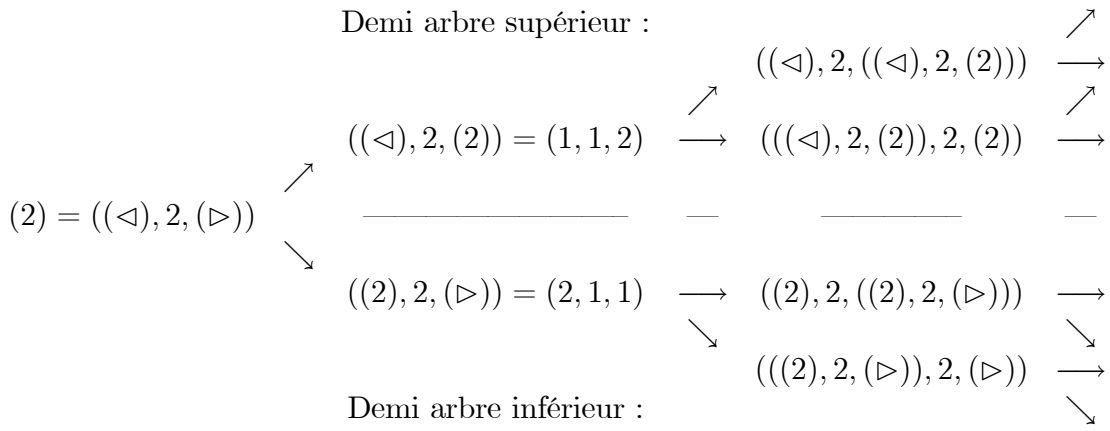


fig. 9 : L'arbre ibérique des suites S^*.

On peut définir pour l'arbre ibérique une notion de **hauteur**. La suite (2) correspond à la hauteur $h = 1$ et au triplet $(3, 3, 6)$. Les suites $(1, 1, 2)$ et $(2, 1, 1)$ correspondent à la hauteur $h = 2$ et respectivement aux triplets $(3, 6, 15)$ et $(6, 3, 15)$, etc.

• Pour aller plus loin, il faut décrire le procédé de construction des suites correspondant aux figures 4 et 5. Commençons par l'équation (2.2) qui transforme les triplets comme suit :

$$(\alpha, \beta, \gamma) \longrightarrow (\alpha, \gamma, 3\alpha\gamma - \beta).$$

Elle est issue de la suite $(S^*) = (X_2, 2, X_1)$ telle que :

$$M_{S^*} = \begin{bmatrix} \omega_{2i} & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} \omega_0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \gamma & \gamma - k \\ k & k - l \end{bmatrix},$$

$$M_{X_2} = \begin{bmatrix} \alpha & \alpha - k_2 \\ k_2 & k_2 - l_2 \end{bmatrix}, \qquad M_{X_1} = \begin{bmatrix} \beta & \beta - k_1 \\ k_1 & k_1 - l_1 \end{bmatrix}, \tag{3.69}$$

On a par construction :

$$tr(M_{(X_2,2)}) = 3\alpha = a,\ tr(M_{(X_1,2)}) = 3\beta = b,\ tr(M_{(S^*,2)}) = 3\gamma = c.$$

Si l'on pose alors :

$$A = M_{(X_2,2)} = \begin{bmatrix} \alpha & \alpha - k_2 \\ k_2 & k_2 - l_2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \in SL(2,\mathbb{Z}),\ tr(A) = a,$$

$$B = M_{(X_1,2)} = \begin{bmatrix} \beta & \beta - k_1 \\ k_1 & k_1 - l_1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \in SL(2,\mathbb{Z}),\ tr(B) = b,$$

$$AB = M_{(S^*,2)} = \begin{bmatrix} \gamma & \gamma - k \\ k & k - l \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \in SL(2,\mathbb{Z}),\ tr(AB) = c,$$

on a par hypothèse sur a, b, c, la relation de Markoff (2.1). Ceci a pour conséquence que la relation de Fricke ([16] ou (2.10)) donne la condition :

$$tr(ABA^{-1}B^{-1}) = tr([A,B]) = -2.$$

A l'arrivée, si on considère la suite :

$$(X_2, 2, S^*) = (X_2, 2, X_2, 2, X_1).$$

Elle correspond au triplet de matrices (A, AB, A^2B) qui vérifie avec (2.22) :

$$(tr(A), tr(AB), tr(A^2B)) = (a, c, ac - b) = (3\alpha, 3\gamma, 3(3\alpha\gamma - \beta)),$$

et donne :

$$a^2 + c^2 + (ac - b)^2 = ac(ac - b),$$

En particulier, il en résulte :

$$tr(A(AB)A^{-1}(AB)^{-1}) = tr(ABA^{-1}B^{-1}) = -2.$$

On a ainsi trouvé sur les suites une construction correspondant à la transformation (2.2). On peut généraliser le raisonnement et résumer la situation globale qui en résulte dans les figures qui suivent pour les périodes $(S^*, 2)$. Mais il faut faire attention pour la figure 11 qui s'obtient de la figure 10 par dualité, comme vu sur le triplet $(6, 3, 15)$. En fait, sachant que l'on travaille sur des triplets de traces, on peut raisonner à un automorphisme intérieur près, et le plus simple est d'appliquer pour ce qui concerne le demi-arbre inférieur l'automorphisme intérieur :

$$A \longrightarrow \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} A \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^{-1}.$$

Ceci donne les figures suivantes pour les suites associées aux matrices A et B :

$fig.\ 10$:

$$Zh : ((X_2, 2), (X_1, 2)) \quad \nearrow \quad Zh : ((X_2, 2), (X_2, 2, X_1, 2)) \quad (2.2)$$

$$\searrow \quad ((X_2, 2, X_1, 2), (X_1, 2)) \quad (2.3)$$

$fig.\ 11$:

$$((2, X_1^*), (2, X_2^*)) \quad \nearrow \quad Zh : ((2, X_1^*), (2, X_1^*, 2, X_2^*)) \quad (2.4)$$

$$\searrow \quad ((2, X_1^*, 2, X_2^*), (2, X_2^*)) \quad (2.5)$$

Comme dans les figures 4 et 5, la mention Zh indique comment combiner les figures 10 et 11 pour passer par récurrence des suites de hauteur $h + 1$ aux suites de hauteur $h + 2$, etc. En particulier on établit avec le tableau n°3 :

Proposition 3.12. *1/ Les périodes des développements en fraction continue des nombres $\theta_2(S)$ de la théorie de Markoff classique ne contiennent que des* 1 *et des* 2.

2/ Pour toute hauteur $h \geq 2$, l'arbre ibérique comprend autant de triplets de Zhang que de triplets qui ne sont pas de Zhang, c'est à dire 2^{h-2} triplets de Zhang de hauteur h. Il suffit de permuter les suites X_1 et X_2 pour passer des triplets de Zhang aux autres.

