UCLouvain

FACULTE DES SCIENCES

Faculté des sciences

Sur les formes quadratiques binaires et les entiers Löschiens

Auteur·es : Sébastien Antoine
Promoteur·rices : Pierre-Emmanuel Caprace
Lecteur·rices : Thimotée Marquis, Enrico Vitale
Année académique 2023-2024

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
FACULTÉ DES SCIENCES
ÉCOLE DE MATHÉMATIQUES

Sur les formes quadratiques binaires et les entiers Löschiens

Sébastien Antoine
Promoteur : Pierre-Emmanuel Caprace
Lecteurs : Thimotée Marquis, Enrico Vitale

Mémoire de master
Juin 2024

Table des matières

Remerciements

Je tiens tout d'abord à remercier mon promoteur, Professeur Pierre-Emmanuel Caprace, pour son aide, sa disponibilité et pour m'avoir proposé ce sujet qui m'a tant passionné ces derniers mois. Sans ses précieux conseils, ce mémoire n'aurait jamais pu aboutir à ce qu'il est aujourd'hui.

Un tout grand merci aux lecteurs, Professeur Thimotée Marquis et Professeur Enrico Vitale, d'avoir accepté ma demande. J'espère que vous apprécierez la lecture de ces quelques pages.

Enfin, je tiens à remercier ma famille qui m'a soutenu durant toutes ces années. Je n'y serais pas arrivé sans vous.

Chapitre 1

Introduction

Dans ce mémoire, nous nous proposons de revisiter la théorie arithmétique des formes quadratiques binaires. Nous tenterons principalement de déterminer quelles sont les conditions qu'un entier n doit satisfaire pour pouvoir s'écrire comme

$$n = ax^2 + bxy + cy^2$$

où a, b, c sont des entiers fixés et x, y des variables entières.

L'étude de cette question est historiquement très chargée. En 1640, P. de Fermat mentionne dans une lettre à M. Mersenne avoir une preuve rigoureuse du théorème suivant,

Théorème 1.1 (Fermat)**.** *Soit p un premier tel que $p \equiv 1 \mod 4$. Alors, il existe des entiers x, y tels que*

$$p = x^2 + y^2.$$

S'il ne donne pas de preuve dans sa lettre, il n'est pas exagéré de dire que ce théorème et la recherche de sa preuve par ses successeurs est le début d'une investigation particulièrement fructueuse. L. Euler dédia une quarantaine d'années à l'élaboration d'une démonstration. Au fil de ses recherches, il découvrit notamment l'importance des résidus quadratiques et surtout de leurs propriétés de réciprocité. S'il n'a jamais pu énoncer le théorème de réciprocité quadratique, ses investigations l'ont tout de même conduit à remarquer le comportement particulier des résidus quadratiques.

Il faudra attendre les travaux fondateurs de J.-L. Lagrange pour introduire des outils efficaces pour résoudre ce genre de problème. Celui-ci introduit la définition d'une forme quadratique binaire, i.e. un polynôme homogène de degré deux à coefficients dans les entiers. Les formes quadratiques binaires ont donc la forme suivante

$$f(X, Y) = aX^2 + bXY + cY^2$$

où a, b, c sont des entiers. Le point central de son travail fut de déterminer que deux formes quadratiques binaires f et F **représentent** les mêmes entiers, c'est-à-dire que

les équations $f(x,y) = n$ et $F(x,y) = n$ ont toutes deux des solutions dans les entiers, s'il existe une relation du type

$$f(X,Y) = F(rX + sY, tX + uY)$$

où r, s, t et u sont des entiers tels que $ru - st = \pm 1$.

Cette observation est le point de départ des considérations de notre chapitre 3. Dans la première partie de ce chapitre, nous allons donner une théorie permettant de déterminer quelles sont les conditions imposées sur un entier pour pouvoir être représenté par une forme quadratique binaire. Nous verrons qu'il n'est en général pas aisé de déterminer ces conditions. Toutefois, nous donnerons un exemple concret au travers du théorème suivant,

Théorème 1.2. *Soit n un naturel et soit $n = 2^{\alpha_1}3^{\alpha_2}p_2^{\alpha_3}\cdots p_t^{\alpha_t}$ sa décomposition en facteurs premiers avec α_1, α_2 possiblement nuls. Alors, n est représenté par la forme quadratique binaire*

$$X^2 + XY + Y^2$$

si et seulement si n satisfait les conditions suivantes :

1. *la puissance α_1 est paire ;*
2. *toute puissance α_i associée à un facteur premier p_i de la forme $6k-1$ pour $k \in \mathbb{N}$ est paire.*

Les entiers décrits par ce théorème sont appelés les **entiers Löschiens** et leur étude sera le fil rouge de notre chapitre 3. Ce théorème sera déduit par nos soins dans la section 3.5 à partir de la théorie générale établie de la section 3.1 jusqu'à la section 3.4 comprise. Ces dernières sont inspirées des références [2] et [5].

Ensuite, nous nous intéresserons au nombre de représentations d'un entier par une forme quadratique binaire. Une fois de plus, la question s'avère ardue en toute généralité. La section 3.6 introduit la théorie et s'inspire de la référence [10]. La dernière section de ce chapitre portera sur le nombre de représentations dites **propres** d'un entier par la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Cette section est en grande partie originale et se cristallise dans le théorème suivant.

Théorème 1.3. *Soit n un entier proprement représenté par la forme quadratique binaire*

$$f(X,Y) = X^2 + XY + Y^2.$$

L'entier n admet $6 \cdot 2^s$ représentations propres distinctes par f, où s est égal au nombre de facteurs premiers de n de la forme $6k+1$, avec $k \in \mathbb{N}$.

Le chapitre 4 prend un tout autre parti pour étudier les formes quadratiques binaires. Nous allons associer des représentations de graphes aux formes quadratiques binaires. Cette façon d'appréhender les formes quadratiques binaires est due à J. H. Conway dans son livre *The sensual quadratic form* [6]. Nous basons une grande partie de notre travail sur le premier chapitre de ce livre. Nous avons également utilisé la référence [11] pour approfondir l'analyse de ces nouvelles méthodes.

Nous commencerons le chapitre 4 par définir la notion de réseau et expliciterons la nature du **topographe** d'un réseau. Ensuite, nous appliquerons ces topographes à la théorie des formes quadratiques binaires. Ces considérations nous mènerons à l'éllaboration des **topographes de Conway** d'une forme quadratique binaire. Ceux-ci apportent une image aux formes quadratiques binaires. Nous décrivons ces images de la section 4.6 jusqu'à la section 4.8 comprises. Ces images donnent de réels informations sur les formes quadratiques binaires et elles nous permettront de conclure notre travail sur un théorème de classification des formes quadratiques binaires.

Nos contributions personnelles sont diverses. En ce qui concerne le chapitre 3 et la théorie arithmétique standard des formes quadratiques binaires, notre travail fut principalement de rassembler les différentes présentations données dans les références [2] et [5] et d'en donner une exposition unifiée. Les résultats concernant la théorie de la **réduction** des formes quadratiques binaires **définies positives** données dans la section 6 du chapitre VI de la référence [5] sont dépourvues de preuve et leur analogue dans la référence [2] sont prouvés ou bien laissés en exercice. Nous avons donc énoncé et prouvé chacun des résultats nécessaires au sein de notre section 3.4. Enfin, l'exemple des entiers Löschiens est, comme mentionné plus tôt, déduit par nos soins.

Les résultats concernant le nombre de représentations propres de la référence [10] sont quelque peu succincts. Nous avons donc grandement étayé les résultats et surtout adapté ceux-ci au formalisme précédemment développé. Une fois de plus, la section 3.7 déduisant le nombre de représentations propres des entiers Löschiens est originale.

Nous faisons désormais un commentaire sur la théorie développée au chapitre 4. Malgré les qualités indéniables du premier chapitre du livre *The sensual quadratic form*, il nous paraît particulièrement important de mentionner certaines imprécisions faites au profit de la concision. Les constructions réalisées dans ce premier chapitre se basent fortement sur la notion de graphe planaire. Les preuves réalisées, notamment pour montrer que les topographes sont des arbres, nécessitent le caractère planaire des topographes en question. Or, il n'est prouvé à aucun moment que les topographes sont planaires. Une tentative naïve de démonstration du caractère planaire de ces graphes à partir de ce premier chapitre induit l'usage de la propriété d'arbre des topographes. Pour ne pas rentrer dans des arguments circulaires, il faut donc s'assurer que les topographes sont des arbres avant d'utiliser les propriétés planaires. Une grande partie de notre travail fut en réalité de ne pas tomber dans cet écueil. Il est à noté que la référence [11] ne démontre pas non-plus le caractère planaire avant d'en utiliser les propriétés.

La théorie des topographes de Conway n'est pas fondamentalement changée par notre ajout de ce formalisme. Cependant, ce formalisme permet de mieux rendre compte du lien entre les **automorphismes de formes quadratiques binaires** et les **automorphismes de topographe de Conway**. Dans son livre, J. Conway ne détaille pas cette correspondance et il semble assumer l'existence d'un lien entre ce qu'il appelle les isométries du plan préservant le topographe de Conway et les isométries de la forme quadratique binaire. Par isométrie de formes quadratiques binaires, nous pouvons entendre automorphisme. Le lien qui existe entre ces deux notions n'est pas clair. Toutefois, nous pourrons au moins montrer que, dans notre formalisme, il n'y a pas d'isomorphisme entre ces groupes d'isométries. Nous établissons ce résultat en fin de section 4.6.

Finalement, dans son livre [6], J. H. Conway conclut son premier chapitre par le théorème suivant,

Théorème 1.4. *Pour tout entier a, b, c et n, il existe un procédé algorithmique permettant de décider si l'équation diophantienne*

$$aX^2 + bXY + cY^2 = n$$

admet une solution dans les entiers et de déterminer ces entiers dans le cas où l'équation est résoluble. Il y a aussi un procédé efficace pour déterminer si deux formes quadratiques binaires sont équivalentes et pour déterminer le groupe d'automorphismes d'une forme quadratique binaire.

Nous donnons en annexe A un code python permettant, dans certains cas, de décider grâce à la théorie des topographes de Conway si une telle équation est résoluble.

Chapitre 2

Préliminaires

La théorie des formes quadratiques binaires constitue un chapitre important de la théorie des nombres. Nous rappelons dans les prochaines sections les notions clefs que nous utiliserons lors des prochains chapitres. Nous rappelons aussi dans ce chapitre certaines propriétés des groupes de matrices inversibles sur l'anneau des entiers.

Les résultats de théorie des nombres présentés ci-dessous, ainsi que leur preuve, peuvent être trouvés dans la référence [9]. Lorsque cela nous semblait pertinent, nous avons pris la liberté d'apporter du contexte aux différents résultats au sein même de leur énoncé. Certains résultats ne sont donc pas repris à l'identique de la référence. Nous espérons toutefois que cela participera à la bonne compréhension du texte.

2.1 Propriétés de l'anneau des entiers, identité de Bézout et théorème fondamental de l'arithmétique

Nous rappelons dans cette section certaines propriétés standards de l'anneau des entiers $\mathbb{Z}$ et l'identité de Bézout. Nous commençons par le fait que l'anneau des entiers est un anneau euclidien.

Proposition 2.1. *[9, en p.9] Soient a un entier et b un entier non nul. Alors, il existe des entiers q et r tels que $a = qb + r$ avec $|r| < |b|$.*

Nous utilisons ci-dessous la structure d'anneau de $\mathbb{Z}$ et de ses idéaux principaux afin de donner une caractérisation en terme d'idéaux de la notion du plus grand commun diviseur.

Lemme 2.2. *[9, Lemma 3 en p.4] Si a et b sont des entiers, alors il existe un entier d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Nous définissons le plus grand commun diviseur.

Définition 2.3. *[9, Definition en p.4] Soient a et b des entiers. On dit d'un entier d qu'il est* ***un plus grand commun diviseur commun*** *de a et b, noté* $\text{pgcd}(a, b)$*, s'il divise a et b et si tous les autres diviseurs communs de a et b divisent d.*

Nous donnons la définition d'entiers premiers entre eux.

Définition 2.4. *Deux entiers a et b sont dits* ***premiers entre eux*** *si leurs seuls diviseurs communs sont ± 1. Nous dirons aussi que des entiers $x_1, x_2, \ldots, x_n$ sont premiers entre eux s'ils sont deux à deux premiers entre eux.*

La proposition suivante fait le lien entre la notion de plus grand commun diviseur et la notion d'idéal dans les entiers.

Proposition 2.5. *[9, Lemma 4 en p.4] Soient a et b des entiers. Si $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, alors d est un plus grand commun diviseur de a et b.*

De ce lemme, nous pouvons donner le théorème suivant. Ce théorème n'étant pas repris dans la référence [9], nous en donnons aussi une preuve.

Théorème 2.6 (Théorème de Bézout)**.** *Soient a et b des entiers. Les entiers a et b sont premiers entre eux si et seulement si l'équation*

$$aX + bY = 1$$

admet une solution entière.

Démonstration. Supposons que les entiers a et b soient premiers entre eux. Alors, leurs plus grands diviseurs communs sont ± 1. Dès lors, par la proposition 2.5, nous savons que l'idéal engendré par a et b est $1\mathbb{Z} = \mathbb{Z}$. Par conséquent, il existe des entiers x, y tels que

$$ax + by = 1.$$

Supposons désormais que l'équation

$$aX + bY = 1$$

admette une solution. Alors, tout diviseur commun à a et b divise 1. L'entier 1 n'admet que deux diviseurs -1 et lui-même. Comme 1 et -1 divisent tous les entiers, on déduit que a et b sont premiers entre eux. □

Nous concluons cette section par le théorème fondamental de l'arithmétique.

Théorème 2.7 (Théorème fondamental de l'arithmétique)**.** *[9, Theorem 1 en p.3] Pour tout entier n, il existe une factorisation en nombre premier*

$$n = (-1)^{\epsilon(n)} \prod_p p^{a(p)},$$

où les exposants $a(p)$ sont des naturels uniquement déterminés par n tels que $a(p) \neq 0$ pour un nombre fini de nombres premiers et où $\epsilon(n) = 0$ si n est positif et $\epsilon(n) = 1$ si n est négatif.

La prochaine section portera sur les notions de base d'arithmétique modulaire.

2.2 Éléments d'arithmétique modulaire

Dans un souci de complétude et afin de fixer les notations, nous rappelons ci-dessous la définition de congruence que nous emploierons par la suite.

Définition 2.8. *Soient a et b deux entiers et n un naturel. On dit que a et b sont* ***congrus modulo*** *n, noté*

$$a \equiv b \mod n,$$

si $a - b$ est un divisible par n.

Dans les prochains chapitres, nous serons amenés à résoudre des équations modulaires ainsi que des systèmes d'équations modulaires. À cet effet, nous rappelons le théorème des restes chinois.

Théorème 2.9 (Théorème des restes chinois)**.** *[9, Theorem 1' en p.35] Soient $m_1, m_2, \ldots, m_k$ des entiers premiers entre eux et $m = m_1 m_2 \cdots m_k$. La fonction*

$$\begin{aligned} \psi : \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_k\mathbb{Z} \\ n &\mapsto (\psi_1(n), \psi_2(n), \ldots, \psi_k(n)) \end{aligned}$$

est un isomorphisme d'anneaux avec $\psi_i : \mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ la projection canonique pour tout $i \in \{1, \ldots, k\}$.

Par la suite, nous utiliserons ce théorème afin de montrer l'existence de solutions à une équation modulaire en la décomposant en un système d'équations que nous pourrons traiter plus facilement.

Nous introduisons désormais une version faible du lemme d'Hensel appliquée aux équations modulaires. Afin de ne pas alourdir les notations, nous l'appellerons par la suite tout simplement le lemme d'Hensel.

Théorème 2.10 (Lemme d'Hensel)**.** *[9, proposition 4.2.3 en p.46] Soient a et n des entiers et p un nombre premier impair tel qu'il ne divise ni a ni n. Si l'équation $x^n \equiv a \mod p$ est résoluble, alors l'équation $x^n \equiv a \mod p^\alpha$ est résoluble pour tout naturel $\alpha \geq 1$. De plus, toutes ces équations admettent le même nombre de solutions.*

Nous rappelons désormais la notion de résidu quadratique et le symbole de Legendre.

Définition 2.11. *Soient a et m des entiers relativement premiers. On dit que a est un **résidu quadratique** modulo m si l'équation $x^2 \equiv a \mod m$ admet une solution entière.*

Définition 2.12. *Soient p un nombre premier impair et a un entier. Le symbole*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un résidu quadratique modulo } p\,; \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p\,; \\ 0 & \text{si } p \text{ divise } a \end{cases}$$

*est appelé le **symbole de Legendre**.*

Nous aurons besoin du théorème de réciprocité quadratique. Nous en donnons son énoncé ci-dessous.

Théorème 2.13 (Réciprocité quadratique)**.** *[9, Theorem 1 (c) en p.53] Soit p et q des nombres premiers impairs. Alors,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

La prochaine section portera sur les groupes de matrices inversibles sur l'anneau des entiers. Nous verrons que nous pourrons tracer un lien évident entre le théorème de Bézout et certaines de ces matrices.

2.3 Les groupes de matrices $\mathrm{GL}_2(\mathbb{Z})$ et $\mathrm{SL}_2(\mathbb{Z})$

Nous introduisons finalement les groupes de matrices inversibles sur l'anneau des entiers. Plus spécifiquement, nous nous concentrerons sur les matrices 2×2. Nous fixons les notations dans la définition suivante.

Définition 2.14. *Le **groupe général linéaire** d'ordre deux sur l'anneau des entiers, noté $\mathrm{GL}_2(\mathbb{Z})$, est l'ensemble des matrices 2×2 à coefficient dans l'anneau des entiers et inversibles. Cette ensemble muni du produit matriciel usuel est un groupe.*

Le déterminant d'une matrice étant multiplicatif, nous pouvons donner la caractérisation suivante des matrices de $\mathrm{GL}_2(\mathbb{Z})$.

Proposition 2.15. *Une matrice M appartient à $\mathrm{GL}_2(\mathbb{Z})$ si et seulement si elle est de la forme*

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

avec $r, s, t, u \in \mathbb{Z}$ et tels que $ru - st = \pm 1$.

Démonstration. Supposons que M appartient à $\mathrm{GL}_2(\mathbb{Z})$. Nous allons utiliser le fait que la matrice inverse M^{-1} appartient elle-aussi à $\mathrm{GL}_2(\mathbb{Z})$. Nous avons donc que

$$M^{-1} = \frac{1}{ru - st} \begin{pmatrix} u & -t \\ -s & r \end{pmatrix}$$

est une matrice à coefficients entiers. Par conséquent, nous avons que son déterminant

$$det(M^{-1}) = \frac{1}{det(M)} = \frac{1}{ru - st}.$$

est une valeur entière. On en conclut que $ru - st = \pm 1$.

Si M est de la forme

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

avec $r, s, t, u \in \mathbb{Z}$ et tels que $ru - st = \pm 1$, alors elle est inversible et sa matrice inverse

$$M^{-1} = \frac{1}{ru - st} \begin{pmatrix} u & -t \\ -s & r \end{pmatrix}$$

est elle aussi à coefficients entiers. Par conséquent, M est bien une matrice de $\mathrm{GL}_2(\mathbb{Z})$, ce qui conclut notre preuve. □

Cette caractérisation des matrices de $\mathrm{GL}_2(\mathbb{Z})$ nous permet de définir un sous-groupe. Le sous-groupe des matrices de déterminant égal à 1.

Définition 2.16. *Le **groupe spécial linéaire** d'ordre deux sur l'anneau des entiers, noté $\mathrm{SL}_2(\mathbb{Z})$, est le sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$ constitué des matrices de déterminant égal à 1.*

Remarque 2.17. Nous avons mentionné plus tôt qu'il y avait un lien entre le théorème de Bézout et les matrices de ces groupes. Ce lien est en fait lié à la construction de matrice de $\mathrm{SL}_2(\mathbb{Z})$. Si nous prenons deux entiers r et s premiers entre eux, le théorème

de Bézout assure qu'il existe des entiers t et u tels que $ru - st = 1$. Cela nous permet de construire une matrice

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

du groupe spécial linéaire $\mathrm{SL}_2(\mathbb{Z})$. Cette construction prendra une place importante dans le chapitre 3.

Nous aurons besoin de deux autres résultats concernant ces groupes de matrices. Le premier concernera l'indice du sous groupe $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathrm{GL}_2(\mathbb{Z})$ tandis que l'autre nous donnera des générateurs du groupe $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 2.18. *Le groupe* $\mathrm{SL}_2(\mathbb{Z})$ *est d'indice deux dans* $\mathrm{GL}_2(\mathbb{Z})$*, où l'indice désigne le nombre de classes latérales d'un sous groupe* H *dans un groupe* G*.*

Démonstration. Pour montrer ce résultat, nous allons considérer la matrice

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Cette matrice a la particularité d'être sa propre inverse et d'être de déterminant -1. Nous montrons que toute matrice M du groupe $\mathrm{GL}_2(\mathbb{Z})$ et de déterminant -1 est égal à un produit AN pour N une matrice de $\mathrm{SL}_2(\mathbb{Z})$. On remarque que AM est une matrice de $\mathrm{SL}_2(\mathbb{Z})$ grâce à la multiplicité du déterminant. Par conséquent, $M = A(AM)$ et nous avons montré que M est égal à un produit entre la matrice A et une matrice de $\mathrm{SL}_2(\mathbb{Z})$. On conclut que $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(Z) \sqcup A \cdot \mathrm{SL}_2(\mathbb{Z})$, où $\sqcup$ désigne l'union disjointe. Donc, $\mathrm{SL}_2(\mathbb{Z})$ est bien d'indice deux dans $\mathrm{GL}_2(\mathbb{Z})$. □

Nous donnons maintenant le résultat concernant les générateurs de $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 2.19. *Les matrices*

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad ; \quad T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

engendrent le groupe de matrices $\mathrm{SL}_2(\mathbb{Z})$*.*

Démonstration. Prenons une matrice

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

appartenant à $\mathrm{SL}_2(\mathbb{Z})$. Nous allons profiter du fait que l'anneau des entiers est euclidien 2.1. On constate que, pour un entier n, le produit $S^n M$ est égal à

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} r+nt & s+nu \\ t & u \end{pmatrix}.$$

On remarque aussi que

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} r & s \\ nr+t & ns+u \end{pmatrix}.$$

Supposons sans perte de généralité que $|r| > |t|$. Puisque $\mathbb{Z}$ est un anneau euclidien, il existe deux entiers q_1 et h_1 tels que $r = q_1 t + h_1$ et $|h_1| < |t|$. Nous déterminons le produit $S^{-q_1} M$. Celui-ci vaut

$$\begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} r-q_1 t & s-q_1 u \\ t & u \end{pmatrix} = \begin{pmatrix} h_1 & s-q_1 u \\ t & u \end{pmatrix}.$$

Nous utilisons une fois de plus le fait que $\mathbb{Z}$ est un anneau euclidien. Puisque $|h_1 < |t|$, il existe donc deux entiers q_2, h_2 tels que $t = q_2 h_1 + h_2$ et $|h_2| < |h_1|$. Nous calculons le produit $T^{-q_2} S^{-q_1} M$. Celui-ci est égal à

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ -q_2 & 1 \end{pmatrix} \begin{pmatrix} h_1 & s-q_1 u \\ t & u \end{pmatrix} &= \begin{pmatrix} h_1 & s-q_1 u \\ -q_2 h_1 + t & -q_2(s-q_1 u)+u \end{pmatrix} \\ &= \begin{pmatrix} h_1 & s-q_1 u \\ h_2 & -q_2(s-q_1 u)+u \end{pmatrix}. \end{aligned}$$

L'application successive de ces matrices est en fait l'algorithme d'Euclide. Puisque, par le lemme de Bézout 2.6, les entiers r et t sont premiers entre eux, appliquer les puissances des matrices S et T un nombre suffisant de fois nous permet d'arriver à une matrice dont l'entrée $(1,1)$ est égal à 1 tandis que l'entrée $(2,1)$ vaudra 0. Puisque le déterminant de cette matrice vaut toujours 1, l'entrée $(2,2)$ vaut elle aussi 1. Nous retrouvons une matrice de la forme

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = S^k$$

pour un entier k. En remontant la chaîne, nous montrons qu'un produit successif de puissance de matrice S et T est égal à la matrice M. Il est à noté que si $|t| \geq |r|$ dans notre matrice M, nous aurions simplement commencé l'algorithme par un produit avec une puissance de la matrice T. Par conséquent, S et T engendrent $\mathrm{SL}_2(\mathbb{Z})$. □

Ces dernières propositions seront utiles lors du chapitre 4. Cela conclut par ailleurs notre chapitre préliminaire.

Chapitre 3

Théorie arithmétique des formes quadratiques binaires

Dans ce chapitre, nous nous proposons d'étudier la théorie arithmétique des formes quadratiques binaires. Nous commencerons par rappeler les définitions des différents objets que nous utiliserons et nous préciserons le cadre dans lequel nous travaillerons. Les questions que nous tenterons de résoudre prennent place dans l'anneau des entiers.

La théorie que nous développerons servira principalement à répondre à deux questions. A l'instar de P. de Fermat, nous essaierons de déterminer quels sont les entiers pouvant être représentés par les formes quadratiques binaires. Le cas le plus connu étant de déterminer les entiers pouvant s'écrire comme la somme de deux carrés. Nous aborderons également la question du nombre de représentations d'un entier par une forme quadratique binaire. Nous tenterons de donner une réponse satisfaisante à ces deux questions pour la forme quadratique binaire

$$X^2 + XY + Y^2.$$

À l'exception de la section 3.6 qui est inspirée de la référence [10], nous avons en majorité basé notre travail sur les références [2] et [5]. La section 3.5 ainsi que la section 3.7 sont déduites de la théorie générale qui les précèdent et ne sont pas explicitement développées dans les références précédemment citées. Toutefois, une autre preuve du théorème 3.40 peut être trouvée dans l'article [7]. Nous mentionnons l'origine des résultats directement dans leur énoncé lorsque ceux-ci sont repris sans grande modifications des références utilisées.

La première partie du chapitre servira à poser les définitions nécessaires à l'énonciation rigoureuse des problèmes précédemment présentés.

3.1 Définitions préliminaires et énoncé des problèmes

Nous introduisons le sujet central notre travail.

Définition 3.1. *Une* ***forme quadratique binaire*** *est un polynôme homogène à coefficients entiers de degré 2 et à deux indéterminées.*

Une forme quadratique binaire est donc un élément de l'anneau des polynômes $\mathbb{Z}[X, Y]$. Par exemple, les polynômes $X^2 + XY + Y^2$ ou encore $X^2 + Y^2$ sont des formes quadratiques binaires. De façon tout à fait générale, une forme quadratique binaire est de la forme

$$f(X, Y) = aX^2 + bXY + cY^2$$

pour des entiers a, b et c.

Une forme quadratique binaire est donc totalement déterminée par ses coefficients. Dans la suite de ce travail, il sera parfois plus pratique de ne mentionner que les coefficients de la forme que nous utilisons. Nous emploierons donc la notation suivante.

Notation 3.2. Soit $f(X, Y) = aX^2 + bXY + cY^2$ une forme quadratique binaire. Nous posons la notation

$$f = aX^2 + bXY + cY^2 = (a, b, c).$$

Nous donnons désormais un sens précis à la notion d'entier représenté par une forme quadratique binaire. Cela correspondra simplement à la notion d'image lorsque nous évaluons une forme quadratique binaire sur un couple d'entiers.

Définition 3.3. *Soit f une forme quadratique binaire. Nous définissons* ***l'image*** *de f par*

$$\mathrm{Im}(f) = \{n \in \mathbb{Z} \mid \exists (x, y) \in \mathbb{Z}^2 \text{ tel que } f(x, y) = n\}.$$

Soient un entier n et un couple d'entiers (x, y) tels que $f(x, y) = n$, nous dirons que n est ***représenté*** *par f* ***via*** *le couple (x, y).*

Nous pouvons donc formuler précisément les deux questions présentées dans l'introduction de ce chapitre.

Problème 3.1. Soit f une forme quadratique binaire. Quels sont les entiers représentés par f ?

Résoudre ce problème reviendrait par exemple à donner une description complète de la décomposition en facteurs premiers des entiers représentés. Cette question, malgré son énoncé relativement aisé à comprendre, s'avère particulièrement ardue à résoudre en toute généralité. Nous n'apporterons une réponse satisfaisante que dans des cas bien particuliers dont nous préciserons la nature par la suite. Une description complète des entiers représentés par une forme quadratique binaire sera faite dans la section 3.5.

Au-delà de la notion de représentation simple, nous pourrions nous demander combien de fois un entier peut-être représenté. Cela nous donne le problème suivant.

Problème 3.2. Soient f une forme quadratique binaire et n un entier représenté par f. Combien existe-t-il de couples d'entiers (x, y) tels que $f(x, y) = n$?

Une fois de plus, nous verrons que répondre à cette question ne sera pas tâche aisée. Les problèmes que nous rencontrerons pour ce problème seront d'ailleurs communs à ceux du problème de représentations d'entiers.

La prochaine section portera sur les notions d'équivalences au sein des formes quadratiques binaires et sur certains types d'entiers représentés. Nous verrons que les notions d'équivalences sur les formes quadratiques binaires seront un premier pas vers la compréhension de la représentation d'entiers. De plus, ces classes combinées aux entiers dits proprement représentés nous permettront d'énoncer un critère de représentabilité fondamental pour la résolution des problèmes 3.1 et 3.2

3.2 Classes d'équivalences des formes quadratiques binaires et représentation propre d'entiers

Afin de résoudre les problèmes énoncés précédemment, nous aurons besoin de définir une action du groupe $\mathrm{GL}_2(\mathbb{Z})$, i.e. des matrices 2×2 inversibles sur l'anneau des entiers, sur les formes quadratiques binaires. Cependant, avant de définir notre action de $\mathrm{GL}_2(\mathbb{Z})$ sur les formes quadratiques binaires, nous allons donner une représentation matricielle à celles-ci. On constate aisément que, pour une forme quadratique binaire (a, b, c), l'égalité suivante est satisfaite

$$(a, b, c) = aX^2 + bXY + cY^2 = (X, Y) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

De là, nous définissons notre action.

Définition 3.4. *Soit $M \in \mathrm{GL}_2(\mathbb{Z})$. On définit* ***l'action*** *α de $\mathrm{GL}_2(\mathbb{Z})$ sur une forme quadratique binaire (a, b, c) par*

$$\alpha(aX^2 + bXY + cY^2, M) = (X, Y)M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M \begin{pmatrix} X \\ Y \end{pmatrix},$$

où M^T désigne la matrice transposée de la matrice M. On appellera la matrice

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

la ***matrice des coefficients*** *de (a, b, c).*

Nous allons montrer que l'action α est bien une action de groupe.

Proposition 3.5. *L'action α du groupe $\mathrm{GL}_2(\mathbb{Z})$ sur l'ensemble des formes quadratiques binaires est une action de groupe à droite.*

Démonstration. Soient Id la matrice 2×2 identité et (a, b, c) une forme quadratique binaire. On remarque que

$$\alpha(aX^2 + bXY + cY^2, \mathrm{Id}) = (X, Y)\mathrm{Id} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \mathrm{Id} \begin{pmatrix} X \\ Y \end{pmatrix} = aX^2 + bXY + cY^2.$$

De plus, pour M, N deux matrices de $\mathrm{GL}_2(\mathbb{Z})$, nous avons les égalités

$$\begin{aligned} \alpha(aX^2 + bXY + cY^2, MN) &= (X, Y)(MN)^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} MN \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= (X, Y)N^T M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} MN \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= \alpha(\alpha(aX^2 + bXY + cY^2, M), N). \end{aligned}$$

On conclut donc que α est bien une action de groupe à droite. □

En outre, le groupe des matrices 2×2 inversibles de déterminant égal à 1 à valeur dans les entiers $\mathrm{SL}_2(\mathbb{Z})$ agit sur les formes quadratiques binaires de façon parfaitement analogue. Ces actions nous donnent des relations d'équivalences ainsi que des classes d'équivalences.

Définition 3.6. *Deux formes quadratiques binaires sont dites* ***équivalentes*** *si elles appartiennent à la même orbite sous l'action de $\mathrm{GL}_2(\mathbb{Z})$. Nous dirons de plus que deux formes sont* ***proprement équivalentes*** *si elles appartiennent à la même orbite sous l'action de $\mathrm{SL}_2(\mathbb{Z})$.*

Les classes d'équivalences induites par l'action de $\mathrm{GL}_2(\mathbb{Z})$ seront dites des ***classes impropres*** *tandis que nous appellerons celles induites par l'action de $\mathrm{SL}_2(\mathbb{Z})$ des* ***classes propres****.*

Ces notions d'équivalence entre les formes quadratiques binaires sont primordiales. En effet, nous allons montrer que deux formes quadratiques binaires équivalentes possèdent les mêmes images.

Proposition 3.7. *Soient f, g deux formes quadratiques binaires équivalentes ou proprement équivalente. Alors,* $\mathrm{Im}(f) = \mathrm{Im}(g)$.