Les figures 10 et 11 qui donnent les transformations à considérer peuvent être présentées autrement. Il est en effet assez facile d'identifier des expressions matricielles qui conviennent. Le plus simple est de poser $A = M_{(X_2,2)}$ et $B = M_{(X_1,2)}$.

On traduit ainsi les figures 10 et 11, en traduisant la dualité sur les suites par la transposition des matrices :

$$\begin{array}{rll}
(2.2) : Zh : (A, B, AB) \longrightarrow Zh : (A, AB, A^2B) & (a, b, c) \longrightarrow (a, c, ac - b) \\
(2.3) : Zh : \ (A, B, AB) \longrightarrow (AB, B, AB^2) & (a, b, c) \longrightarrow (c, b, bc - a) \\
(2.4) : \ ({}^tB, {}^tA, {}^tB\,{}^tA) \longrightarrow Zh : ({}^tB, B^tA, ({}^tB)^2({}^tA)) & (b, a, c) \longrightarrow (b, c, bc - a) \\
(2.5) : \ ({}^tB, {}^tA, {}^tB\,{}^tA) \longrightarrow ({}^tB\,{}^tA, {}^tA, ({}^tB)({}^tA)^2) & (b, a, c) \longrightarrow (c, a, ac - b)
\end{array}$$

On a facilement pour les traces :

$$tr({}^tB\,{}^tA({}^tB^{-1})({}^tA^{-1})) = tr((A^{-1}B^{-1})(AB)) = tr((AB)(A^{-1}B^{-1})),$$

et sachant que l'on part pour chacune de ces transformations d'un triplet de Markoff :

$$tr(ABA^{-1}B^{-1}) = tr({}^tB\,{}^tA({}^tB^{-1})({}^tA^{-1})) = -2.$$

On en déduit aisément :

$$tr(A(AB)(A^{-1})(AB)^{-1}) = tr((AB)(B)(AB)^{-1}(B)^{-1}) = -2,$$

$$tr({}^tB({}^tB\,{}^tA)({}^tB^{-1})({}^tB\,{}^tA)^{-1}) = tr(({}^tB\,{}^tA)({}^tA)({}^tB\,{}^tA)^{-1}({}^tA)^{-1}) = -2.$$

Ces égalités garantissent par la formule de Fricke (2.10) et l'égalité (2.22) qu'on passe avec nos transformations d'un triplet ibérique à un triplet ibérique. Les expressions (2.4) et (2.5) ne concernent plus les bases du $\mathbb{Z}$-module $\mathbf{H}$ de rang 3 que l'on a introduites avant. On peut remarquer aussi que l'expression (2.3) ne donne pas non plus un triplet admissible tel qu'on l'a défini précédemment, car y apparait le triplet (AB, B, AB^2) au lieu de (B, AB, AB^2). Remarquons que la question des notations est très délicate. Si l'on note le triplet de matrices considérées (A, B, AB) on a tendance à écrire le triplet de traces associé (a, b, c). Mais si l'on veut appliquer (2.4) ou (2.5) il faut considérer avec les notations adoptées $(b, a, c) = ({}^ta, {}^tb, {}^tc)$ comme triplet de départ. D'où l'idée de faire jouer un rôle à la dualité. Egalement, en regardant bien les calculs faits ci-dessus, on voit qu'il peut y avoir aussi équivoque sur les suites que l'on désigne par X_1 et X_2. Il faut être très précis pour décrire de façon fiable la situation.

3.3.4. Des précisions pour la racine de l'arbre ibérique

Le triplet de hauteur $h = 1$: Il n'y a à cette hauteur qu'un triplet ibérique $(3, 3, 6)$, pour lequel on a calculé ci-dessus $X_1 = (\triangleright)$ et $X_2 = (\triangleleft)$ avec (3.14) à

(3.20). Ceci donne le triplet (A_1, B_1, A_1B_1) où :

$$A_1 = M_{(\lhd,2)} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = B_0^{-1},$$

$$B_1 = M_{(\rhd,2)} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = A_0^{-1}{B_0}^{-1},$$

$$A_1B_1 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = {B_0}^{-1}A_0^{-1}{B_0}^{-1},$$

Les deux triplets de hauteur $h = 2$: On examine les expressions obtenues avec la figure 10, à partir de $(a_1, b_1, c_1) = (3, 3, 6)$.

1/ Avec (2.2), $(A_1, B_1, A_1B_1) \longrightarrow (A_1, A_1B_1, A_1^2B_1) = (A_2, B_2, A_2B_2)$ donne :

$$A_2 = A_1 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix},\ B_2 = A_1B_1 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix},\ A_2B_2 = A_1^2B_1 = \begin{bmatrix} 12 & 5 \\ 7 & 3 \end{bmatrix},$$

$$(a_2, b_2, c_2) = (tr(A_2),\ tr(B_2),\ tr(A_2B_2)) = (3, 6, 15).$$

Pour ce triplet, on a obtenu ci-dessus en (3.67) et (3.68) :

$$M_{X_2} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} = M_{(\lhd)}, \qquad M_{X_1} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = M_{(2)}.$$

Ceci redonne les expressions que l'on vient d'exhiber :

$$A_2 = M_{(\lhd,2)} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \qquad B_2 = M_{(2,2)} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}.$$

2/ Avec (2.3), et $(A_1, B_1, A_1B_1) \longrightarrow (A_1B_1, B_1, A_1B_1^2) = (A_{2'}, B_{2'}, A_{2'}B_{2'})$:

$$A_{2'} = A_1B_1 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix},\ B_{2'} = B_1 = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix},\ A_{2'}B_{2'} = A_1B_1^2 = \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix},$$

$$(a_{2'}, b_{2'}, c_{2'}) = (tr(A_{2'}),\ tr(B_{2'}),\ tr(A_{2'}B_{2'})) = (6, 3, 15).$$

Pour ce dernier triplet on a obtenu ci-dessus des expressions pour les deux suites apparaissant dans S^*, on les désigne ici avec des notations que l'on choisit pour relier les suites du présent cas à celles du cas précédent :

$$M_{X_2'} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = M_{(2)} = M_{X_1}, \qquad M_{X_1'} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = M_{(\rhd)} = M_{X_2^*},$$

$$X'_1 = (\triangleright) = X^*_2, \qquad X'_2 = (2) = X_1 = X^*_1. \tag{3.70}$$

On trouve ainsi pour les expressions que l'on vient d'exhiber :

$$\begin{aligned} A_{2'} &= M_2^{-1}\,{}^tB_2M_2 = M_{(2,2)} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = B_2, \\ B_{2'} &= M_2^{-1}\,{}^tA_2M_2 = M_{(\triangleright,2)} = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = A_2^{-1}B_2. \end{aligned}$$

Et ceci est parfaitement cohérent avec notre figure 9. On peut pour la suite associer au triplet $(6,3,15)$ qui n'est pas de Zhang le triplet de matrices $({}^tB_2, {}^tA_2, {}^tB_2\,{}^tA_2)$, et noter alors en cohérence avec le cas précédent :

$$(6,3,15) = ({}^tb_2, {}^ta_2, {}^tc_2) = (b_2, a_2, c_2) = (a_{2'}, b_{2'}, c_{2'}).$$

Le calcul avec les automorphismes intérieurs donne :

$${}^tB_2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = B_2 = M_{(2,2)},\ {}^tA_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = A_2 = M_{(2,\triangleright)} = M_{(\triangleleft,2)}.$$

3/ Les relations (2.4) et (2.5) ne semblent rien devoir apporter de plus car elles se réduisent aux précédentes en permutant A et B. Toutefois, si l'on applique (2.4) à (B_1, A_1, B_1A_1), on obtient :

$$(\begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -2 & -1 \end{bmatrix}, \begin{bmatrix} 19 & 11 \\ -7 & -4 \end{bmatrix}).$$

Le triplet de traces associé est $(3,6,15)$ comme avec (A_2, B_2, A_2B_2). On comprend facilement comment ceci est possible, en écrivant :

$$\begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^{-1},$$

$$\begin{bmatrix} 7 & 4 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^{-1}.$$

Si l'on applique (2.5) à (B_1, A_1, B_1A_1), on obtient :

$$(\begin{bmatrix} 7 & 4 \\ -2 & -1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 18 & 11 \\ -5 & -3 \end{bmatrix}).$$

Le triplet de traces associé est ici $(6,3,15)$ comme avec $(A_{2'}, B_{2'}, A_{2'}B_{2'})$. On comprend aussi facilement comment ceci est possible, en écrivant :

$$\begin{bmatrix} 7 & 4 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^{-1},$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^{-1}.$$

Et le lien entre les deux derniers automorphismes intérieurs mis en évidence est étroit parce que :

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^2 = M_{(\triangleright)} = \mathbf{1}_2.$$

Le même genre de raisonnement peut être fait en comparant (A_2, B_2, A_2B_2) et $(A_{2'}, B_{2'}, A_{2'}B_{2'})$. En fait avec les traces on est conduit à supposer qu'il existe U vérifant $U^{-1}B_{2'}U = A_2$ et $U^{-1}A_{2'}U = B_2$, soit aussi $A_2B_2 = U^{-1}B_{2'}A_{2'}U$. La recherche de U est facile et l'on obtient :

$$A_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = U^{-1}B_{2'}U,$$

$$B_2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = U^{-1}A_{2'}U.$$

Par contre on n'a aucun automorphisme intérieur entre les deux couples (A_2, B_2) et $(A_{2'}, B_{2'}) = (B_2, A_2^{-1}B_2)$. Ceci confirme, si besoin était encore après ([39]), qu'on doit raisonner sur les systèmes de générateurs de $\mathbf{F}_2$ à l'action près des automorphismes intérieurs. Pour cette même raison, on a établit que du point de vue des triplets ibériques on n'a pas besoin à la hauteur $h = 1$ d'appliquer les expressions (2.4) ni (2.5). A cette hauteur on n'a à considérer qu'un triplet de matrices $(A_1, B_1, A_1B_1) = (A_2, A_2^{-1}B_2, B_2)$. On a aussi vu qu'en appliquant (2.2) on fabrique à la hauteur $h = 2$ le triplet de matrices (A_2, B_2, A_2B_2), correspondant au triplet de Zhang $(a_2, b_2, c_2) = (3, 6, 15)$ et à $((\triangleleft), 2, (2), 2)$, et que par (2.3) combiné avec un automorphisme intérieur on obtient le triplet de matrices $({}^tB_2, {}^tA_2, {}^tB_2\,{}^tA_2) = (B_2, A_2, B_2A_2)$, associé au triplet qui n'est pas de Zhang $(b_2, a_2, c_2) = (3, 6, 15)$ et à $(2, (2), 2, (\triangleright))$. Il y a cohérence avec la figure 9 à un automorphisme intérieur près. Il y a aussi cohérence avec les premières colonnes des figures 10 et 11 puisqu'on trouve (A_2, B_2) à la racine de la première, soit $((X_2, 2), (X_1, 2)) = ((\triangleleft, 2), (2_1, 2))$, et (B_2, A_2) à la racine de la seconde, soit

$((2,X_1^*),(2,X_2^*)) = ((2,2),(2,\triangleright))$. Notons que $(\triangleleft,2)$ et $(2,\triangleright)$ s'identifient à $(1,1)$ et correspondent au facteur $A_2 = M_{(1,1)}$, alors que $(2,2)$ correspond au facteur $B_2 = M_{(2,2)}$.

Les quatre triplets de hauteur $h = 3$: On change ici de méthode. Les triplets sont donnés par le tableau n°3 après calcul avec (3.14) à (3.20), on montre que tout ce qui les concerne peut être obtenu en suivant les flêches des figures 10 et 11. Et surtout on regarde de façon précise la question des notations à utiliser.

1/Le passage de $(a_2,b_2,c_2) = (3,6,15)$ à $(a_3,b_3,c_3) = (3,15,39)$ est fait par l'égalité traduisant la relation (2.2) :

$$\begin{bmatrix} 3 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 & 15 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 39 \\ 0 & 1 & 15 \\ 0 & 0 & 1 \end{bmatrix},$$

où l'on a par la matrice donnée par la proposition 2.1 :

$$N_{(2,3)} = \begin{bmatrix} 3 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = P^{-1}(3).$$

On part des matrices :

$$A_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = M_{(\triangleleft,2)},\ B_2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = M_{(2,2)},\ A_2B_2 = \begin{bmatrix} 12 & 5 \\ 7 & 3 \end{bmatrix}, \quad (3.71)$$

et avec l'extrait du tableau n°3 :

(α,β,γ)	(k,k_1,k_2)	(l,l_1,l_2)	X_2	X_1	$S^* = (X_2,2,X_1)$
$(1,5,13)$	$(8,3,1)$	$(5,2,2)$	$(\triangleleft)$	$(1,1,2)$	$(1,1,\overleftarrow{1,1,2})$

on obtient :

$$A_3 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = M_{(1,1)},\ B_3 = \begin{bmatrix} 12 & 5 \\ 7 & 3 \end{bmatrix} = M_{(1,1,2,2)},\ A_3B_3 = \begin{bmatrix} 31 & 13 \\ 19 & 8 \end{bmatrix},$$

$$A_3 = A_2,\ B_3 = A_2B_2,\ A_3B_3 = A_2^2B_2 = tr(A_2)A_2B_2 - B_2.$$

Ceci donne la matrice de changement de base de déterminant 1 :

$$(A_3,B_3,A_3B_3) = (A_2,B_2,A_2B_2) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 6 \end{bmatrix}.$$