Démonstration. Commençons par le cas ou f et g sont équivalentes. Supposons que l'entier n soit représenté par f. Soient $M \in \mathrm{GL}_2(\mathbb{Z})$ la matrice transformant $g = (a, b, c)$ en f et (x, y) le couple d'entiers tel que $f(x, y) = n$. Alors, on remarque que

$$n = (x, y)M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M \begin{pmatrix} x \\ y \end{pmatrix}.$$

On en déduit que n est représenté par g via le couple $(x, y)M^T$. Par conséquent, nous avons que $Im(f) \subseteq Im(g)$. L'autre inclusion se fait de façon parfaitement analogue en considérant cette fois-ci la transformée de f par la matrice M^{-1}. Le cas ou f et g sont proprement équivalentes découle directement de ce cas □

Afin de donner une réponse complète au problème de représentation, il est inutile de considérer tous les nombres. Nous montrerons sous peu qu'il suffit de regarder les nombres représentés via un couple d'entiers (x, y) où x et y sont premiers entre eux. Cela nous donne la définition suivante.

Définition 3.8. *Un entier n est dit **proprement représenté** par une forme quadratique binaire f s'il est représenté par f via un couple d'entiers (x, y) tel que x et y sont premiers entre eux.*

On énonce et démontre le commentaire fait plus haut.

Lemme 3.9. *Un entier n est représenté par une forme quadratique binaire $f = (a, b, c)$ si et seulement s'il existe un couple d'entiers (x', y') avec x', y' premiers entre eux et un naturel k tels que $n = k^2 f(x', y')$.*

Démonstration. Supposons que l'entier n soit représenté par la forme quadratique binaire $f = (a, b, c)$. Alors, il existe un couple d'entier (x, y) tel que

$$n = ax^2 + bxy + cy^2.$$

En posant $k = \mathrm{pgcd}(x, y)$, on constate que les entiers $x' = x/k$ et $y' = y/k$ sont premiers entre eux et nous obtenons l'égalité recherchée

$$n = k^2(x'^2 + x'y' + y'^2) = k^2 f(x', y').$$

Réciproquement, si $n = k^2 f(x', y')$ pour un naturel k et un couple d'entiers premiers entre eux (x', y'), alors il est représenté par f via le couple (kx, ky). Cela termine notre preuve. □

Remarque 3.10. Le lemme précédent 3.9 nous assure que déterminer les entiers proprement représentés suffit pour résoudre le problème de représentation comme annoncé plus haut. Un tel exercice sera réalisé dans la section 3.5 dans la preuve du théorème

3.40. Celui-ci apportera une réponse complète au problème 3.1 dans le cas précis de la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Cette distinction entre les représentations nous permet de donner un élément de réponse à notre question de représentation.

Théorème 3.11. *[2, Lemma 2.3. en p.23] Un entier n est proprement représenté par une forme quadratique binaire (a, b, c) si et seulement s'il existe des entiers h, l tels que la forme quadratique binaire (n, h, l) est proprement équivalente à (a, b, c).*

Démonstration. Soit n un entier proprement représenté par (a, b, c) via le couple d'entiers (r, t) :

$$n = ar^2 + brt + ct^2.$$

A partir des entiers r et t, nous utilisons le théorème de Bézout 2.6 afin de déterminer des entiers s, u tels que $ru - st = 1$. De là, nous construisons la matrice

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

Par construction, M appartient à $\mathrm{SL}_2(\mathbb{Z})$ et la transformée de (a, b, c) par M est la forme quadratique binaire

$$(X, Y) \begin{pmatrix} ar^2 + brt + ct^2 & ars + \frac{1}{2}b(st + ru) + ctu \\ ars + \frac{1}{2}b(st + ru) + ctu & as^2 + bsu + cu^2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

On remarque donc que le premier coefficient de cette forme quadratique binaire est égal à n. Nous posons $h = 2ars + b(st + ru) + 2ctu$ et $l = as^2 + bsu + cu^2$ et cela nous donne la forme quadratique binaire (n, h, l). Celle-ci est bien proprement équivalente à (a, b, c) par construction.

Réciproquement, supposons qu'il existe des entiers h, l tels que (n, h, l) est une forme quadratique binaire proprement équivalente à (a, b, c). L'entier n est proprement représenté par (n, h, l) via le couple $(1, 0)$. Nous savons de plus que n est représenté par (a, b, c) via le couple $(1, 0)M^T$, où $M \in \mathrm{SL}_2(\mathbb{Z})$ est la matrice transformant (n, h, l) en (a, b, c). Plus précisément, si

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

alors n est représenté par (a, b, c) via le couple (r, t). Or, puisque $ru - st = 1$, cela nous permet de conclure via le théorème de Bézout 2.6 que r et t sont premiers entre eux. Par conséquent, n est proprement représenté par (a, b, c). □

Au vu du résultat précédent 3.11, afin de résoudre le problème 3.1, nous devons être capable de distinguer quelle forme quadratique binaire appartient à quelle classe propre.

Une telle réflexion nous guide vers l'élaboration d'un invariant de classe. Nous donnerons donc dans la prochaine section un premier invariant. Celui-ci, bien qu'élémentaire, nous permettra d'élaborer un critère de représentation par une forme quadratique binaire.

3.3 Discriminant et critère de représentation propre par une forme quadratique binaire

Nous allons désormais introduire un outil nous permettant de distinguer les classes d'équivalence entre les formes quadratiques binaires.

Définition 3.12. *Soit (a, b, c) une forme quadratique binaire. On définit le* ***discriminant*** *de (a, b, c) par la valeur*

$$d = b^2 - 4ac.$$

Une des propriétés fondamentales du discriminant est qu'il est préservé par nos notions d'équivalences.

Proposition 3.13. *Soient (a, b, c) et (a', b', c') deux formes quadratiques binaires respectivement de discriminant d et d'. Si (a, b, c) et (a', b', c') sont équivalentes ou proprement équivalentes, alors $d = d'$.*

Démonstration. Partons du cas ou (a, b, c) et (a', b', c') sont équivalentes. Cela implique qu'il existe une matrice M appartenant à $\mathrm{GL}_2(\mathbb{Z})$ telle que la transformée de (a, b, c) par M est la forme quadratique binaire (a', b', c'). On en déduit que

$$\begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} = M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M.$$

Puisque le déterminant de M et sa transposée vaut 1 ou -1, on remarque que

$$\begin{aligned} \frac{-d'}{4} = \det\left(\begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c \end{pmatrix}\right) &= \det\left(M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M\right) \\ &= \det(M)^2 \det\left(\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\right) \\ &= \det\left(\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\right) \\ &= \frac{-d}{4}. \end{aligned}$$

Dès lors, d et d' sont égaux. On constate que l'argument fonctionne aussi pour l'équivalence propre ce qui conclut notre preuve. □

Remarque 3.14. Il n'est cependant pas vrai que deux formes quadratiques binaires partageant le même discriminant sont équivalentes. Comme contre-exemple, nous pourrions prendre les deux formes quadratiques binaires $(1, 0, 6)$ et $(2, 0, 3)$. Elles sont toutes deux de discriminant -24. Cependant, elles ne partagent pas la même image puisque 1 est représenté par $(1, 0, 6)$ tandis que $(2, 0, 3)$ ne représente pas 1. Nous donnerons une analyse plus complète de ce comportement dans la prochaine section 3.4 lorsque nous déterminerons dans la proposition 3.32 l'entier non nul minimal représenté par certaines formes quadratiques binaires.

Le discriminant d'une forme quadratique binaire nous donne des informations sur les valeurs pouvant être représentées.

Proposition 3.15. *[5, Chapitre VI, section 3 en p.121] Soit (a, b, c) une forme quadratique binaire de discriminant $d < 0$. Alors, tout entier représenté par (a, b, c) possède le même signe. De plus, ce signe est le même que celui de a.*

Démonstration. Multiplions (a, b, c) par $4a$. Cela nous donne

$$4a(aX^2 + bXY + cY^2) = 4a^2X^2 + 4abXY + 4acY^2.$$

De là, nous pouvons compléter le carré avec $4a^2X^2 + 4abXY$. Nous obtenons

$$4a(aX^2 + bXY + cY^2) = (2aX + bY)^2 + (4ac - b^2)Y^2.$$

Puisque $d < 0$, on déduit que $4ac - b^2 > 0$. Par conséquent, l'évaluation de $4a(aX^2 + bXY + cY^2)$ en tout couple d'entiers est positive. Donc, l'évaluation de $aX^2 + bXY + cY^2$ en tout couple d'entiers est positive si a est positive et négative si a est négative. Cela conclut la preuve. □

Ce résultat nous conduit à la distinction suivante entre les formes quadratiques binaires.

Définition 3.16. *Une forme quadratique binaire (a, b, c) est dite **définie** si son discriminant $d < 0$. Plus précisément, une forme quadratique binaire est dite **définie positive** (resp. **négative**) si son discriminant $d < 0$ et $a > 0$ (resp. $a < 0$).*

Remarque 3.17. L'étude des formes quadratiques binaires définies peut se restreindre à celle des formes définies positives puisqu'il suffit d'inverser le signe des coefficients d'une forme définie négative afin de retrouver une forme définie positive.

Lorsque le discriminant d'une forme est positif, il n'est plus possible de donner une réponse aussi précise que dans le cas des formes quadratiques binaires définies.

Proposition 3.18. *[5, Chapitre VI, section 3 en p.121-122] Soit (a, b, c) une forme quadratique binaire de discriminant $d > 0$. Alors, l'image de (a, b, c) admet des entiers négatifs et positifs.*

Démonstration. Reprenons le début de la preuve de la proposition précédente et multiplions (a, b, c) par $4a$. Nous retrouvons

$$\begin{aligned} 4a(aX^2 + bXY + cY^2) &= 4a^2X^2 + 4abXY + 4acY^2 \\ &= (2aX + bY)^2 + (4ac - b^2)Y^2. \end{aligned}$$

Puisque le discriminant d est positif, nous pouvons factoriser l'expression. Nous obtenons l'égalité

$$4a(aX^2 + bXY + cY^2) = (2aX + bY + \sqrt{d}Y)(2aX + bY - \sqrt{d}Y).$$

Supposons pour l'instant que $a \neq 0$. Alors, nous avons

$$4a(aX^2 + bXY + cY^2) = 4a^2(X - \theta Y)(X - \varphi Y),$$

où

$$\theta = \frac{-b + \sqrt{d}}{2a} \quad ; \quad \varphi = \frac{-b - \sqrt{d}}{2a}.$$

On remarque que le produit $(X - \theta Y)(X - \varphi Y)$ est négatif s'il est évalué en un couple d'entiers (x, y) tel que $\frac{x}{y}$ appartient à l'intervalle ayant pour borne θ et φ. Tandis que si le couple (x, y) est tel que $\frac{x}{y}$ est à l'extérieur de cet intervalle, alors le produit $(X - \theta Y)(X - \varphi Y)$ évalué en ce couple sera positif. Par conséquent, l'image d'une telle forme (a, b, c) admet des entiers négatifs et positifs.

Si $a = 0$, alors la forme $(0, b, c)$ se factorise par

$$bXY + cY^2 = Y(bX + cY)$$

et on constate que l'image de $(0, b, c)$ admet des entiers positifs et négatifs. Dans tous les cas, nous avons montré que l'image d'une forme quadratique binaire de discriminant positif admet des entiers de signes négatifs et positifs, ce qui conclut la preuve. □

Cette distinction nous donne donc un autre type de forme quadratique binaire.

Définition 3.19. *Une forme quadratique binaire est dite* ***indéfinie*** *si son discriminant $d > 0$.*

La distinction entre les formes quadratiques binaires définies et indéfinies est fondamentale dans la résolution du problème de représentation 3.1. Nous verrons que le bon comportement des formes quadratiques binaires définies sera d'une aide précieuse dans nos prochaines investigations.

Avant d'énoncer notre critère de représentation d'un entier, nous allons donner des précisions sur les valeurs que peuvent prendre un discriminant. Nous aurons besoin de ce résultat basique de théorie des nombres.

Lemme 3.20. *Soit n un entier, alors $n^2 \equiv 0, 1 \mod 4$.*

Démonstration. Nous séparons la preuve en deux cas : soit n est pair ; soit n est impair. Si n est pair, il s'écrit pour un certain entier k comme $n = 2k$ et $n^2 \equiv 4k^2 \equiv 0 \mod 4$. Si n est impair, alors il s'écrit pour un certain entier k comme $n = 2k + 1$ et $n^2 \equiv 4k^2 + 4k + 1 \equiv 1 \mod 4$. □

Ce lemme nous donne le corollaire suivant sur les valeurs du discriminant.

Corollaire 3.21. *Soit (a, b, c) une forme quadratique binaire de discriminant d. Alors, $d \equiv 0, 1 \mod 4$.*

Démonstration. On constate que $d = b^2 - 4ac \equiv b^2 \mod 4$ et nous concluons par le lemme 2.19. □

Cela nous permet finalement d'énoncer notre critère de représentation d'un entier par une forme quadratique binaire.

Théorème 3.22. *[5, Chapitre VI section 4 en p.123] Soient (a, b, c) une forme quadratique binaire de discriminant d et n un entier. Si n est proprement représenté par (a, b, c), alors l'équation*

$$x^2 \equiv d \mod |4n| \tag{3.1}$$

admet une solution.

Réciproquement, soient d un entier tel que $d \equiv 0, 1 \mod 4$ et un entier n tels que l'équation (3.1) admette une solution. Alors, n est proprement représenté par une forme quadratique binaire de discriminant d.

Démonstration. Supposons dans un premier temps que l'entier n soit proprement représenté par une forme quadratique binaire (a, b, c) de discriminant d. Alors, par le théorème 3.11, il existe des entiers h, l tels que la forme quadratique binaire (n, h, l) est proprement équivalente à (a, b, c). Puisqu'elles sont proprement équivalentes, la proposition 3.13 nous assure qu'elles ont le même discriminant. Par conséquent, $h^2 - 4nl = d$. Autrement dit, $h^2 - d$ est un multiple de $4n$. Donc,

$$h^2 \equiv d \mod |4n|$$

et h est une solution de l'équation (3.1).

Supposons désormais qu'il existe un entier d tel que $d \equiv 0, 1 \mod 4$ et un entier n tels que l'équation (3.1) admette une solution. Soit h un entier solution de l'équation (3.1). Alors, on remarque que

$$h^2 \equiv d \mod |4n|.$$

Il existe donc un entier l tel que $h^2 - d = 4nl$. Nous pouvons donc construire la forme quadratique binaire (n, h, l). Celle-ci représente proprement n et elle est bien de discriminant d. Cela conclut notre preuve. □

Nous déduisons de ce théorème un corollaire concernant le cas ou il n'y aurait qu'une seule classe propre de formes quadratiques binaires pour un discriminant donné.

Corollaire 3.23. *Soit d un entier tel que $d \equiv 0, 1 \mod 4$ et tel que toutes les formes quadratiques binaires de discriminant d soient proprement équivalentes. Soit f une forme quadratique binaire de discriminant d. Un entier n est proprement représenté par f si et seulement si l'équation (3.1)*

$$x^2 \equiv d \mod |4n|$$

admet une solution.

Démonstration. Si n est un entier proprement représenté par la forme quadratique binaire f, alors le théorème 3.22 implique directement que l'équation (3.1) admet une solution.

Si maintenant, l'équation (3.1) admet une solution, la réciproque du théorème 3.22 indique que n est proprement représenté par une forme quadratique binaire de discriminant d. Or, par hypothèse, il n'y a qu'une seule classe propre associé au discriminant d. Par conséquent, puisque des formes proprement équivalentes partagent la même image par la proposition 3.7, on déduit que n est proprement représenté par f. □

Remarque 3.24. Dans le cas bien précis du corollaire précédent, nous pouvons donner une réponse complète au problème 3.1. L'idée sera de déterminer pour quels entiers n le discriminant de la forme quadratique binaire sera un résidu quadratique modulo $|4n|$. Dans les faits, nous décomposerons l'entier en ses facteurs premiers et résoudrons ces congruences modulo des nombres premiers grâce au théorème des restes chinois 2.9. Ensuite, nous utiliserons le lemme 3.9 afin de conclure. Une telle analyse sera faite sur l'exemple particulier de la forme quadratique binaire $X^2 + XY + Y^2$ dans la suite de ce chapitre en section 3.5.

Comme mentionné dans la remarque précédente, ce théorème nous permet de résoudre le problème 3.1 dans certains cas. Cependant, il n'est pas aisé de déterminer le nombre de classes d'équivalence propres qu'un déterminant peut admettre. La prochaine section mettra en exergue le bon comportement des formes quadratiques binaires définies

positives. Nous construirons un invariant de classe propre qui nous permettra de déterminer le nombre de classes d'équivalences propres associé à un déterminant négatif.

3.4 Réduction des formes quadratiques binaires primitives définies positives

Afin d'affiner notre compréhension des formes quadratiques binaires définies positives 3.16, nous allons rajouter une condition sur les formes quadratiques binaires que nous étudions. Nous définissons les formes quadratiques binaires primitives.

Définition 3.25. *Soit (a, b, c) une forme quadratique binaire. La forme quadratique binaire (a, b, c) est dite* ***primitive*** *si* $\text{pgcd}(a, b, c) = 1$*, i.e. si a, b et c sont deux à deux premiers entre eux.*

Une fois de plus, nous constatons que prendre des coefficients premiers entre eux ne nous prive d'aucune information comme le montre le lemme suivant.