Et avec :

$$tr(A_2) = a_2 = 3,\ tr(B_2) = b_2 = 6,\ tr(A_2B_2) = c_2 = 15,$$

on retrouve la relation (2.2) donnée ici par la matrice $Q^{-1}(3)$. Pour les traces on obtient :

$$(a_3, b_3, c_3) = (a_2, b_2, c_2) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & a_2 \end{bmatrix} = (a_2, b_2, c_2)Q^{-1}(a_2) = (3, 15, 39).$$

Avec les notations retenues, on retrouve ainsi la flêche :

$$(2.2) : (A_2, B_2, A_2B_2) \longrightarrow (A_2, A_2B_2, A_2^2B_2) = (A_3, B_3, A_3B_3),$$

$$tr(A_3) = a_3 = 3,\ tr(B_3) = b_3 = 15,\ tr(A_3B_3) = c_3 = 39,$$

et pour le lien avec les suites, en cohérence avec le tableau n°3 :

$$A_3 = A_2 = M_{(\lhd,2)}, \qquad B_3 = A_2B_2 = M_{(\lhd,2,2,2)}.$$

2/ Le passage de $(a_2, b_2, c_2) = (3, 6, 15)$ à $(a_{3'}, b_{3'}, c_{3'}) = (15, 6, 87)$ est fait par une égalité qui traduit la relation (2.3) :

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 6 \end{bmatrix} \begin{bmatrix} 1 & 3 & 15 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 15 & 87 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{bmatrix},$$

c'est à dire par la matrice suivante donnée par la proposition 2.1 :

$$N_{(2,3')} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 6 \end{bmatrix} = Q^{-1}(6).$$

On utilise encore (3.71), et avec l'extrait du tableau n°3 :

(α, β, γ)	(k, k_1, k_2)	(l, l_1, l_2)	X_2	X_1	$S^* = (X_2, 2, X_1)$
$(5, 2, 29)$	$(17, 1, 3)$	$(10, 1, 2)$	$(1, 1, 2)$	(2)	$(\overrightarrow{1, 1, 2}, 2, \overleftarrow{2})$

on obtient :

$$A_{3'} = \begin{bmatrix} 12 & 5 \\ 7 & 3 \end{bmatrix},\ B_{3'} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix},\ A_{3'}B_{3'} = \begin{bmatrix} 70 & 29 \\ 41 & 17 \end{bmatrix},$$

$$A_{3'} = A_2B_2,\ B_{3'} = B_2,\ A_{3'}B_{3'} = A_2B_2^2 = tr(B_2)A_2B_2 - A_2.$$

Pour la comparaison avec le triplet de matrices de hauteur $h = 3$ déjà rencontré :

$$A_{3'} = B_3, \qquad B_{3'} = A_3^{-1}B_3, \qquad A_{3'}B_{3'} = B_3A_3^{-1}B_3,$$

$$A_3 = A_{3'}B_{3'}^{-1}, \qquad B_3 = A_{3'}, \qquad A_3B_3 = A_{3'}B_{3'}^{-1}A_{3'}.$$

Apparait une matrice 3×3 de changement de base de déterminant 1 :

$$(A_{3'}, B_{3'}, A_{3'}B_{3'}) = (A_2, B_2, A_2B_2) \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 6 \end{bmatrix}.$$

On trouve précisément la transformation $(\Sigma(3,1,2)P^{-1}(6)\Sigma(3,1,2)^{-1})$ que l'on a mise en évidence ci-dessus pour la relation (2.3), sachant qu'il faut encore convenir ici :

$$tr(A_2) = a_2 = 3,\ tr(B_2) = b_2 = 6,\ tr(A_2B_2) = c_2 = 15.$$

Pour les traces ceci donne :

$$\begin{aligned} (a_{3'}, b_{3'}, c_{3'}) &= (a_2, b_2, c_2) \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & b_2 \end{bmatrix} \\ &= (a_2, b_2, c_2)(\Sigma(3,1,2)P^{-1}(b_2)\Sigma(3,1,2)^{-1}) \\ &= (15, 6, 87). \end{aligned}$$

Avec les notations choisies, on retrouve aussi la flêche :

$$(2.3) : (A_2, B_2, A_2B_2) \longrightarrow (A_2B_2, B_2, A_2B_2^2) = (A_{3'}, B_{3'}, A_{3'}B_{3'}).$$

$$tr(A_{3'}) = a_{3'} = 15,\ tr(B_{3'}) = b_{3'} = 6,\ tr(A_{3'}B_{3'}) = c_{3'} = 87.$$

Et pour le lien avec les suites, en cohérence avec le tableau n°3 :

$$A_{3'} = A_2B_2 = M_{(\lhd,2,2,2)}, \qquad B_{3'} = B_2 = M_{(2,2)}.$$

3/ Le passage de $(a_{2'}, b_{2'}, c_{2'}) = (6, 3, 15)$ à $(a_{3"}, b_{3"}, c_{3"}) = (6, 15, 87)$ est fait par une égalité qui traduit la relation (2.4) :

$$\begin{bmatrix} 6 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 6 & 15 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 6 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 6 & 87 \\ 0 & 1 & 15 \\ 0 & 0 & 1 \end{bmatrix},$$

c'est à dire par la matrice suivante donnée par la proposition 2.1 :

$$N_{(2',3")} = \begin{bmatrix} 6 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = P^{-1}(6).$$

On pose :

$$A_{2'} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = B_2,\ B_{2'} = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = A_2^{-1}B_2,\ A_{2'}B_{2'} = \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix},$$

puis pour se mettre dans les conditions d'appliquer (2.4) :

$$B_{2"} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = B_2,\ A_{2"} = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix} = A_2^{-1}B_2,\ B_{2"}A_{2"} = \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix}. \quad (3.72)$$

Avec l'extrait du tableau n°3, la période étant $(S^*, 2)$:

(α, β, γ)	(k, k_1, k_2)	(l, l_1, l_2)	X_2	X_1	$S^* = (X_2, 2, X_1)$
$(2, 5, 29)$	$(12, 2, 1)$	$(5, 1, 1)$	(2)	$(2, 1, 1)$	$(\overrightarrow{2}, 2, \overleftarrow{2, 1, 1})$

on obtient alors :

$$A_{3"} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix},\ B_{3"} = \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix},\ A_{3"}B_{3"} = \begin{bmatrix} 75 & 29 \\ 31 & 12 \end{bmatrix},$$

$$A_{3"} = B_{2"}, B_{3"} = B_{2"}A_{2"},\ A_{3"}B_{3"} = B_{2"}^2A_{2"} = tr(B_{2"})B_{2"}A_{2"} - A_{2"}.$$

Ceci donne la matrice de changement de base de déterminant 1 :

$$(A_{3"}, B_{3"}, A_{3"}B_{3"}) = (B_{2"}, A_{2"}, B_{2"}A_{2"}) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 6 \end{bmatrix}.$$

Avec :

$$tr(B_{2^\omega}) = b_{2^\omega} = 6,\ tr(A_{2^\omega}) = a_{2^\omega} = 3,\ tr(B_{2^\omega}A_{2^\omega}) = c_{2^\omega} = 15,$$

on obtient la relation (2.4) donnée ici par la matrice $Q^{-1}(6)$, et pour les traces la formule (2.25) :

$$(a_{3^\omega}, b_{3^\omega}, c_{3^\omega}) = (b_{2^\omega}, a_{2^\omega}, c_{2^\omega}) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 6 \end{bmatrix} = (b_{2^\omega}, a_{2^\omega}, c_{2^\omega})Q^{-1}(a_{2^\omega}) = (6, 15, 87).$$

Avec les notations choisies, on retrouve aussi la flêche :

$$(2.4) : (B_{2^\omega}, A_{2^\omega}, B_{2^\omega}A_{2^\omega}) \longrightarrow (B_{2^\omega}, B_{2^\omega}A_{2^\omega}, B_{2^\omega}^2A_{2^\omega}) = (A_{3^\omega}, B_{3^\omega}, A_{3^\omega}B_{3^\omega}),$$

$$tr(A_{3^\omega}) = a_{3^\omega} = 6,\ tr(B_{3^\omega}) = b_{3^\omega} = 15,\ tr(A_{3^\omega}B_{3^\omega}) = c_{3^\omega} = 87.$$

Et pour les suites, on a bien en cohérence avec le tableau n°3 :

$$A_{3^\omega} = B_2 = M_{(2,2)}, \qquad B_{3^\omega} = B_2A_2^{-1}B_2 = M_{(2,2,\triangleright,2)}.$$

Le choix des notations fait ici est essentiel pour ne pas confondre les matrices entre elles tout en respectant la convention de notation que l'on s'est donnée à l'issue de la proposition 2.1. En particulier on voit que l'on fait un choix bien particulier avec (3.72) qui est très différent de (3.71). En fait on s'est un peu compliqué la vie en passant par $(B_{2^\omega}, A_{2^\omega})$. On aurait plutôt du utiliser $({}^tB_2, {}^tA_2)$. Avec ce que l'on a vu antérieurement :

$$\begin{aligned} (B_{2^\omega}, A_{2^\omega}) &= (\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^{-1} ({}^tB_2) \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^{-1} ({}^tA_2) \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}) \\ &= (B_2, A_2^{-1}B_2), \end{aligned}$$

soit :

$${}^tB_2 = M_{(2,2)}, \qquad {}^tA_2 = M_{(2,\triangleright)},$$

et la relation (2.4) s'écrit alors :

$$\begin{aligned} ({}^tB_2, {}^tA_2, ({}^tB_2)({}^tA_2)) &\longrightarrow ({}^tB_2, ({}^tB_2)({}^tA_2), ({}^tB_2)^2({}^tA_2)) \\ &= (\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 12 & 7 \\ 5 & 3 \end{bmatrix}, \begin{bmatrix} 70 & 41 \\ 29 & 17 \end{bmatrix}). \end{aligned}$$

Elle donne le bon triplet de traces, mais pas le même triplet de matrices. En réalité on trouve encore un automorphisme intérieur permettant de passer de l'un à l'autre, et qui conserve la cohérence avec le tableau n°3 si l'on remarque simplement qu'au lieu de considérer une expression de forme $(S^*, 2)$ on doit regarder maintenant un terme de forme $(2, S)$:

$$\begin{aligned} {}^tB_2 &= M_{(2,2)} = M_{(2)} A_{3''} M_{(2)}^{-1}, \\ ({}^tB_2)({}^tA_2) &= M_{(2,2,2,\triangleright)} = M_{(2)} B_{3''} M_{(2)}^{-1} = M_{(2)} M_{(2,2,\triangleright,2)} M_{(2)}^{-1}. \end{aligned}$$

4/ Le passage de $(a_{2'}, b_{2'}, c_{2'}) = (6, 3, 15)$ à $(a_{3'''}, b_{3'''}, c_{3'''}) = (15, 3, 39)$ est fait par une égalité qui traduit la relation (2.5) :

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 6 & 15 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 15 & 39 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix},$$

c'est à dire par la matrice suivante donnée par la proposition 2.1 :

$$N_{(2',3''')} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 3 \end{bmatrix} = Q^{-1}(3).$$

On pose cette fois encore, en cohérence avec (3.72) :

$$A_{2'} = B_{2''} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix},\ B_{2'} = A_{2''} = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix},\ A_{2'}B_{2'} = \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix},$$

et avec l'extrait du même tableau n°3, la période étant $(S^*, 2)$:

(α, β, γ)	(k, k_1, k_2)	(l, l_1, l_2)	X_2	X_1	$S^* = (\overrightarrow{X_2}, 2, \overleftarrow{X_1})$
$(5, 1, 13)$	$(5, 0, 2)$	$(2, 1, 1)$	$(2, 1, 1)$	$(\triangleright)$	$(\overrightarrow{2, 1, 1}, 1, 1)$

on obtient avec (**??**) :

$$A_{3'''} = \begin{bmatrix} 13 & 5 \\ 5 & 2 \end{bmatrix},\ B_{3'''} = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix},\ A_{3'''}B_{3'''} = \begin{bmatrix} 34 & 13 \\ 13 & 5 \end{bmatrix},$$

$$A_{3'''} = B_{2''}A_{2''},\ B_{3'''} = A_{2''},\ A_{3'''}B_{3'''} = B_{2''}A_{2''}^2 = tr(A_{2''})B_{2''}A_{2''} - B_{2''}.$$

Ceci donne la matrice de changement de base de déterminant 1 :

$$(A_{3'''}, B_{3'''}, A_{3'''}B_{3'''}) = (B_{2"}, A_{2"}, B_{2"}A_{2"}) \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix}.$$

Avec :

$$tr(B_{2"}) = b_{2"} = 6,\ tr(A_{2"}) = a_{2"} = 3,\ tr(B_{2"}A_{2"}) = c_{2"} = 15,$$

on retrouve la relation (2.5) par la matrice $(\Sigma(3,1,2)P^{-1}(3)\Sigma(3,1,2)^{-1})$, et pour les traces on obtient la formule (2.28) :

$$\begin{aligned}(a_{3'''}, b_{3'''}, c_{3'''}) &= (b_{2"}, a_{2"}, c_{2"}) \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & a_{2"} \end{bmatrix} \\ &= (b_{2"}, a_{2"}, c_{2"})(\Sigma(3,1,2)P^{-1}(a_{2"})\Sigma(3,1,2)^{-1}).\end{aligned}$$