Lemme 3.26. *Soit (a, b, c) une forme quadratique binaire. Il existe une forme quadratique binaire primitive (a', b', c') et un entier k tels que $(a, b, c) = k(a', b', c')$.*

Démonstration. Soit $k = \text{pgcd}(a, b, c)$. Alors, nous avons que

$$aX^2 + bXY + cY^2 = k\left(\frac{a}{k}X^2 + \frac{b}{k}XY + \frac{c}{k}Y^2\right).$$

La forme quadratique binaire $\left(\frac{a}{k}, \frac{b}{k}, \frac{c}{k}\right)$ est bien primitive et cela nous donne notre conclusion. □

Remarque 3.27. Si nous voulions étudier une forme quadratique binaire non-primitive, il suffirait donc de déterminer sa forme quadratique binaire primitive associée, de l'étudier et ensuite de multiplier chaque élément de son image par le plus grand commun diviseur des coefficients de la forme quadratique binaire d'origine.

Les résultats développés dans la sous-partie précédente s'appliquent aux formes quadratiques binaires primitives. En effet, les formes quadratiques binaires primitives sont dans des classes d'équivalences propres contenant uniquement des formes quadratiques binaires primitives.

Proposition 3.28. *Une forme quadratique binaire est primitive si et seulement si elle est proprement équivalente à une forme quadratique binaire primitive.*

Démonstration. Toute forme quadratique binaire est proprement équivalente à elle-même. On en déduit que si une forme quadratique binaire est primitive, alors elle est bien équivalente à une forme quadratique binaire primitive.

Soit maintenant (a, b, c) une forme quadratique binaire proprement équivalente à une forme quadratique binaire primitive (A, B, C). Disons que la transformée de (a, b, c) par la matrice

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

est (A, B, C). Posons $k = \mathrm{pgcd}(a, b, c)$. Nous pouvons déterminer les valeurs de A, B, C en fonction de a, b, c. Celles-ci nous sont données par

$$A = ar^2 + brt + ct^2;$$

$$B = 2ars + b(st + ru) + ctu;$$

$$C = as^2 + bsu + cu^2.$$

On constate que k divise à la fois A, B et C. Par conséquent, puisque (A, B, C) est primitive, on en conclut que $k = 1$ et (a, b, c) est bien une forme quadratique binaire primitive. □

Afin de traiter explicitement les formes quadratiques binaires primitives, une idée raisonnable serait de trouver, au sein d'une même classe d'équivalence propre, la forme quadratique binaire avec les coefficients les plus «simples» possibles. Lorsque nous traitons de classes propres de formes quadratiques binaires primitives définies positives, cette idée s'avère fructueuse et elle nous donne la définition suivante.

Définition 3.29. *Une forme quadratique binaire primitive définie positive (a, b, c) est dite **réduite** si les deux conditions suivantes sont satisfaites :*

1. $|b| \leq a \leq c$;
2. *si* $a = |b|$ *ou* $a = c$, *alors* $b > 0$.

Nous allons désormais montrer plusieurs résultats. Dans un premier temps, nous démontrerons que toute classe propre de formes quadratiques binaires primitives définies positives admet une forme quadratique binaire réduite. Ensuite, nous montrerons que cette forme quadratique binaire réduite est unique au sein de sa classe propre. Par conséquent, cela nous donnera un nouvel invariant de classe propre de formes quadratiques binaires primitives définies positives. Tous ces résultats sont inspirés du théorème 2.8. de la référence [2]. Nous avons scindé ce théorème en plusieurs partie et en avons complété la preuve au sein de nos différents résultats.

Théorème 3.30. *Toute classe propre de formes quadratiques binaires primitives définies positives admet une forme quadratique binaire réduite.*

Démonstration. Nous allons dans un premier temps montrer que toute forme quadratique binaire primitive définie positive est proprement équivalente à une forme quadratique binaire (a', b', c') telle que la première condition $|b'| \leq a' \leq c'$ est satisfaite. Parmi toutes les formes quadratiques binaires proprement équivalentes à (a, b, c), nous prenons une forme quadratique binaire (n, l, k) telle que $|l|$ soit minimal au sein de cette classe propre. Supposons par l'absurde que $n < |l|$. Alors, pour un entier s, la transformée de (n, l, k) par la matrice

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

est la forme quadratique binaire $(n, 2ns + l, k')$ avec $k' = k + ls + ns^2$. Si $l < 0$, nous pouvons prendre $s = 1$. Si $l > 0$, nous prenons $s = -1$. Dans ces deux cas, puisque $n < |l|$, on constate que $|2ns + l| < |l|$, ce qui contredit la minimalité de $|l|$. Notons que si $l = 0$, alors nécessairement $|l| \leq n$. On en déduit que dans chaque cas $|l| \leq n$. Nous pouvons raisonner de la même façon pour montrer que $|l| \leq k$. Cette fois-ci, c'est la transformée de (n, l, k) par la matrice

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

pour un entier t qui nous donne le résultat souhaité. Si $k < n$, nous constatons que la transformée de (n, l, k) par la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

est la forme quadratique binaire (k, l, n). Nous avons donc bien trouvé une forme quadratique binaire (a', b', c') satisfaisant la condition condition $|b'| \leq a' \leq c'$.

Afin de conclure, il nous suffit de montrer que la forme quadratique binaire $(a,', b', c')$ obtenue plus haut est proprement équivalente à une forme quadratique binaire réduite. On remarque que (a', b', c') est réduite sauf si $b' < 0$ et $a' = -b'$ ou $a' = c'$. Or, dans ces cas, la forme quadratique binaire $(a', -b', c')$ est réduite. Si nous sommes dans le cas $a' = -b'$, alors la transformée de $(a', b,', c')$ par la matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

est $(a', -b', c')$. Tandis que si $a' = c'$, la transformée de (a', b', c') par la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

est $(a', -b', c')$. Nous avons donc bien montré l'existence d'une forme quadratique binaire réduite dans chaque classe propre. □

Afin de démontrer l'unicité de telles formes quadratiques binaires au sein d'une même classe propre, nous aurons besoin d'un résultat sur les entiers minimaux représentés par une forme quadratique binaire primitive réduite définie positive. À cet effet, nous emploierons le lemme suivant.

Lemme 3.31. *Soit $f = (a, b, c)$ une forme quadratique binaire telle que $|b| \leq a \leq c$. Alors, pour tout entiers x, y, l'inégalité*

$$f(x, y) \geq (a - |b| + c) \min(x^2, y^2)$$

est satisfaite.

Démonstration. Nous scindons la preuve du lemme en trois parties. Supposons dans un premier temps que $|x| = |y|$. Alors, on constate que

$$\begin{aligned} f(x, y) &= ax^2 + bxy + cy^2 \\ &\geq ax^2 - |b||xy| + cx^2 \\ &\geq (a - |b| + c)x^2. \end{aligned}$$

Supposons désormais que $|x| > |y|$. Alors,

$$\begin{aligned} f(x, y) &= ax^2 + bxy + cy^2 \\ &\geq a|xy| - |b||xy| + cy^2 \\ &\geq (a - |b|)|xy| + cy^2 \\ &\geq (a - |b| + c)y^2. \end{aligned}$$

Le cas $|y| > |x|$ étant parfaitement analogue à l'étape précédente, nous pouvons conclure. □

Proposition 3.32. *Soit $f = (a, b, c)$ une forme quadratique binaire primitive définie positive réduite de discriminant $d \neq -3$. Alors,*

$$a = \min\{\mathrm{Im}(f) \setminus \{0\}\}.$$

De plus, si $a < c$, ce minimum est atteint si et seulement si f est évaluée en $(\pm 1, 0)$. Si $c = a$, il est atteint si et seulement si f est évaluée en $(\pm 1, 0)$ et $(0, \pm 1)$.

Démonstration. Puisque (a, b, c) est telle que $|b| \leq a \leq c$, le lemme 3.31 nous assure que, pour tout $x, y \in \mathbb{Z}$,

$$f(x, y) \geq (a - |b| + c) \min(x^2, y^2).$$

Si $x, y \neq 0$, nous voyons que $f(x, y) \geq a - |b| + c \geq a$. De plus, si x ou y est égal à 0, alors $f(x, y) \geq a$. Donc, l'entier minimal représenté par f est bien a.

Supposons désormais que $a < c$, nous voyons toujours que $f(x,y) \geq a - |b| + c > a$ pour $x, y \neq 0$. En outre, si $y \neq 0$, on constate que $f(0,y) \geq c > a$. Par conséquent, les seules valeurs du couple (x,y) telles que $f(x,y) = a$ sont du type $(x,0)$. On en déduit que les deux seuls couples représentant a sont $(x,y) = (\pm 1, 0)$.

Prenons le cas où $a = c$. Puisque nous avons exclu les formes quadratiques binaires de discriminant $d = -3$, on constate que $|b| \neq a$. Donc, $c - |b| > 0$ et par le même raisonnement que précédemment, nous déduisons que $f(x,y) > a$ si $x, y \neq 0$. Les valeurs minimales sont donc représentées via les couples $(\pm 1, 0)$ et $(0, \pm 1)$. □

Remarque 3.33. Ce résultat nous permet de mieux comprendre le commentaire fait dans la remarque 3.14. En effet, les formes quadratiques binaires $(1,0,6)$ et $(2,0,3)$ sont toutes deux réduites. Par conséquent, si elles étaient proprement équivalentes, elles auraient le même entier minimal représenté, i.e. elles auraient le même premier coefficient. Cela n'est évidemment pas le cas et nous concluons qu'elles n'appartiennent pas à la même classe propre. Le prochain résultat sur l'unicité des formes quadratiques binaires réduites au sein d'une même classe propre nous donnera une autre confirmation de ce fait.

Avant de commencer la preuve sur l'unicité de telles formes quadratiques binaires au sein d'une même classe propre, nous faisons remarquer au lecteur que la proposition précédente ne prend pas en compte les formes quadratiques binaires primitives de discriminant $d = -3$. Nous devrons donc traiter ce cas séparément. Nous commençons par le cas général.

Théorème 3.34. *Soient $f = (a,b,c)$ et $g = (a',b',c')$ deux formes quadratiques binaires primitives définies positives réduites de discriminant $d \neq -3$. Si f et g sont proprement équivalentes, alors $f = g$.*

Démonstration. Puisque f et g sont proprement équivalentes, alors il existe une matrice

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

telle que

$$\begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Autrement dit,

$$\begin{pmatrix} rX + sY & tX + uY \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} rX + sY \\ tX + uY \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}. \tag{3.2}$$

Supposons dans un premier temps que $a < c$. Par la proposition 3.32, nous savons que $a = a'$ puisque f et g ont la même image. De plus, nous savons que a est représenté par g via le couple $(\pm 1, 0)$. Donc, au vu de l'égalité (3.2), l'évaluation de f aux couples $(\pm r, \pm t)$ est égal à

$$f(\pm r, \pm t) = g(\pm 1, 0) = a.$$

L'entier a étant représenté par f uniquement via les couples $(\pm 1, 0)$, on en déduit que $(\pm r, \pm t) = (\pm 1, 0)$. En outre, par la condition sur le déterminant de M, on calcule que $u = \pm 1$. De là, en réécrivant la transformée de (a, b, c) par la matrice M avec ces nouvelles informations, on constate que

$$\begin{pmatrix} \pm 1 & 0 \\ s & \pm 1 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \pm 1 & s \\ 0 & \pm 1 \end{pmatrix} = \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix}.$$

Si les entrées de la matrice M sont $r = u = 1$, alors on constate que la matrice M a déjà été utilisée lors de la preuve du théorème sur l'existence d'une forme quadratique binaire primitive définie positive réduite 3.30. On constate que $b' = b \pm 2as$. Or, puisque f et g sont réduites, $s = 0$. En effet, supposons par l'absurde que $s \neq 0$. Alors, $|b - b'| = |2as| \geq |2a|$. Si $b = b'$, alors $a = 0$ ce qui est absurde puisque f et g sont définie positives. Si $b \neq b'$, alors $|b|$ ou $|b'|$ est supérieur à a. C'est aussi absurde puisque f et g sont réduites. On en déduit que $s = 0$ et cela implique que $b = b'$. Il en découle que $f = g$ puisque $a = a'$; $b = b'$; et que f et g sont de même discriminant d.

Développons désormais le cas $a = c$. De la même façon que précédemment, nous pouvons utiliser la proposition 3.32 afin de montrer que

$$f(\pm r, \pm t) = g(\pm 1, 0) = a \quad \text{ou} \quad f(\pm s, \pm u) = g(0, \pm 1) = a.$$

Dans le cas de gauche, nous pouvons simplement reprendre l'argument utilisé précédemment. Dans le cas de droite, on constate que $(\pm s, \pm u) = (0, \pm 1)$. La condition sur le discriminant nous assure une fois de plus que $r = \pm 1$. De là, Nous obtenons l'égalité suivante,

$$\begin{pmatrix} \pm 1 & t \\ 0 & \pm 1 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ t & \pm 1 \end{pmatrix} = \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix}.$$

Une fois encore, si les entrées de M sont $r = u = 1$, on observe que la matrice M fut aussi utilisée lors de la preuve du théorème 3.30. Un calcul explicite du membre de gauche nous donne

$$\begin{pmatrix} \pm 1 & t \\ 0 & \pm 1 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ t & \pm 1 \end{pmatrix} = \begin{pmatrix} a \pm bt + ct^2 & \frac{b}{2} \pm ct \\ \frac{b}{2} \pm ct & c \end{pmatrix} = \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix}.$$

On remarque que $c = c'$. De plus, nous avons par hypothèse que $a = a' = c = c'$. Or, puisque f et g sont réduites, il est clair que $b > 0$ et $b' > 0$. On en déduit que $f = g$, ce qui conclut notre preuve puisque f et g partage le même discriminant. □

Afin d'énoncer complètement le théorème d'existence et d'unicité, il nous reste à traiter le cas où le discriminant vaut -3.

Proposition 3.35. *Il n'existe qu'une unique forme quadratique binaire primitive réduite de discriminant -3. De plus, cette forme quadratique binaire réduite est la forme quadratique binaire*

$$X^2 + XY + Y^2.$$

Démonstration. Soit (a, b, c) une forme quadratique binaire primitive réduite de discriminant $d = -3$. Puisque (a, b, c) est réduite, les coefficients satisfont les inégalités $|b| \leq a \leq c$. Cela induit que

$$3 = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

On en déduit que $a = 1$. En effet, si $a = 0$, alors $b = 0$. Or, la forme quadratique binaire $(0, 0, c)$ ne peut être de discriminant -3. De plus, puisque $a = 1$, le coefficient b est nécessairement non nul. En effet, il n'existe pas de coefficient entier c tel que $3 = 4ac = 4c$. Par conséquent, $b = \pm 1$. Dans ces deux cas, on constate que $c = 1$ et, puisque (a, b, c) est réduite, le coefficient $b = 1$. L'analyse précédente nous indique donc que la forme quadratique binaire $(1, 1, 1)$ est bien l'unique forme quadratique binaire primitive réduite de discriminant -3, ce qui conclut la preuve. □

Les propositions et théorèmes précédents nous permettent donc d'énoncer et de prouver le théorème d'existence et d'unicité des formes quadratiques binaires primitives définies positives réduites au sein d'une même classe propre.

Théorème 3.36. *Toute classe propre de formes quadratiques binaires primitives définies positives admet une unique forme quadratique binaire réduite.*

Démonstration. Soit $\mathcal{C}$ une classe propre de formes quadratiques binaires primitives de discriminant différent de -3. Le théorème d'existence 3.30 nous assure dans un premier temps que $\mathcal{C}$ admet une forme quadratique binaire primitive définie positive réduite. Ensuite, le théorème 3.34 implique, puisque les formes quadratiques binaires d'une même classe propre sont proprement équivalentes par définition, que la forme quadratique binaire réduite assurée par le théorème 3.30 est bien l'unique forme quadratique binaire réduite dans $\mathcal{C}$.

Supposons désormais que $\mathcal{C}$ soit une classe propre de formes quadratiques binaires primitives de discriminant -3. Alors, le théorème d'existence 3.30 et la proposition 3.35 montre non-seulement l'existence et l'unicité d'une forme quadratique binaire réduite dans $\mathcal{C}$, mais aussi l'unicité de la classe propre $\mathcal{C}$ puisqu'il n'existe qu'une unique forme quadratique binaire réduite de discriminant -3. □

Comme mentionné à la fin de la preuve du théorème d'existence et d'unicité 3.36, nous pouvons donner un résultat plus précis concernant le nombre de classes propres de formes quadratiques binaires de discriminant -3.

Corollaire 3.37. *Il n'existe qu'une seule classe de forme quadratique binaire primitive de discriminant $d = -3$.* □

Le corollaire 3.37 nous permet de confirmer le commentaire fait dans la remarque 3.23 sur l'unicité de la classe propre de la forme quadratique binaire $(1, 1, 1)$. Nous allons procéder dans la prochaine section à l'évaluation de l'image de la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Au vu du théorème 3.22, cette section utilisera extensivement la théorie des résidus quadratiques.

3.5 Les entiers Löschiens

Nous allons désormais appliquer la théorie développée dans les dernières sections afin de déterminer les entiers représentés par la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Ces nombres furent introduit par l'économiste allemand August Lösch. Dans la suite de ce travail, et comme il est coutume de le faire, nous appellerons ces entiers des **entiers Löschiens**.

Nous allons tout d'abord déterminer quels sont les entiers proprement représentés par la forme quadratique binaire $(1, 1, 1)$. Nous rappelons que cette forme quadratique binaire est de discriminant -3. Elle est donc définie positive 3.16. Elle est aussi primitive 3.25 et le corollaire 3.37 nous assure qu'il n'existe qu'une unique classe propre de formes quadratiques binaires primitives de discriminant -3. Au vu du corollaire 3.23, nous pouvons déterminer tous les entiers proprement représentés. De plus, la remarque 3.24 nous donne la procédure à suivre.

Nous commençons par un lemme de caractérisation des nombres premiers.

Lemme 3.38. *Soit p un nombre premier différent de 2 et 3. Alors, il existe un naturel k tel que $p = 6k + 1$ ou $p = 6k - 1$.*

Démonstration. Pour montrer ce lemme, il suffit de constater que $6k + 2$; $6k + 3$; et $6k + 4$ sont respectivement divisibles par $2, 3$ et 2. Par conséquent, il ne reste plus que $6k + 1$ et $6k + 5$ comme candidats. On conclut en remarquant que $6k + 5$ est équivalent à $6(k + 1) - 1$. □

Ce lemme nous permettra de traiter les problèmes de résidus quadratiques de façon général. En effet, afin de savoir si un naturel n est un entier Löschien, il suffira d'utiliser le théorème de réciprocité quadratique 2.13 sur les premiers 2 ; 3 ; les premiers de la forme $6k+1$; et enfin les premiers de la forme $6k-1$ de la décomposition en facteurs premiers du naturel n.

Avec ces idées en tête, nous pouvons aborder le théorème de caractérisation des entiers Löschiens proprement représentés.

Théorème 3.39. *Un naturel n est proprement représenté par la forme quadratique binaire*

$$X^2 + XY + Y^2$$

si et seulement si n satisfait les conditions suivantes :

1. *n est impair ;*
2. *n n'est pas divisible par 9 ;*
3. *n n'admet pas de diviseur premier de la forme $6k-1$ pour $k \in \mathbb{N}$.*

Démonstration. Supposons dans un premier temps que le naturel n est proprement représenté par la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Grâce au théorème 3.22 et plus précisément au corollaire 3.23, nous savons que n est proprement représenté par la forme quadratique binaire $(1,1,1)$ si et seulement si l'équation modulaire (3.1) adaptée à notre cas

$$x^2 \equiv -3 \mod 4n \tag{3.3}$$

admet une solution. Soit $n = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$ la décomposition en facteur premier de n avec α_1, α_2 possiblement nuls. Par le théorème des restes chinois 2.9, résoudre l'équation (3.3) revient à résoudre le système suivant

$$\begin{cases} x^2 \equiv -3 \mod 4 \cdot 2^{\alpha_1} \\ x^2 \equiv -3 \mod 3^{\alpha_2} \\ x^2 \equiv -3 \mod p_3^{\alpha_3} \\ \quad \vdots \\ x^2 \equiv -3 \mod p_t^{\alpha_t} \end{cases}.$$

Dès lors, déterminer pour quels nombres premiers et quels puissances de ceux-ci les équations modulaires du système admettent une solution nous donnera les conditions que doit remplir n.

Nous remarquons dans un premier temps que l'équation

$$x^2 \equiv -3 \mod 8$$

n'admet pas de solution. Par conséquent, la valeur α_1 doit être égal à 0. Cela revient à dire que si n est proprement représenté par $(1,1,1)$, il est impair. Cela est notre première condition. De plus, l'équation

$$x^2 \equiv -3 \mod 4$$

admet bien des solutions. Le système peut donc bien être résolu pour des choix pertinents de nombres premiers.

Regardons désormais le cas des puissances de 3. L'équation

$$x^2 \equiv -3 \mod 3$$

admet une solution triviale. Cependant, ce n'est pas le cas de l'équation

$$x^2 \equiv -3 \mod 9$$

qui elle n'en admet pas. On en déduit que si n est proprement représenté par $(1,1,1)$, alors il n'est pas divisible par 9.

Passons aux cas des nombres premiers de la forme $6k-1$ pour $k \in \mathbb{N}$. Puisqu'ils sont relativement premiers à -3, nous pouvons utiliser la théorie des résidus quadratiques 2.11 et plus précisément les propriétés du symbole de Legendre 2.12. Nous voulons déterminer si -3 est un résidu quadratique modulo un premier de la forme $6k-1$. Via le théorème de réciprocité quadratique 2.13, nous calculons que

$$\begin{aligned}\left(\frac{-3}{6k-1}\right) = \left(\frac{-1}{6k-1}\right)\left(\frac{3}{6k-1}\right) &= (-1)^{\frac{(6k-1)-1}{2}}\left(\frac{3}{6k-1}\right) \\ &= \left(\frac{3}{6k-1}\right)^2\left(\frac{6k-1}{3}\right) \\ &= \left(\frac{6k-1}{3}\right).\end{aligned}$$

Il découle de ce calcul que -3 est un résidu quadratique d'un nombre premier de la forme $6k-1$ si et seulement si le nombre premier de la forme $6k-1$ est un résidu quadratique modulo 3. Or, l'équation

$$x^2 \equiv 6k-1 \equiv -1 \mod 3$$

est insolvable. Par conséquent, un nombre proprement représenté par $(1,1,1)$ ne peut admettre de diviseur premier de la forme $6k-1$.

Il nous reste à traiter le cas de nombres premiers de la forme $6k+1$ avec $k \in \mathbb{N}$. En utilisant le théorème de réciprocité quadratique 2.13 comme dans le cas précédent, on déduit que -3 est un résidu quadratique modulo un premier de la forme $6k+1$ si et

seulement si le premier $6k+1$ est un résidu quadratique modulo 3. Cette fois-ci, l'équation

$$x^2 \equiv 6k+1 \equiv 1 \mod 3$$

admet des solutions. Il faut désormais investiguer le cas des puissances de ces nombres premiers. Nous utilisons alors le lemme d'Hensel 2.10. Nous vérifions simplement les conditions. Les premiers de la forme $6k+1$ ne divisent ni 2 ni -3. Par la discussion précédente, l'équation

$$x^2 \equiv -3 \mod 6k+1$$

admet au moins une solution. Par conséquent, nous pouvons appliquer le lemme d'Hensel 2.10 à chaque puissance de $6k+1$ et chaque puissance de ce nombre est donc admissible dans la décomposition en facteurs premiers de l'entier n. Par conséquent, puisque nous savons par le lemme 3.38 que nous avons traité tous les nombres premiers, nous pouvons en conclure que si un naturel n est proprement représenté par $(1,1,1)$, alors n satisfait les conditions 1, 2 et 3.

Réciproquement, si n satisfait les conditions 1, 2 et 3, alors au vu des développements faits précédemment dans la preuve, l'équation (3.3)

$$x^2 \equiv -3 \mod 4n$$

admet au moins une solution. On conclut par le théorème 3.22 que n est proprement représenté par la forme quadratique binaire $(1,1,1)$, ce qui conclut notre preuve. □

Nous pouvons désormais déterminer l'image de la forme quadratique binaire

$$X^2+XY+Y^2.$$

Pour ce faire, nous emploierons le lemme 3.9. Nous rappelons que celui-ci nous indique simplement que tout nombre représenté par une forme quadratique binaire est le produit d'un nombre mis au carré et d'un entier proprement représenté. Nous verrons que les conditions de représentabilité sont différentes de celles de représentabilité propre. La preuve reviendra une fois de plus à une analyse de la décomposition en facteurs premiers des entiers représentés. Cependant, elle ne nécessitera pas l'usage de résultats d'arithmétique modulaire.

Théorème 3.40. *Soit n un naturel et soit $n = 2^{\alpha_1}3^{\alpha_2}p_2^{\alpha_3}\cdots p_t^{\alpha_t}$ sa décomposition en facteurs premiers avec α_1, α_2 possiblement nuls. Alors, n est représenté par la forme quadratique binaire*

$$X^2+XY+Y^2$$

si et seulement si n satisfait les conditions suivantes :

1. *la puissance α_1 est paire ;*
2. *toute puissance α_i associée à un facteur premier de la forme $6k-1$ pour $k \in \mathbb{N}$ est paire.*

Démonstration. Supposons que $n = 2^{\alpha_1}3^{\alpha_2}p_2^{\alpha_3}\cdots p_t^{\alpha_t}$ soit représenté par la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Alors, par le lemme 3.9, il existe deux naturels l et m tels que $n = l^2m$ avec m proprement représenté par $(1, 1, 1)$. Supposons par l'absurde que n admette dans sa décomposition en facteur premier une puissance de 2 impaire. Disons, pour fixer les idées, que $\alpha_1 = 2r + 1$ avec r un naturel. Par le théorème 3.39, nous savons que m est impair. Donc, puisque $n = l^2m$, il va de soi que si la décomposition en facteurs premiers de l vaut $l = 2^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$, alors $2r + 1 = 2\beta_1$. Cependant, cela est absurde puisque le membre de gauche est impaire et le membre de droite est quant à lui pair. Nous avons donc une contradiction. Nous en déduisons que α_1 doit être pair.

De façon tout à fait analogue, nous pouvons reprendre l'argument précédent et l'appliquer aux cas des nombres premiers de la forme $6k - 1$ pour k un naturel. Puisque m est proprement représenté par $(1, 1, 1)$, il n'est pas divisible par ces nombres premiers. Par conséquent, toute puissance associée à un nombre premier de la forme $6k - 1$ se doit d'être pair sous peine d'engendrer la même contradiction que précédemment.

Supposons désormais que n satisfait les conditions 1 et 2. Supposons en plus que l'exposant α_2 soit pair. Nous posons $k^2 = 2^{\alpha_1}3^{\alpha_2}(6k_1 - 1)^{\gamma_1}\cdots(6k_v - 1)^{\gamma_v}$, où les nombres $(6k_i - 1)$ avec $1 \leq i \leq v$ sont les facteurs premiers de la forme $6k - 1$ de n pour des naturels $k, k_1, \ldots, k_v$. Le nombre n/k^2 est bien un naturel. De plus, il est impair car sa décomposition en facteurs premiers ne contient pas de puissance de 2. Il n'est pas non plus divisible par 9 parce que sa décomposition en facteurs premiers n'admet pas non plus de puissance de 3. Et finalement, il n'admet encore une fois pas de diviseur premier de la forme $6k - 1$ puisque nous les avons tous mis dans k^2. Nous pouvons donc en déduire par le théorème 3.39 que le naturel n/k^2 est proprement représenté. Le naturel n étant trivialement égal à $n = k^2 \cdot n/k^2$, on conclut finalement par le lemme 3.9 que l'entier n est représenté par la forme quadratique binaire $(1, 1, 1)$.

Si l'on suppose désormais que α_2 est impair, on reproduit le même argument que précédemment, mais cette fois-ci nous posons $k^2 = 2^{\alpha_1}3^{\alpha_2-1}(6k_1 - 1)^{\gamma_1}\cdots(6k_v - 1)^{\gamma_v}$. Le naturel n/k^2 sera impair et sa décomposition en facteurs premier n'admettra toujours pas de premier de la forme $6k-1$. En outre, il sera divisible par 3, mais toujours pas par 9 et nous pouvons appliquer le théorème 3.39 et le lemme 3.9 afin de conclure comme dans le cas précédent. Cela conclut notre preuve. □

Nous terminons cette section en énonçant des corollaires du théorème précédent 3.40. Le corollaire suivant provient de l'article [7].

Corollaire 3.41. *[7, Corollary 4 en p.425] Le produit de deux entiers Löschiens est un entier Löschien.*

Démonstration. Pour ce faire, on utilise comme attendu le théorème 3.40. Soient $n, m \in \mathbb{N}$ deux entiers Löschiens, alors leur produit a nécessairement une puissance associée à 2 et aux nombres premiers de la forme $6k-1$ pour $k \in \mathbb{N}$ pair puisque la somme de deux nombres pairs est pair. Par conséquent, $n \cdot m$ est Löschien par les conditions du théorème 3.40. □

Puisque 1 est bien un entier Löschien, nous obtenons le corollaire suivant.

Corollaire 3.42. *L'ensemble des entiers Löschiens forme un monoïde commutatif pour la multiplication usuelle.*

Démonstration. Par le corollaire 3.41, nous avons que le multiplication usuelle induit sur l'image de la forme quadratique binaire $(1,1,1)$ une loi interne. De plus, comme mentionné plus haut, le nombre 1 nous sert de neutre et la multiplication usuelle est bien une application associative et commutative. □

Ces résultats ne tiennent plus pour des formes quadratiques binaires de discriminant admettant plusieurs classes propres. Nous donnons ci-dessous un contre-exemple.

Contre-exemple 3.43. Reprenons les formes quadratiques binaires $(1,0,6)$ et $(2,0,3)$. Ces formes quadratiques binaires sont toutes deux de discriminant -24. On remarque que

$$3 = 2 \cdot 0^2 + 3 \cdot 1^2 \quad ; \quad 11 = 2 \cdot 2^2 + 3 \cdot 1^2.$$

Cependant, l'équation

$$2x^2 + 3y^2 = 33$$

n'admet pas de solution [1] . On constate aussi que les équations

$$x^2 + 6y^2 = 3 \quad ; \quad x^2 + 6y^2 = 11$$

n'admettent pas de solution, mais

$$33 = 1 \cdot 3^2 + 6 \cdot 2^2.$$

Le discriminant -24 est un résidu quadratique modulo $4 \cdot 33$. Cependant, nous voyons bien que 33 n'est pas proprement représenté par toutes les formes quadratiques binaires de discriminant -24.

Cela conclut la section sur les entiers Löschien. Nous allons désormais nous intéresser au problème du nombre de représentations 3.2.

1. Soit nous vérifions à la main soit nous utilisons l'algorithme développé en annexe A

3.6 Le nombre de représentations propres d'un entier par une forme quadratique binaire définie positive

Nous allons désormais aborder la question énoncée au problème 3.2. Pour ce faire, nous allons pousser les conclusions que nous pouvons tirer du théorème 3.22 un peu plus loin. Reprenons une forme quadratique binaire (a, b, c) de discriminant d et n un entier proprement représenté par (a, b, c) via le couple d'entiers (r, t). Alors, le théorème 3.22 nous indique que nous pouvons trouver une solution à l'équation (3.1)

$$x^2 \equiv d \mod |4n|.$$

Chaque représentation propre de n par (a, b, c) est donc liée à au moins une solution de l'équation (3.1). De ces observations, nous donnons la définition suivante.

Définition 3.44. *Soient (a, b, c) une forme quadratique binaire de discriminant d et n un entier proprement représenté par (a, b, c) via le couple d'entiers (r, t). Soit h une solution de l'équation (3.1)*

$$x^2 \equiv d \mod |4n|.$$

*La solution h est **associée** à la représentation propre (r, t) de n si h est une solution induite du couple (r, t) par le théorème 3.22.*

Notre stratégie afin de déterminer le nombre de représentations propres de n par (a, b, c) se scinde en deux parties :

1. déterminer les solutions de l'équation (3.1) associées aux mêmes représentations propres ;
2. trouver toutes les représentations propres distinctes associées à une solution de l'équation (3.1).

Pour répondre au premier point, nous allons rappeler comment les preuves des théorèmes 3.11 et 3.22 permettent, à partir d'une représentation propre, d'obtenir une solution à l'équation (3.1).

Reprenons notre représentation propre (r, t) de l'entier n par (a, b, c). Nous utilisons le théorème de Bézout 2.6 afin de choisir des entiers s, u tels que $ru - st = 1$. Nous construisons la matrice

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

La transformée de (a, b, c) par cette matrice est la forme quadratique binaire (n, h, l), où $h = 2ars + b(st + ru) + 2ctu$ et $l = as^2 + bsu + cu^2$. La forme quadratique binaire (n, h, l) est de discriminant d puisque le discriminant est un invariant de classes propres. Donc, $h^2 - d = 4nl$ et on conclut que

$$h^2 \equiv d \mod |4n|.$$

Un élément que nous n'avions pas mentionné dans les théorèmes utilisés plus tôt est que les entiers s et u ne sont pas uniques. En effet, nous pourrions prendre les entiers $u' = u + t$ et $s' = s + r$. L'argument énoncé serait identique. Cependant, la solution à l'équation (3.1) serait $h' = h - 2n$. Nous précisons ces observations dans le lemme suivant.