Avec les notations choisies, on retrouve aussi la flêche :

$$(2.5) : (B_{2"}, A_{2"}, B_{2"}A_{2"}) \longrightarrow (B_{2"}A_{2"}, A_{2"}, B_{2"}A_{2"}^2) = (A_{3'''}, B_{3'''}, A_{3'''}B_{3'''}),$$

$$tr(A_{3'''}) = a_{3"} = 15,\ tr(B_{3'''}) = b_{3"} = 3,\ tr(A_{3'''}B_{3'''}) = c_{3"} = 39.$$

Et pour les suites, on a bien en cohérence avec le tableau n°3 :

$$A_{3'''} = B_{2"}A_{2"} = B_2A_2^{-1}B_2 = M_{(2,2,\triangleright,2)}, \qquad B_{3'''} = A_{2"} = A_2^{-1}B_2 = M_{(\triangleright,2)}.$$

Mais comme on l'a vu ci-dessus, on aurait pu utiliser plutôt ${}^tB_2 = M_{(2,2)}$ et ${}^tA_2 = M_{(2,\triangleright)}$ qui donnent avec un automorphisme intérieur :

$$A_{2'} = M_2^{-1}({}^tB_2)M_2 = M_{(2,2)}, \qquad B_{2'} = M_2^{-1}({}^tA_2)M_2 = M_{(\triangleright,2)}.$$

On aurait alors trouvé avec la flêche (2.5) :

$$({}^tB_2, {}^tA_2, B_{2"}({}^tA_2)) \longrightarrow ({}^tB_2\,{}^tA_2, {}^tA_2, {}^tB_2({}^tA_2)^2) = (B_{3''''}, A_{3''''}, B_{3''''}A_{3''''}),$$

où avec un automorphisme intérieur :

$$\begin{aligned}B_{3''''} &= {}^tB_2\,{}^tA_2 = M_{(2,2,2,\triangleright)} = M_2A_{3'''}M_2^{-1}, \\ A_{3''''} &= {}^tA_2 = M_{(2,\triangleright)} = M_2B_{3'''}M_2^{-1}.\end{aligned}$$

4. Conclusion provisoire

Sur les quatre cas que l'on vient d'étudier, on a rendu plus précises les notations. On a assuré la cohérence avec toutes les informations du tableau n°3. On a aussi explicité les automorphismes intérieurs qui ont permis de mettre en forme ces informations pour permettre l'application des figures 10 et 11. Ceci permet de décrire la racine de l'arbre ibérique comme suit :

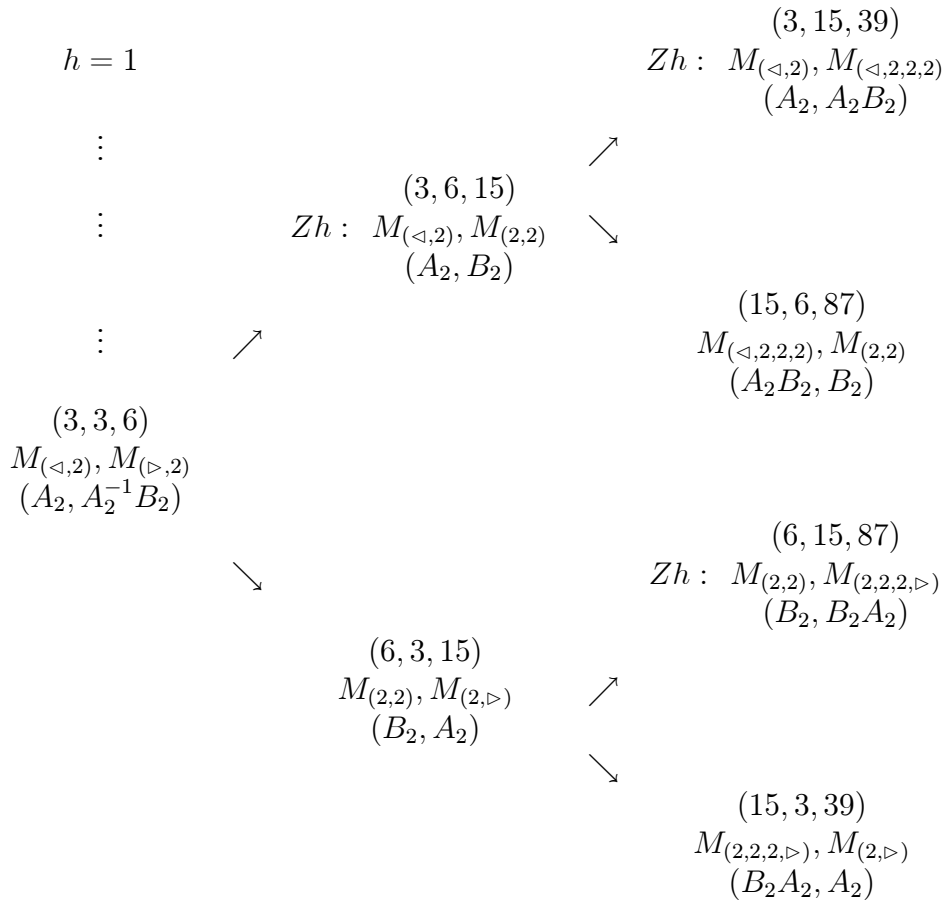


fig. 12 : L'arbre ibérique.

On a vu comment à la hauteur $h = 2$ de l'arbre ibérique on ne trouvait que les triplets $(3, 6, 15)$ correspondant au couple de matrices (A_2, B_2), et $(6, 3, 15)$

correspondant au couple de matrices $({}^tB_2, {}^tA_2) = (B_2, A_2)$, avec :

$$A_2 = M_{(\lhd,2)} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = {}^tA_2,\ B_2 = M_{(2,2)} = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix} = {}^tB_2,$$

Sur ces racines on peut construire tout l'arbre des triplets ibériques grâce aux figures 10 et 11, arbre dans lequel on fait apparaitre les décompositions de suites associées, les couples de matrices (A, B) qui s'en déduisent par récurrence. La figure n°12 résume la structure pour les suites situées à la racine de l'arbre ibérique. Pour $h > 1$ le premier terme du couple (A, B) commence par A_2 si et seulement si on est dans le demi arbre supérieur, et par B_2 si et seulement si on est dans le demi arbre inférieur. En réalité les couples (A, B) qui apparaissent dans cet arbre ne peuvent se déduire les uns des autres par des automorphismes intérieurs, car les triplets de Markoff associés sont différents ([40] p.183 prop 5.3.). Chacun de ces couples engendre le groupe $\mathbf{F}_2 = [SL(2,\mathbb{Z}), SL(2,\mathbb{Z})]$, ceci s'établit facilement par récurrence avec les figures 10 et 11, et surtout en utilisant le fait de départ rappelé ci-dessus que l'on peut choisir pour engendrer ce groupe les deux matrices ([37] p. 998) :

$$A_0 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \qquad B_0 = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix},$$

On a aussi vu, lorsque l'on a étudié ce qui se passe aux hauteurs $h = 1$ ou $h = 2$, que l'on a :

$$(B_0^{-1}, A_0^{-1}{B_0}^{-1}, {B_0}^{-1}A_0^{-1}{B_0}^{-1}) = (A_1, B_1, A_1B_1) = (A_2, A_2^{-1}B_2, B_2).$$

De sorte que (A_2, B_2) est aussi un système générateur de $\mathbf{F}_2$, ceci se déduit du fait que (A_0, B_0) en est un.