Lemme 3.45. *Soit (a, b, c) une forme quadratique binaire de discriminant d. Soient n un entier proprement représenté par (a, b, c) et h, h' deux solutions distinctes de l'équation*

$$x^2 \equiv d \mod |4n|.$$

Si les solutions h et h' sont associées à la même représentation propre, alors $h = h' + 2kn$ pour k un entier.

Démonstration. Supposons que h et h' soient associées à la même représentation propre de l'entier n par (a, b, c). Plus précisément, disons que le couple d'entiers (r, t) est un couple tel que

$$n = ar^2 + brt + ct^2$$

et est associée à h et h'. Les formes quadratiques binaires (n, h, l) et (n, h', l') sont toutes deux proprement équivalentes à (a, b, c). Disons que les matrices de $\mathrm{SL}_2(\mathbb{Z})$ transformant (a, b, c) en (n, h, l) et (n, h', l') sont respectivement

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \quad ; \quad M' = \begin{pmatrix} r & s' \\ t & u' \end{pmatrix}.$$

Il est clair que $u \neq u'$ et $s \neq s'$ puisque h et h' sont des solutions distinctes. En outre, on déduit grâce à leur déterminant que

$$ru - st = ru' - s't.$$

Donc,

$$r(u - u') = t(s - s').$$

De là, puisque r et t sont premiers entre eux, r divise $s - s'$ tandis que t divise $u - u'$. Par conséquent, on obtient pour un certain entier k les égalités suivantes

$$s = s' + kr \quad ; \quad u = u' + kt.$$

Nous pouvons désormais écrire la matrice de coefficients de (n, h, l) comme

$$\begin{pmatrix} n & \frac{h}{2} \\ \frac{h}{2} & l \end{pmatrix} = \begin{pmatrix} r & t \\ s' + kr & u' + kt \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} r & s' + kr \\ t & u' + kt \end{pmatrix}.$$

Nous calculons que

$$h = 2ars' + b(ru' + s't) + 2ctu' + 2kar^2 + 2kbrt + 2kct^2 = h' + 2kn.$$

Cela prouve bien que $h = h' + 2kn$ pour k un entier. □

Avec l'aide du lemme précédent, nous déduisons la proposition suivante.

Proposition 3.46. *[10, Theorem 58. en p.74] Soient (a, b, c) une forme quadratique binaire de discriminant d et n un entier proprement représenté par (a, b, c) via le couple d'entiers (r, t). Il existe une unique solution h à l'équation (3.1)*

$$x^2 \equiv d \mod |4n|$$

associée à la représentation propre (r, t) de n par (a, b, c) telle que

$$0 \leq h < |2n|.$$

De plus, il n'existe que deux entiers s, u tels que la matrice

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

appartient à $\mathrm{SL}_2(\mathbb{Z})$ et telle que la transformée de (a, b, c) par M est la forme quadratique binaire (n, h, l), où l est l'entier tel que $d = h^2 - 4nl$.

Démonstration. Démontrons le premier point. Supposons par l'absurde qu'il existe deux solutions h, h' distinctes à l'équation (3.1) associées à la représentation propre (r, t) de n par (a, b, c) telle que

$$0 \leq h, h' < |2n|.$$

Alors, par le lemme 3.45, nous savons qu'il existe un entier k tel que $h = h' + 2kn$. Or, puisque

$$0 \leq h, h' < |2n|,$$

nous concluons que $k = 0$ et $h = h'$ ce qui est absurde.

Nous passons à la seconde assertion. L'existence des entiers s, u nous est garantie par le théorème 3.11. Démontrons l'unicité. Supposons qu'il existe des entiers s, u, s', u' tels que les matrices

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \quad ; \quad M' = \begin{pmatrix} r & s' \\ t & u' \end{pmatrix}$$

appartiennent à $\mathrm{SL}_2(\mathbb{Z})$ et la transformée de (a, b, c) par M et M' est la forme quadratique binaire (n, h, l). Lors de la preuve de la proposition 3.45, nous avons montré que, dans ce cas,

$$s = s' + kr \quad ; \quad u = u' + kt$$

pour un entier k. Par conséquent, la transformée de (a, b, c) par ces deux matrices est la forme quadratique binaire (n, h, l) uniquement si $k = 0$. On en déduit que $s = s'$ et $u = u'$, ce qui conclut notre preuve. □

Remarque 3.47. Le lemme 3.45 et la proposition 3.46 sont déterminants dans le fait qu'ils répondent au premier point de notre stratégie visant à déterminer le nombre de représentations propres d'un entier par une forme quadratique binaire. Plus précisément, la proposition 3.46 affirme que chacune des représentations propres d'un entier n par une forme quadratique binaire de discriminant d sera associée à une unique solution h de l'équation (3.1)

$$x^2 \equiv d \mod |4n|$$

telle que

$$0 \leq h < |2n|.$$

Il ne nous reste donc plus qu'à déterminer ces solutions et examiner combien de représentations propres leur sont associées.

Au vu des résultats précédents, nous pouvons entamer la deuxième étape de notre stratégie. Pour ce faire, nous allons utiliser la deuxième assertion de la proposition 3.46. Celle-ci nous donne le corollaire suivant.

Corollaire 3.48. *Soit (a, b, c) une forme quadratique binaire de discriminant d. Soit n un entier proprement représenté par (a, b, c) et soit h une solution à l'équation (3.1)*

$$x^2 \equiv d \mod |4n|$$

telle que

$$0 \leq h < |2n|.$$

Notons $R_h(n)$ l'ensemble des représentations propres de n par (a, b, c) associées à la solution h et notons $S_h(n)$ l'ensemble des matrices transformant (a, b, c) en la forme quadratique binaire (n, h, l), où l est l'entier tel que $d = h^2 - 4nl$. La fonction

$$\varphi : R_h(n) \to S_h(n), (r, t) \mapsto \begin{pmatrix} r & s \\ t & u \end{pmatrix},$$

où s et u sont les uniques entiers garantis par la seconde assertion du corollaire 3.46, est une bijection d'ensemble.

Démonstration. Par la seconde assertion de la proposition 3.46, la fonction f est bien définie puisque s et u sont déterminés de façon unique. De plus, son inverse est la fonction

$$\psi : S_h(n) \to R_h(n), \begin{pmatrix} r & s \\ t & u \end{pmatrix} \mapsto (r, t).$$

Cette fonction envoie bien une matrice de $S_h(n)$ sur une représentation propre de n par (a,b,c), car

$$\begin{aligned} n &= (1,0)\begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= (r,t)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} r \\ t \end{pmatrix} \end{aligned}$$

et les entiers r, t sont premiers entre eux par le théorème de Bézout 2.6. De plus, il est clair que ces deux fonctions sont inverses l'une de l'autre puisque

$$\psi(\varphi(r,t)) = (r,t)$$

et par l'unicité des entiers s, u

$$\varphi\left(\psi\left(\begin{pmatrix} r & s \\ t & u \end{pmatrix}\right)\right) = \begin{pmatrix} r & s \\ t & u \end{pmatrix}.$$

□

Remarque 3.49. Déterminer le nombre de représentations propres d'un entier n par une forme quadratique binaire de discriminant d associée à une solution h de l'équation (3.1)

$$x^2 \equiv d \mod |4n|$$

telle que

$$0 \leq h < |2n|$$

revient donc à déterminer le nombre de matrices de $\mathrm{SL}_2(\mathbb{Z})$ transformant (a,b,c) en la forme quadratique binaire (n,h,l), où l est l'entier tel que $d = h^2 - 4nl$.

Afin d'utiliser à son plein potentiel la bijection établie au corollaire 3.48 et la remarque précédente, nous introduisons la notion d'automorphismes d'une forme quadratique binaire.

Définition 3.50. *Soit (a,b,c) une forme quadratique binaire. Une matrice A appartenant à $\mathrm{SL}_2(\mathbb{Z})$ est un* ***automorphisme*** *de (a,b,c) si*

$$\alpha((a,b,c),A) = (a,b,c).$$

L'ensemble des automorphismes de (a,b,c) est noté $\mathrm{Aut}((a,b,c))$ et muni du produit matricielle, $\mathrm{Aut}((a,b,c))$ est un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$. L'ordre de ce groupe sera noté $|Aut((a,b,c))|$.

Nous allons montrer que l'ordre du groupe d'automorphismes de formes quadratiques binaires définies positives est fini.

Proposition 3.51. *Soit (a,b,c) une forme quadratique binaire définie positive. Le groupe d'automorphismes* $\mathrm{Aut}((a,b,c))$ *est un groupe fini.*

Démonstration. Nous cherchons toutes les matrices $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$ satisfaisant l'équation

$$\begin{pmatrix} w & y \\ x & z \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Résoudre cette équation revient à résoudre dans les entiers le système suivant,

$$\begin{cases} aw^2 + bwy + cy^2 = a \\ 2awx + bwz + bxy + 2cyz = b \\ ax^2 + bxz + cz^2 = c \\ wz - yx = 1. \end{cases}$$

Afin de montrer que ce système n'admet qu'un nombre fini de solutions, nous allons nous contenter de regarder la première et la troisième équation. Ces équations sont celles de coniques. Nous allons procéder à la réduction de celles-ci pour déterminer quels types de coniques elles représentent.

Commençons par la première. Puisque la forme quadratique binaire (a,b,c) est définie positive, cela nous garantit que le déterminant de la matrice $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ est positif. On constate que les valeurs propres de cette matrice sont réelles. En effet, un calcul rapide montre que le polynôme caractéristique de la matrice $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ est égal à

$$\det \begin{pmatrix} a - X & \frac{b}{2} \\ \frac{b}{2} & c - X \end{pmatrix} = X^2 - (a+c)X + ac - \frac{b^2}{4}.$$

Le discriminant du polynôme caractéristique vaut

$$\begin{aligned} \Delta = (-(a+c))^2 + b^2 - 4ac &= a^2 + 2ac + c^2 + b^2 - 4ac \\ &= a^2 - 2ac + c^2 + b^2 \\ &= (a-c)^2 + b^2. \end{aligned}$$

On constate que le discriminant du polynôme caractéristique est positif. Par conséquent, les valeurs propres de la matrice $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ sont bien réelles. En outre, puisque le produit des valeurs propres est égal au discriminant, elles sont soit toutes deux positives soit toutes deux négatives. Notons les valeurs propres de cette matrice λ_1 et λ_2. Ces valeurs propres sont égales si et seulement si $a = c$ et $b = 0$. Dans ce cas, la matrice est déjà diagonale. Dans le cas contraire, les valeurs propres sont distinctes et en conséquence,

la matrice $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ est diagonalisable. Soit P la matrice de vecteurs propres tels que

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = P \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} P^{-1}.$$

La conique $aw^2 + bwy + cy^2 = a$ se réduit donc à

$$\lambda_1 u^2 + \lambda_2 v^2 = a,$$

où u et v sont tels que $P(w, y)^T = (u, v)^T$. Or, l'équation $aw^2 + bwy + cy^2 = a$ admet au moins une solution : $w = 1, y = 0$. Par conséquent, il en va de même pour l'équation $\lambda_1 u^2 + \lambda_2 v^2 = a$. C'est le cas uniquement lorsque λ_1 et λ_2 sont positives, car a est positif par définition. On en déduit que la conique $aw^2 + bwy + cy^2 = a$ est une ellipse. Elle est donc bornée et ne peut intersecter qu'un nombre fini de fois $\mathbb{Z}^2$. La première équation n'admet donc qu'un nombre fini de solutions.

Il nous reste à vérifier que la troisième équation n'admet elle aussi qu'un nombre fini de solutions. En suivant le même procédé que pour la première équation, nous réduisons cette conique et obtenons une équation du type

$$\lambda_1 s^2 + \lambda_2 t^2 = c$$

pour s, t des variables judicieusement choisies. Puisque la forme quadratique binaire (a, b, c) est définie positive et le coefficient c appartient à son image, on déduit que c est positif par la proposition 3.15. Donc, la conique $ax^2 + bxy + cz^2 = c$ est bien une ellipse et de façon tout à fait analogue au traitement fait pour la première équation, nous concluons que le nombre de solutions dans les entiers de la troisième équation est fini. Par conséquent, il n'y a qu'un nombre fini d'entiers w, x, y, z satisfaisant la première équation et la troisième. Donc, le nombre de matrices $\begin{pmatrix} w & y \\ x & z \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$ satisfaisant l'équation

$$\begin{pmatrix} w & y \\ x & z \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

est fini concluant notre preuve. □

La notion d'automorphisme de formes quadratiques binaires et le corollaire 3.48 nous permettent d'énoncer le critère suivant sur le nombre de représentations propres.

Théorème 3.52. *[10, Theorem 59. en p.75] Soit (a, b, c) une forme quadratique binaire définie positive de discriminant d telle que $w = |Aut((a, b, c))|$. Soient n un entier proprement représenté par (a, b, c) et h une solution de l'équation (3.1)*

$$x^2 \equiv d \mod |4n|.$$

On pose la forme quadratique binaire (n, h, l) avec l l'entier tel que $d = h^2 - 4nl$. Le nombre de représentations propres associées à h est égal à :

- *0 si (a, b, c) et (n, h, l) ne sont pas proprement équivalentes ;*
- *w si (a, b, c) et (n, h, l) sont proprement équivalentes.*

Démonstration. Le premier cas est trivial par le corollaire 3.48.

Nous passons désormais au second cas. Supposons que (n, h, l) soit une forme quadratique binaire proprement équivalente à (a, b, c). Alors, il existe une matrice M appartenant à $\mathrm{SL}_2(\mathbb{Z})$ transformant (a, b, c) en (n, h, l). Considérons un automorphisme A de (a, b, c). Il est clair que la matrice AM transforme la forme quadratique binaire (a, b, c) en (n, h, l). Réciproquement, si N est une autre matrice de $\mathrm{SL}_2(\mathbb{Z})$, alors la matrice NM^{-1} est un automorphisme de (a, b, c). Par conséquent, pour un certain automorphisme T de (a, b, c), $N = TM$. Ces observations nous permettent de construire une bijection. Nous posons la fonction

$$\varphi : \mathrm{Aut}((a, b, c)) \to S_h(n), A \mapsto AM,$$

où $S_h(n)$ est l'ensemble des matrices dont transformant (a, b, c) en (n, h, l). On définit désormais la fonction

$$\psi : S_h(n) \to \mathrm{Aut}((a, b, c)), N \mapsto NM^{-1}.$$

Il est clair que les fonctions φ et ψ sont inverses l'une de l'autre. Elles sont donc des bijections. Par conséquent, le corollaire 3.48 nous permet de déduire que le nombre de représentations propres associées à h vaut w. □

Une fois de plus, dans les cas ou le discriminant n'admet qu'une classe propre de formes quadratiques binaires, nous pouvons totalement résoudre le problème du nombre de représentations propres.

Corollaire 3.53. *Soit d un entier négatif tel que $d \equiv 0, 1 \mod |4n|$ et tel que toutes les formes quadratiques binaires de discriminant d soient proprement équivalentes. Soit (a, b, c) une forme quadratique binaire définie positive de discriminant d et telle que $w = |\mathrm{Aut}((a, b, c))|$. Soit n un entier proprement représenté par la forme quadratique binaire (a, b, c). Notons S le nombre de solutions h admises par l'équation (3.1)*

$$x^2 \equiv d \mod |4n|$$

telles que

$$0 \leq h < |2n|.$$

Alors, le nombre de représentations propres de n par (a, b, c) est égal à $w \cdot S$.

Démonstration. Par le théorème 3.52, nous savons que le nombre de représentation associé à une solution h de l'équation est égal à w. De plus, puisque d n'admet qu'une seule classe propre de formes quadratiques binaires, chaque solution h à l'équation

$$x^2 \equiv d \mod |4n|$$

induit w solutions. Par le lemme 3.45, si nous rajoutons la condition

$$0 \leq h < |2n|,$$

toutes les solutions h sont associées à des représentations distinctes. Par conséquent, le nombre de représentations propres de n par (a, b, c) est bien égal à $w \cdot S$. □

Nous donnons dans la prochaine section un exemple sur les entiers Löschiens proprement représentés.

3.7 Le nombre de représentations propres d'un entier Löschien

Nous allons désormais déterminer le nombre de représentations propres des entiers Löschiens. Nous rappelons que les entiers Löschiens sont les entiers représentés par la forme quadratique binaire

$$X^2 + XY + Y^2.$$

Cette forme quadratique binaire est de discriminant -3 et nous avons montré dans la proposition 3.35 qu'elle est l'unique forme quadratique binaire réduite de discriminant -3. Cela implique, entre autres par le corollaire 3.53, que nous pouvons déterminer le nombre de représentations propres des entiers Löschiens. Nous allons donc devoir déterminer le nombre d'automorphismes de cette forme quadratique binaire. À cet effet, nous aurons besoin du lemme suivant.

Lemme 3.54. *[9, Proposition 9.1.1 en p.109] L'entier* 1 *admet six représentations par la forme quadratique binaire*

$$X^2 + XY + Y^2.$$

Celles-ci sont données par les couples d'entiers $(\pm 1, 0)$ *;* $(0, \pm 1)$ *; et* $(\pm 1, \mp 1)$.

Démonstration. Nous cherchons tous les couples d'entiers (x, y) tels que

$$x^2 + xy + y^2 = 1.$$

En multipliant les deux membres par quatre, on remarque que cette équation est équivalente à

$$(2x + y)^2 + 3y^2 = 4.$$

Les couples d'entiers positifs dont la somme vaut quatre sont les suivants : $(4,0)$; $(0,4)$; $(1,3)$; $(3,1)$; et $(2,2)$. Les équations

$$(2x+y)^2 = 3 \quad ; \quad 3y^2 = 2 \quad ; \quad 3y^2 = 4$$

n'admettent pas de solution dans les entiers. On en déduit que seuls les couples $(4,0)$; et $(1,3)$ peuvent induire des solutions. Dans le cas où $(2x+y)^2 = 4$ et $3y^2 = 0$, il faut nécessairement que $y = 0$. Donc, $2x^2 = 4$ et on déduit que x est soit égal à 1 soit à -1. Cela nous donne les couples $(\pm 1, 0)$. Dans le cas $(1,3)$, y peut prendre les valeurs 1 ou -1. Si $y = 1$, alors l'équation $(2x+1)^2 = 1$ est satisfaite si x est nul ou bien si x est égal à -1. Cela nous donne les couples $(0,1)$ et $(-1,1)$. Si y vaut -1, alors l'équation $(2x-1)^2 = 1$ est satisfaite si $x = 1$ ou si $x = 0$. Cela nous donne les couples $(1,-1)$ et $(0,-1)$, concluant notre preuve. □

Nous donnons désormais une description du groupe d'automorphismes de la forme quadratique binaire $(1,1,1)$.

Proposition 3.55. *Il y a exactement six automorphismes de la forme quadratique binaire*

$$X^2 + XY + Y^2.$$

En outre, le groupe $\mathrm{Aut}((1,1,1))$ *est isomorphe au groupe cyclique* $\mathbb{Z}/6\mathbb{Z}$.

Démonstration. Nous commençons par montrer que l'ordre du groupe $\mathrm{Aut}((1,1,1))$ est égal à six. Pour ce faire, nous explicitons la définition d'automorphismes dans notre cas. Nous cherchons les matrices $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ appartenant à $\mathrm{SL}_2(\mathbb{Z})$ tels que

$$\begin{pmatrix} w & y \\ x & z \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}.$$

Autrement dit, nous voulons résoudre dans les entiers le système d'équations suivant,

$$\begin{cases} w^2 + wy + y^2 = 1 \\ 2wx + wz + xy + 2yz = 1 \\ x^2 + xz + z^2 = 1 \\ wz - yx = 1. \end{cases} \tag{3.4}$$

On remarque que la première ainsi que la troisième équation du système sont de la même forme que celle traitée dans le lemme 3.54. Elles admettent donc toutes deux les six mêmes solutions. Nous avons donc trente-six potentielles solutions à tester pour notre système. Le tableau 3.1 ci-dessous indique quelles paires de couples nous donnent une solution au système d'équation (3.4). Lorsqu'une case est marquée du symbole ✓, cela indique que les entiers w, x, y, z sont des solutions du système d'équation (3.4). Lorsque

la case est marqué par $\times$, cela indique que les entiers des deux couples ne forment quant à eux pas une solution du système d'équation (3.4).

TABLE 3.1 – Solutions du système d'équations (3.4)

(w,y) \ (x,z)	$(1,0)$	$(-1,0)$	$(0,1)$	$(0,-1)$	$(1,-1)$	$(-1,1)$
$(1,0)$	$\times$	$\times$	✓	$\times$	$\times$	$\times$
$(-1,0)$	$\times$	$\times$	$\times$	✓	$\times$	$\times$
$(0,1)$	$\times$	$\times$	$\times$	$\times$	$\times$	✓
$(0,-1)$	$\times$	$\times$	$\times$	$\times$	✓	$\times$
$(1,-1)$	✓	$\times$	$\times$	$\times$	$\times$	$\times$
$(-1,1)$	$\times$	✓	$\times$	$\times$	$\times$	$\times$

Nous constatons qu'il n'y a que six solutions au système d'équation (3.4). Par conséquent, l'ordre du groupe $\mathrm{Aut}((1,1,1))$ vaut bien six. Afin de montrer que le groupe d'automorphismes de la forme $(1,1,1)$ est bien isomorphe à $\mathbb{Z}/6\mathbb{Z}$, nous allons montrer que $\mathrm{Aut}((1,1,1))$ admet un élément d'ordre six. Ainsi, $\mathrm{Aut}((1,1,1))$ sera cyclique et donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Cet élément est la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

En effet, nous calculons que

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad ; \quad \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Cet élément est donc bien d'ordre six ce qui conclut notre preuve. □

Afin de déterminer le nombre de représentations d'un entier Löschien proprement représenté, nous aurons besoin de la proposition suivante ainsi que de son corollaire.

Proposition 3.56. *Soient d et n des entiers. L'entier h est une solution de l'équation*

$$x^2 \equiv d \mod |4n|$$

si et seulement si $h + |2n|$ est aussi une solution.

Démonstration. Supposons que l'entier h soit une solution, alors

$$\begin{aligned}(h+|2n|)^2 &\equiv h^2 + |4n|h + |4n||n| \mod |4n| \\ &\equiv h^2 \mod |4n| \\ &\equiv d \mod |4n|.\end{aligned}$$

L'entier $h + |2n|$ est donc bien une solution.

Supposons désormais que $h + |2n|$ soit une solution. Alors,

$$\begin{aligned}(h + |2n|)^2 &\equiv h^2 + |4n|h + |4n||n| \mod |4n| \\ &\equiv h^2 \mod |4n|.\end{aligned}$$

Puisque $(h+|2n|)^2 \equiv d \mod |4n|$, on déduit que $h^2 \equiv d \mod |4n|$ comme recherché. □

Cette proposition nous permet de donner le corollaire suivant.

Corollaire 3.57. *Soit d et n des entiers. Le nombre de solutions h à l'équation*

$$x^2 \equiv d \mod |4n|$$

telles que

$$0 \leq h < |2n|$$

est égal à la moitié des solutions de l'équation

$$x^2 \equiv d \mod |4n|.$$

Démonstration. Par la proposition 3.56, nous savons que h est une solution de l'équation

$$x^2 \equiv d \mod |4n|$$

si et seulement si l'entier $h + |2n|$ est lui-même une solution. Par conséquent, l'ensemble $\{0, 1, \ldots, |2n| - 1\}$ possède le même nombre de solutions que l'ensemble $\{|2n|, |2n| + 1, \ldots, |4n| - 1\}$. Il en découle que le nombre total de solutions vaut deux fois le nombre de solutions appartenant à l'ensemble $\{0, 1, \ldots, |2n|-1\}$, ce qui conclut notre preuve. □

Nous sommes désormais en mesure d'énoncer et de prouver le théorème sur le nombre de représentations d'un entier Löschien proprement représenté.

Théorème 3.58. *Soit n un entier proprement représenté par la forme quadratique binaire*

$$X^2 + XY + Y^2.$$

L'entier n admet $6 \cdot 2^s$ représentations propres distinctes par $(1, 1, 1)$, où s est égal au nombre de facteurs premiers de n de la forme $6k + 1$, avec $k \in \mathbb{N}$.

Démonstration. Pour démontrer ce théorème, nous allons utiliser le critère développé au théorème 3.52. Puisque, par le corollaire 3.37, il n'existe qu'une seule classe propre

associée au discriminant -3, la remarque 3.53 ainsi que la remarque 3.49 nous assure qu'il suffit de déterminer le nombre de solutions h de l'équation

$$x^2 \equiv -3 \mod 4n$$

telles que

$$0 \leq h < 2n.$$

Plutôt que de ne considérer que les solutions h telles que $0 \leq h < 2n$, le corollaire 3.57 nous indique que nous pouvons simplement compter le nombre de solutions de l'équation

$$x^2 \equiv -3 \mod |4n|$$

et diviser ce nombre par deux. Ensuite, il faut multiplier ce nombre par $w = |Aut((1,1,1))|$. La proposition 3.55 nous indique que $w = 6$.

Par le théorème des restes chinois 2.9, le nombre de solution à l'équation

$$x^2 \equiv -3 \mod 4n$$

est égal au nombre de solutions du système

$$\begin{cases} x^2 \equiv -3 \mod 4 \cdot 2^{\alpha_1} \\ x^2 \equiv -3 \mod 3^{\alpha_2} \\ x^2 \equiv -3 \mod p_3^{\alpha_3} \\ \quad \vdots \\ x^2 \equiv -3 \mod p_t^{\alpha_t} \end{cases},$$

où $n = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$ est la factorisation en nombres premiers de n avec α_1, α_2 potentiellement nuls. L'entier n étant proprement représenté par $(1,1,1)$, le théorème 3.5 nous indique que α_1 est nul et, hormis le nombre premier 3, tous les facteurs premiers de n sont de la forme $6k+1$ pour $k \in \mathbb{N}$. On remarque tout d'abord qu'avec ces nouvelles conditions, la première équation du système admet toujours deux solutions : $x = 1$ et $x = 3$. Pour tout premier de la forme $6k+1$, la réciprocité quadratique 2.13 nous assure l'équation

$$x^2 \equiv -3 \mod 6k+1$$

admet une solution si et seulement si

$$x^2 \equiv 6k+1 \equiv 1 \mod 3.$$

admet une solution (voir théorème 3.39). Par conséquent, puisque l'équation précédente admet une solution quand $x = 1$, le polynôme

$$X^2 + 3$$

admet au moins une racine non nulle dans le corps $\mathbb{Z}/(6k+1)\mathbb{Z}$. Disons que h est une racine. Alors, $-h$ est aussi une racine du polynôme. De plus, $6k+1$ étant premier et impair, $h \not\equiv -h \mod 6k+1$. Puisqu'un polynôme du second degré admet au plus deux racines dans un corps, on déduit que pour tout facteur premier de la forme $6k+1$, l'équation

$$x^2 \equiv -3 \mod 6k+1$$

admet deux solutions. De plus, le lemme d'Hensel 2.10 garantit que le nombre de solutions de l'équation

$$x^2 \equiv -3 \mod p_i^{\alpha_i}$$

est égal au nombre de solutions de l'équation

$$x^2 \equiv -3 \mod p_i,$$

pour $p_i^{\alpha_i}$ un facteur premier de n. De plus, l'équation

$$x^2 \equiv -3 \equiv 0 \mod 3$$

n'admet qu'une solution. On en déduit donc que le nombre de solutions du système vaut 2^{s+1}, où s est le nombre de facteurs premiers de la forme $6k+1$ de n. Par conséquent, l'équation

$$x^2 \equiv -3 \mod 2n$$

admet 2^{s+1} solutions. Nous multiplions ce résultat par six et le divisons par deux comme mentionné plus haut. On conclut que n admet $6 \cdot 2^s$ représentations propres. □

Nous donnons ci-dessous un exemple apparaissant dans l'article [12] traitant de la géométrie d'une certaine classe de polyèdres.

Exemple 3.59. Nous allons déterminer le nombre de représentations propres de l'entier 8281. La décomposition en facteurs premiers de ce nombre est $8281 = 7^2 13^2$. Les premiers 7 et 13 étant de la forme $6k+1$ pour $k \in \mathbb{N}$, nous déterminons par le théorème 3.58 que 8281 admet $6 \cdot 2^2 = 24$ représentations propres. L'auteur de l'article [12], M. Goldberg, fut amener à considérer les différentes représentations propres de 8281 dans l'optique de déterminer le nombre de polyèdres dits multi-symétriques composés de 8281 faces hexagonales. Il donne dans son article cinq configurations possibles de tels polyèdres.

Chapitre 4

Les topographes de Conway

Nous allons désormais envisager un autre point de vue afin d'étudier les formes quadratiques binaires. Nous allons introduire les topographes de Conway. Conçus par le mathématicien britannique John H. Conway, les topographes de Conway donnent une théorie visuelle de la théorie des formes quadratiques binaires.

Dans ce chapitre, nous tâcherons d'établir le lien entre la théorie arithmétique développée au chapitre précédent et cette théorie beaucoup plus visuelle dans le but de faire transparaître concrètement les similitudes et les différences de ces deux approches. Certaines notions déjà exposées seront d'ailleurs réintroduites dans un nouveau cadre. Le concept même de forme quadratique binaire sera reformulé de manière à mieux s'ajuster à nos différentes considérations.

L'approche des topographes de Conway se veut en son essence algorithmique comme en témoigne le résultat final 1.4 du chapitre les introduisant dans le livre *The sensual quadratic form* de J. H. Conway. Celui-ci énonce que pour tout entier et toute forme quadratique binaire, il existe un procédé algorithmique permettant de déterminer si ce nombre est représenté par la forme quadratique binaire ou non. Nous proposons dans l'annexe A un algorithme répondant à cette question dans certains cas.

Pour réaliser ce chapitre, nous nous basons sur le premier chapitre de la référence [6] ainsi que sur le dixième et onzième chapitre de la référence [11]. Nous référençons dans les énoncés la provenance des résultats que nous exposons lorsque ceux-ci ne sont pas grandement modifiés.

4.1 Réseaux et topographe d'un réseau

Nous commençons cette section par définir la notion de réseaux.

Définition 4.1. *[8, 1.2 Basis and sublattices en p.9] Soient $e_1, \ldots, e_n \in \mathbb{R}^n$ des vecteurs linéairement indépendants. L'ensemble des points Λ de la forme*

$$r = u_1 e_1 + \ldots + u_n e_n$$

avec $u_1, \ldots, u_n$ des entiers est appelé un ***réseau*** *pour la* ***base*** *$\{e_1, \ldots, e_n\}$. On définit la* ***dimension*** *d'un réseau par le nombre d'éléments dans la base.*

On remarque qu'un même réseau peut être généré par plusieurs bases.

Proposition 4.2. *Soit Λ un réseau pour la base $\{e_1, \ldots, e_n\}$. Soient $e'_1, \ldots, e'_n \in \mathbb{R}^n$ des vecteurs linéairement indépendants. Les vecteurs $e'_1, \ldots, e'_n$ génèrent Λ si et seulement s'il existe une matrice M appartenant à $\mathrm{GL}_n(\mathbb{Z})$ telle que*

$$(e_1, \ldots, e_n) = (e'_1, \ldots, e'_n)M.$$

Démonstration. Supposons que les vecteurs $e'_1, \ldots, e'_n$ génèrent Λ. Alors, ils génèrent tous les vecteurs $e_1, \ldots, e_n$. Par conséquent, il existe des coefficients entiers $(v_{ij})_{1 \leq i,j \leq n}$ tels que

$$\begin{cases} e_1 = v_{11}e'_1 + v_{12}e'_2 + \ldots + v_{1n}e'_n \\ e_2 = v_{21}e'_1 + v_{22}e'_2 + \ldots + v_{2n}e'_n \\ \quad \vdots \\ e_n = v_{n1}e'_1 + v_{n2}e'_2 + \ldots + v_{nn}e'_n. \end{cases}$$

Ainsi, nous définissons la matrice $M = (v_{ij})_{1 \leq i,j \leq n}$. Nous allons désormais montrer que $\det(M) = \pm 1$. Puisque $\{e_1, \ldots, e_n\}$ est une base du réseau Λ, il existe une matrice W à coefficients entiers telle que

$$(e'_1, \ldots, e'_n) = (e_1, \ldots, e_n)W.$$

Par conséquent, on constate que

$$(e_1, \ldots, e_n) = (e_1, \ldots, e_n)WM.$$

On en déduit que

$$(e_1, \ldots, e_n)(I - WM) = 0,$$

où I est la matrice identité. Puisque les vecteurs $e_1, \ldots, e_n$ sont linéairement indépendants, le déterminant de la matrice $(e_1, \ldots, e_n)$ est non-nul. Par conséquent, $I = WM$. Donc,

$$1 = \det(WM) = \det(W)\det(M).$$

Le déterminant de ces matrices est un nombre entier. Par conséquent, $\det(M) = 1$ ou $\det(M) = -1$. La matrice M appartient donc bien à $\mathrm{GL}_n(\mathbb{Z})$.