Pour terminer cette première partie, on résume les résultats que l'on a obtenus dans ce qui précède :

1/ On a indiqué que plusieurs arbres peuvent être considérés pour l'étude de la théorie de Markoff, et on a donné les différences entre eux. Pour l'arbre de Zhang et l'arbre ibérique on a détaillé comment en construire plusieurs modèles, le modèle arithmétique utilisant les triplets (a, b, c), le modèle 2×2 utilisant les triplets de matrices (A, B, AB), le modèle 3×3 utilisant les matrices $M(a, b, c)$. On a indiqué l'origine de ces modèles en les reliant les uns aux autres, et on a donné tous les algorithmes permettant de les constuire de façon directe.

2/ On a montré comment l'arbre de Zhang semblait très adapté à l'étude de la conjecture de Frobenius, tout en établissant que les triplets de l'arbre ibérique

vérifiant la propriété Z semblaient aussi bien adaptés à cette étude. On a caractérisé cette propriété Z.

3/ On a détaillé comment les matrices $M(a,b,c)$ donnent le groupe de Heisenberg, ainsi que le contexte dans lequel la conjecture de Frobenius se traduit par la conjecture de Tyurin.

4/ On a donné de nouvelles propriétés de divisibilité pour les triplets ibériques (a,b,c) qui adaptent à l'arbre ibérique des propriétés analogues trouvées par Riedel [47] pour son arbre.

5/ On a fourni les moyens de passer directement du formalisme utilisé par Cassels ([13] p. 27-30) à celui de l'arbre ibérique dans son modèle arithmétique. On en a déduit de nouvelles formules qui généralisent celles qui apparaissent dans [13].

6/ Avec l'algorithme permettant de constuire de façon directe les suites S, on a établi que ces dernières ne contiennent qu'un nombre pair de termes, ce ne sont que des 1 et des 2.

7/ On a montré comment les propriétés de palindromie des suites S se traduisent en des décompositions en somme de deux carrés premiers entre eux $\gamma = a_{11}^2 + a_{12}^2$. A partir de là le lemme 4.2 de [47] a été complètement démontré. Il joue un rôle essentiel dans les travaux de Riedel.

8/ Sur ces bases on a démontré la conjecture de Frobenius dans le cas très particulier où $c = 2^{e_c}3p^e$ où $e_c \in \{0,1\}$, p premier, et $e \in \mathbb{N}^*$. Ceci permet d'identifier une signification plus générale de la conjecture : elle dirait que pour les valeurs de c apparaissant dans l'arbre ibérique, $c = 3\gamma = 2^{e_c}3\mathfrak{c}$, $e_c \in \{0,1\}$, $\mathfrak{c}$ premier à 6, les suites associées S ne contiendraient des 1 et des 2 que dans un cas au plus pour c. Chaque valeur du facteur $\gamma = a_{11}^2 + a_{12}^2$ peut posséder plusieurs décompositions en somme de deux carrés premiers entre eux, mais au plus une d'entre elles serait associée à des suites S de longueur paire et ne contenant que des 1 et des 2, sachant que l'on a :

$$\frac{\gamma}{k} = [\lhd S] = [1, \omega_0 - 1, \omega_1, ..., \omega_{2j}].$$

Fin de la première partie

References

[1] M. Aigner, Markov theorem and 100 years of the uniqueness conjecture, A mathematical journey from irrational numbers to perfect matching, Springer, 2013

[2] D. Alpern, Generic two integer variable equation solver, www.alpertron.com.ar/QUAD.HTM

[3] G.P. Basharin, A.N. Langville, V.A. Naumov, The life and work of A.A. Markoff, Linear algebra and its applications, 2004, vol. 386, pp.3-26

[4] A. Baragar, On the unicity conjecture for Markoff numbers, Canad. Math. Bull., 1996, n°39, pp. 3-9

[5] Z.I. Borevitch, I.R. Chafarevitch, Théorie des nombres, Gauthier-Villars, 1967

[6] G.Y. Belyi, Markov's numbers and quadratic forms, Journal of Mathematical Sciences, 2001, vol 106, issue 4, pp. 3087-3097

[7] E. Bombieri, Continued fractions and the Markoff tree, Expositiones Mathematicae, 2007, 25 n°3, pp. 187-213

[8] I. Borosh, Numerical evidence of the uniqueness of Markov numbers, Notices A.M.S. 21, A55 Abstract n°711-10, 1974, p. 32 (voir aussi : BIT 15, n°4, 1975, pp. 351-357)

[9] D.A. Buell, Binary quadratic forms - Classical theory and modern computations, Springer Verlag, 1989

[10] Y. Bugeaud, C. Reutenauer, S. Siksek, A sturmian sequence related to the uniqueness conjecture for Markoff numbers, Theoretical Computer Science, n°410, 2009, pp. 2864-2869

[11] J.O. Button, On the uniqueness of prime Markoff numbers, J. London Math. Soc., 1998 n°2, 58, pp. 9-17

[12] J.O. Button, Markoff numbers, principal ideals and continued fractions expansions, Journal of Number Theory, 2001, n°87, pp. 77-95

[13] J.W.S. Cassels, An introduction to Diophantine Approximation, Cambridge Univ. Press., 1957, Chapitre 2

[14] F.J. Chen, Y.G. Chen, On the Frobenius conjecture for Markoff numbers, Journal of Number Theory, vol 133, issue 7, July 2013, pp. 2363-2373

[15] H. Cohn, Approach to Markoff's minimal forms through modular functions, Ann. of Math., 1955, n°61, pp. 1-12

[16] H. Cohn, Representation of Markoff's binary quadratic forms by geodesics on a perforated torus, Acta Arithmetica, XIII, 1971, pp. 123-136

[17] H. Cohn, Markoff forms and Primitive Words, Math. Ann. 196, 1972, pp. 8-22

[18] H. Cohn, Minimality bounds for traces of Markoff matrices, Canadian Math. Soc. Conference Proceedings vol. 15, 1975 pp. 109-121

[19] H. Cohn, Ternary forms as invariants of Markoff forms and other $SL_2(\mathbb{Z})$-bundles, Linear algebra and its applications, n°21, 1978, pp. 3-12

[20] D.A.Cox, Primes of the form $x^2 + ny^2$, Wiley, 1989

[21] T.W. Cusick, M.E. Flahive, The Markoff and Lagrange spectra, Mathematical Surveys and Monographs, 30, American Mathematical Society, 1989

[22] S. Cecotti, C. Vafa, Topological-anti-topological fusion, Nuclear Phys B, 1991, 367 n°2, p. 359-461

[23] S. Cecotti, C. Vafa, On classification of N=2 supersymmetric theories, Commun. Math. Phys. 158, 1993, pp. 569-644

[24] B.N. Delone, On the work of A.A. Markoff "On binary quadratics forms with positive determinant", Usp. Math. Nauk. n°5, 1948, pp.3-5

[25] F.G. Frobenius, Über die Markoffschen Zahlen, Preuss. Akad. Wiss. Sitzungsber., 1913, pp. 458-487

[26] A.L. Gorodentsev, A.N. Rudakov, Exceptional vector bundles on projective spaces, Duke Math. J., 1987, n°54, pp. 115-130

[27] D.S. Gorshkov, Geometry of Lobachevski in connection with certain questions of arithmetics, J. Soviet Math. 16, 1981, n°1, pp.788-826

[28] R.K. Guy, Unsolved problems in number theory, Vol.1, Problem books in Mathematics, Springer Verlag, 1981

[29] G.H. Hardy, E.M. Wright, Introduction to the theory of numbers, fifth edition, Oxford, 1979

[30] H.L. Keng, Introduction to number theory, Springer Verlag, 1982

[31] M. Kibler, Variations on a theme of Heisenberg, Pauli and Weyl, http://arXiv:0807.2837 v1 [quant-ph]1Jul 2008

[32] E. Landau, Elementary number theory, Chelsea Piblishing Company, 1958

[33] W.J. Leveque, Topics in number theory, vol. 1 and 2, Dover, 2002

[34] M.L. Lang, S.P. Tan, A simple proof of the Markoff conjecture for prime powers, arXiv:0508443v1 [math.NT] 24 aug 2005

[35] A.V. Malyshev, Markov and Lagrange spectra, (Survey of the literature), J. Soviet Math. 16, 1981, n°1, pp.767-788

[36] A.A. Markoff, Sur les formes quadratiques indéfinies, partie 1: Math. Ann. 6, 1879, pp. 381-406, partie 2: Math. Ann. 17, 1880, pp. 379-399

[37] W. Magnus, A. Karass, D. Solitar, Combinatorial group theory, Dover, 1976

[38] G. McShane, H. Parlier, Multiplicities of simple closed geodesics and hypersurface in Teichmüller space, arXiv:math/0701835v2 [math.GT] 25 Jul 2007

[39] S. Perrine, L'interprétation matricielle de la théorie de Markoff classique, Int. J. Math. Sci. 32, 2002, n°4, pp.193-262

[40] S. Perrine, La théorie de Markoff et ses développements, Tessier & Ashpool, 2002

[41] S. Perrine, Recherches autour de la théorie de Markoff, arXiv:0307032v1 [math-ph] 16 Jul 2003

[42] S. Perrine, De Frobenius à Riedel : analyse des solutions de l'équation de Markoff, conférence à la journée « Groupes, géométrie discrète et information quantique », organisée à l'Institut de Physique Nucléaire de Lyon, le 11 juin 2009 (revue détaillée de N. Riedel, Markoff equation and nilpotent matrices, arXiv:0709.1499 v4 [math.NT] 5 Aug 2008), http//hal.archives-ouvertes.fr/docs/00/40/66/01/PDF/Perrine.ori.pdf

[43] X. Peng, J. Zhang, Cluster algebras and Markoff numbers, CaMUS n°3, 2012, pp. 19-26

[44] O. Perron, Die Lehre Von den Kettenbruchen, Teubner, 1913, Kessinger Legacy Reprints

[45] C. Ricke, On the cluster algebra associated with the once punctured torus, Master Thesis, Universität Bonn, 2013

[46] N. Riedel, Markoff equation and nilpotent matrices, arXiv:0709.1499 v1 [math.NT] 10 Sep 2007, revu plusieurs fois jusqu'à 1499 v7 [math.NT] 29 Mar 2013, http://arxiv.org/abs/0709.1499

[47] N. Riedel, On the Markoff Equation, arXiv:1208.4032 v8 [math.NT] 12 Jan 2014, http://arxiv.org/abs/1208.4032

[48] H.E. Rose, A course in number theory, Oxford Science publications, 1988

[49] D. Rosen, G.S. Patterson, Some numerical evidence concerning the uniqueness of the Markoff numbers, Math. of Comp., 1971, 25, pp. 919-921

[50] G. Rosenberg, The uniqueness of the Markoff numbers, Math.of Comp., 1976, n°134, pp. 361 365 (review by R. Bumby M.R. 1977, p. 280)

[51] A.N. Rudakov, Markov numbers and exceptionnal bundles on P^2, english translation in Math. USSR Izv. 32, 1989, n°1, pp. 99-112

[52] P. Schmutz, Systoles of arithmetic surfaces and the Markoff spectrum, Math. Ann., 1996, 305 n°1, pp. 191-203

[53] V. Senkel, Markoffzahlen, Diplomarbeit, Universität Biekefeld, November 1997

[54] A. Srinivasan, A realy simple proof of the Markoff conjecture for prime powers, www.numbertheory.org/pdfs/simpleproof.pdf

[55] B. Stolt, On the diophantine equation $u^2 - Dv^2 = \pm 4N$, Arkiv für Matematik, Band 2 n°1, 1951, pp. 1-23

[56] L. Szalay, On the resolution of simultaneous Pell equations, Annales Mathematicae et Informaticae, n°34, 2007, pp. 77-87

[57] A. Tyurin, Vector bundles, Universitätverlag Gottingen, 2006

[58] M. F. Vigneras, Arithmétique des corps de quaternions, Lecture Notes in Mathematics n°800, Springer Verlag, 1980

[59] M. Waldschmidt, Open diophantine problems, Moscow Mathematical Journal 4 (2004), n°1, pp. 245-305

[60] M. Waldschmidt, Autour de l'équation de Markoff $x^2 + y^2 + z^2 = 3xyz$, Rencontres stéphanoises en théorie de nombres, Approximation diophantienne et théorie analytique des nombres, St Etienne, 5 au 7 juin 2008, http://www.math.jussieu.fr/~miw/articles/pdf/MarkoffBeamerFrVI.pdf

[61] D. Zagier, On the number of Markoff numbers below a given bound, Mathematics of Computations, 39, 1982, n°160, pp. 709-723

[62] Y. Zhang, Congruence and uniqueness of certain Markoff numbers, arXiv:math/0612620v2 [math.NT] 29 Dec 2006 Acta Arithmetica, n°128, 207, pp. 295-301

[63] Y. Zhang, An elementary proof of Markoff conjecture for prime powers, arXiv:math/0606283v2 [math.NT] 1 Feb 2007

[64] Q. Zhou, On the uniqueness conjecture for Markoff triples, arXiv.math/0010131v1, [math.GT] 13 Oct 2000