Supposons qu'il existe une matrice $M = (v_{ij})_{1 \leq i,j \leq n}$ appartenant à $\mathrm{GL}_n(\mathbb{Z})$ telle que

$$(e_1, \ldots, e_n) = (e'_1, \ldots, e'_n)M.$$

Nous voulons montrer que tout élément r du réseau Λ est égal à une combinaison linéaire des vecteurs $e'_1, \ldots, e'_n$. Comme $\{e_1, \ldots, e_n\}$ est une base de Λ, il existe des entiers $u_1, \ldots, u_n$ tels que

$$r = u_1 e_1 + \ldots + u_n e_n.$$

Alors, nous pouvons écrire r sous forme de combinaison linéaire des vecteurs $e'_1, \ldots, e'_n$. En effet, nous voyons que

$$r = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} u_i v_{ij} \right) e'_j.$$

Puisque $u_1, \ldots, u_n$ sont des entiers et qu'il en va de même pour les entrées v_{ij} de la matrice M, nous déduisons que $\sum_{i=1}^{n} u_i v_{ij}$ est un entier pour tout $i, j \in \{1, \ldots, n\}$. Nous avons donc montrer que les vecteurs $e'_1, \ldots, e'_n$ génèrent le réseau Λ. □

Nous introduisons désormais la notion de vecteurs relâchés. Par la suite, cette définition rendra compte du fait que les formes quadratiques binaires ne différencient pas le signe des vecteurs sur lesquelles on les évalue.

Définition 4.3. *Soit Λ un réseau pour la base $\{e_1, e_2\}$. Soit r un vecteur de Λ, nous appellerons le couple $\pm r$ un* ***vecteur relâché****.*

La définition précédente nous permet de définir les notions de bases strictes et relâchées et de bien faire la distinction avec une base dans le sens usuel.

Définition 4.4. *Soient Λ un réseau et $\{e_1, e_2\}$ une base du réseau Λ. Nous appellerons la paire ordonnée (e_1, e_2) une* ***base stricte*** *tandis que l'ensemble de cardinal quatre $\{\pm e_1, \pm e_2\}$ formé des vecteurs relâchés de la base stricte sera appelée une* ***base relâchée****.*

Nous introduisons la notion de super-bases ainsi que de super-bases relâchées.

Définition 4.5. *Soit Λ un réseau de dimension deux. Une* ***super-base stricte*** *du réseau Λ est un triplet de vecteurs ordonnés (e_1, e_2, e_3) appartenant à $\mathbb{R}^2$ tel que*

1. *$e_1 + e_2 + e_3 = 0$;*
2. *(e_1, e_2) est une base stricte du réseau Λ.*

Soit (e_1, e_2, e_3) une super-base du réseau Λ. L'ensemble $\{\pm e_1, \pm e_2, \pm e_3\}$ est appelé une ***super-base relâchée****.*

Afin de construire les topographes, nous allons montrer le lien qu'il existe entre les bases et les super-bases.

Proposition 4.6. *Soit Λ un réseau de dimension deux. Toute super-base relâchée $\{\pm e_1, \pm e_2, \pm e_3\}$ de Λ contient exactement trois bases relâchées distinctes de Λ et celles-ci sont*

$$\{\pm e_1, \pm e_2\} \quad ; \quad \{\pm e_1, \pm e_3\} \quad ; \quad \{\pm e_2, \pm e_3\}.$$

Toute base relâchée $\{\pm e_1, \pm e_2\}$ de Λ est contenue dans exactement deux super-bases relâchées distinctes de Λ et celles-ci sont

$$\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\} \qquad ; \qquad \{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}.$$

Démonstration. Nous commençons par la première assertion. Il est clair que les seules candidats pour être des bases relâchées dans les sous-ensembles de $\{\pm e_1, \pm e_2, \pm e_3\}$ sont les ensembles

$$\{\pm e_1, \pm e_2\} \quad ; \quad \{\pm e_1, \pm e_3\} \quad ; \quad \{\pm e_2, \pm e_3\}.$$

Il faut donc montrer que chacun de ces ensembles est une base relâchée. Par définition, L'ensemble $\{\pm e_1, \pm e_2\}$ est une base relâchée puisque (e_1, e_2) est une base stricte. De plus, nous savons que

$$e_1 + e_2 + e_3 = 0.$$

Par conséquent, $e_2 = -e_1 - e_3$ et est donc combinaison linéaire de e_1 et e_3. On déduit donc que le couple ordonné (e_1, e_3) est une base stricte et il en découle que $\{\pm e_1, \pm e_3\}$ est une base relâchée. Le cas $\{\pm e_2, \pm e_3\}$ est parfaitement analogue. Nous notons que toutes ces bases relâchées sont différentes. En effet, prenons par exemple le cas où $\{\pm e_1, \pm e_2\} = \{\pm e_1, \pm e_3\}$. Alors, soit $e_2 = e_3$ ou bien $e_2 = -e_3$, dans les deux cas, nous avons une contradiction puisque cela implique que $e_1 = 2e_2$ ou que $e_1 = 0$. Puisque (e_1, e_2) est une base stricte, cela est impossible. Des arguments analogues montrent que les bases relâchées annoncées sont bien toutes distinctes.

Prenons désormais $\{\pm e_1, \pm e_2\}$ une base relâchée du réseau Λ. Nous pouvons associer quatre bases strictes à cette base relâchée : (e_1, e_2) ; $(-e_1, e_2)$; $(e_1, -e_2)$; $(-e_1, -e_2)$. Dès lors, pour former une super-base stricte à partir des bases strictes précédentes, le troisième vecteur e_3 doit respectivement être égal à $-e_1 - e_2$, $e_1 - e_2$, $-e_1 + e_2$ ou $e_1 + e_2$. Ces différents choix ne nous donnent au final que deux super-bases relâchées,

$$\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\} \qquad ; \qquad \{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}.$$

Nous montrons désormais qu'elles sont distinctes. Supposons par l'absurde qu'elles sont égales. Alors, $e_1 + e_2 = e_1 - e_2$ ou $e_1 + e_2 = -e_1 + e_2$. Dans les deux cas, nous arrivons à une contradiction puisque $e_2 = 0$ dans le premier cas et $e_1 = 0$ dans le second - (e_1, e_2) ne pouvant donc pas être une base stricte. Cela conclut notre preuve. □

Nous sommes désormais en mesure de construire les topographes.

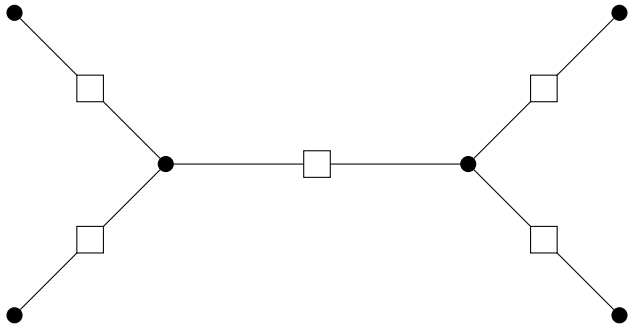
Définition 4.7. *Soit Λ un réseau. Un* ***topographe*** *pour le réseau Λ est un graphe $\Gamma = \{V, E\}$, où les sommets V sont les super-bases relâchées de Λ et ou deux super-bases relâchées distinctes sont reliées par une arête si elles contiennent une même base relâchée.*

Nous allons expliciter la forme des topographes.

Proposition 4.8. *Soient Λ un réseau et T son topographe. Alors, le graphe T est régulier de valence égale à trois.*

Démonstration. Nous utilisons la proposition 4.6. À chaque super-base relâchée, nous pouvons associer trois bases relâchées distinctes et chaque bases relâchées est contenue dans deux super-bases relâchées distinctes. Par conséquent, tout sommet d'un topographe admet exactement trois arêtes incidentes. □

Les topographes ont donc la forme suivante,



où les carrés □ représentent des bases relâchées tandis que les disques ● représentent des super-bases relâchées.

Nous pouvons déjà montrer que le topographe d'un réseau est connexe.

Théorème 4.9. *Soit Λ un réseau et T son topographe. Alors, T est un graphe connexe.*

Démonstration. Pour montrer qu'un topographe T est connexe, il nous suffit de montrer qu'il existe un chemin reliant deux arêtes arbitraires. Prenons une arête quelconque du topographe $\{\pm e_1, \pm e_2\}$. Par la proposition 4.8, cette arête a quatre arêtes adjacentes. La proposition 4.6 nous permet de les déterminer. Celles-ci sont

$$\{\pm e_1, \pm(e_1 - e_2)\} \quad ; \quad \{\pm(e_1 - e_2), \pm e_2\} \quad ; \quad \{\pm e_1; \pm(e_1 + e_2)\} \quad ; \quad \{\pm(e_1 + e_2), \pm e_2\}.$$

Une base relâchée n'est jamais déterminée que par les vecteurs d'une base stricte. Autrement dit, une base stricte est associée à une unique base relâchée et la fonction qui envoie une base stricte sur sa base relâchée est une surjection entre l'ensemble des bases

strictes vers l'ensemble des bases relâchées. Prenons la base stricte (e_1, e_2) dont les vecteurs proviennent de la base relâchée $\{\pm e_1, \pm e_2\}$. Soit M une matrice de $\mathrm{GL}_2(\mathbb{Z})$, la proposition 4.2 indique que le couple ordonné $(e_1, e_2)M$ est une base stricte de Λ. On déduit que le produit

$$(e_1, e_2)\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = (e_1, e_1 - e_2)$$

est une base stricte et les vecteurs de celle-ci appartiennent à la base relâchée $\{\pm e_1, \pm(e_1 - e_2)\}$. Nous pouvons appliquer d'autres matrices à la base stricte (e_1, e_2). On constate que les vecteurs de la base stricte

$$(e_1, e_2)\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = (e_1 - e_2, e_2)$$

appartiennent à la base relâchée $\{\pm(e_1 - e_2), \pm e_2\}$. Ceux de la base stricte

$$(e_1, e_2)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (e_1, e_1 + e_2)$$

appartiennent à la base relâchée $\{\pm e_1; \pm(e_1 + e_2)\}$. Tandis que ceux de

$$(e_1, e_2)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (e_1 + e_2, e_2)$$

appartiennent à la base relâchée $\{\pm(e_1 + e_2), \pm e_2\}$. Nous avons donc trouvé des matrices envoyant une base stricte sur d'autres bases strictes dont les vecteurs appartiennent aux bases relâchées adjacentes de la base relâchée d'origine. Cette méthode permet de se déplacer sur le topographe. Pour montrer que le topographe est connexe, la proposition 4.2 assure qu'il suffit de montrer que les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

génèrent le groupe $\mathrm{GL}_2(\mathbb{Z})$. En effet, si ces matrices génèrent $\mathrm{GL}_2(\mathbb{Z})$, alors à partir d'une base stricte, nous pouvons atteindre chacune des bases strictes du réseaux Λ via ces matrices. Ainsi, nous passerions par chaque base relâchée. Pour ce faire, nous utilisons les propositions 2.18 et 2.19. Cette première nous dit que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est d'indice deux dans $\mathrm{GL}_2(\mathbb{Z})$ et la seconde démontre que les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

génèrent le groupe $\mathrm{SL}_2(\mathbb{Z})$. La matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

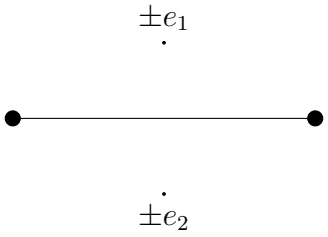
étant de déterminant -1, on conclut que les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

génèrent $\mathrm{GL}_2(\mathbb{Z})$. □

Nous introduisons désormais une notation afin de simplifier la représentation des topographes.

Notation 4.10. Soit Λ un réseau et T un topographe de ce réseau. Le dessin suivant représente le fait que deux super-bases relâchées sont reliées l'une à l'autre par la base relâchée $\{\pm e_1, \pm e_2\}$.



Nous allons pouvoir entamer la section sur les formes quadratiques binaires. Nous rappelons que l'idée derrière ce chapitre est de rendre visuelle la théorie des formes quadratiques binaires. Nous montrerons donc dans un premier temps que la nouvelle définition que nous prenons est équivalente à celle présentée dans le chapitre 3. Ensuite, nous donnerons une représentation aux formes quadratiques binaires grâce à la notion de topographe.

4.2 Formes quadratiques binaires et équivalence des définitions

Nous réintroduisons désormais la notion de formes quadratiques binaires.

Définition 4.11. *Soit Λ un réseau de dimension deux. Une fonction $f : \Lambda \to \mathbb{Z}$ est une* ***forme quadratique binaire*** *sur Λ si, pour tout élément x, y, z du réseau Λ et tout entier a,*

1. *la fonction f est quadratique, i.e. $f(ax) = a^2 f(x)$;*
2. *la fonction $B(x, y) = f(x + y) - f(x) - f(y)$ est symétrique et bilinéaire, i.e. pour tout réel λ, μ,*

$$B(x, y) = B(y, x);$$

$$B(\lambda x + \mu z, y) = \lambda B(x, y) + \mu B(z, y).$$

Notre nouvelle définition de forme quadratique binaire semble bien différente de notre première définition du chapitre 3. En effet, nous partions dans le chapitre précédent d'une définition où les formes quadratiques binaires sont des polynômes. Désormais, nous les définirons comme des fonctions munies de certaines propriétés. Cette distinction est dans notre cas peu importante. Nous allons montrer que les fonctions polynomiales homogènes de degré deux à deux indéterminés et à coefficients dans les entiers sont des formes quadratiques binaires au sens de la définition 4.11 et vice versa. De plus, nous laisserons le soin au lecteur de constater que considérer des fonctions polynomiales plutôt que des polynômes au chapitre précédent ne change en rien les résultats démontrés dans celui-ci.

Proposition 4.12. *Soit Λ un réseau de dimension deux pour la base $\{e_1, e_2\}$. La fonction $f : \Lambda \to \mathbb{Z}$ définie par*

$$f(xe_1 + ye_2) = ax^2 + bxy + cy^2,$$

où a, b et c sont des entiers, est une forme quadratique binaire au sens de la définition 4.11.

De plus, toute forme quadratique binaire dans le sens de la définition 4.11 sur le réseau Λ est une fonction telle que pour tout élément $xe_1 + ye_2$ du réseau Λ,

$$f(xe_1 + ye_2) = f(e_1)x^2 + B(e_1, e_2)xy + f(e_2)y^2.$$

Toute forme quadratique binaire au sens de la définition 4.11 est donc une fonction polynomiale homogène de degré deux à deux indéterminées et à coefficients dans les entiers.

Démonstration. [1] Nous commençons par la première assertion. Il est clair que la fonction f est quadratique. Nous passons donc directement à la vérification du second point de la définition. Nous allons utiliser la représentation matricielle de telles fonctions. On remarque que

$$f(xe_1 + ye_2) = (x, y) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Posons la notation

$$A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

1. La première partie de cette preuve est entièrement reprise de la preuve de la propriété 17.5.1 de la référence [4].

Nous calculons que

$$\begin{aligned} B(x_1e_1+y_1e_2, x_2e_1+y_2e_2) &= (x_1+x_2, y_1+y_2)A\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix} \\ &= (x_1,y_1)A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + (x_1,y_1)A\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + (x_2,y_2)A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \\ &\quad + (x_2,y_2)A\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} - (x_1,y_1)A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} - (x_2,y_2)A\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\ &= (x_1,y_1)A\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + (x_2,y_2)A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}. \end{aligned}$$

Puisque la matrice A est symétrique, nous voyons que

$$(x_2,y_2)A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \left((x_2,y_2)A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}\right)^T = (x_1,y_1)A\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Par conséquent,

$$B(x_1e_1+y_1e_2, x_2e_1+y_2e_2) = 2(x_1,y_1)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Puisque le produit matriciel est distributif, la fonction B est bilinéaire. De plus, la matrice $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ étant symétrique, la fonction B est elle aussi symétrique. Nous avons donc montré que les fonctions polynomiales homogènes de degré deux à deux indéterminées et à coefficients entiers sont des formes quadratiques binaires au sens de la définition 4.11.

Nous passons désormais à la preuve de la seconde assertion. On remarque que pour toute forme quadratique binaire $f : \Lambda \to \mathbb{Z}$ et pour tout élément r du réseau Λ,

$$f(r) = \frac{1}{2}B(r,r).$$

Dans notre cas, Λ est un réseau pour la base $\{e_1, e_2\}$. Alors, nous pouvons écrire tout élément r du réseau comme $r = xe_1 + ye_2$. Par conséquent,

$$\begin{aligned} f(r) &= \frac{1}{2}B(r,r) \\ &= \frac{1}{2}B(xe_1+ye_2, xe_1+ye_2) \\ &= \frac{1}{2}(x^2B(e_1,e_1) + 2xyB(e_1,e_2) + y^2B(e_2,e_2)) \\ &= f(e_1)x^2 + B(e_1,e_2)xy + f(e_2)y^2. \end{aligned}$$

Nous avons donc trouvé l'expression recherchée. De plus, puisque f est une fonction à

valeurs dans les entiers, les coefficients sont bien des entiers. On déduit de cette écriture que les formes quadratiques binaires au sens de la définition 4.11 sont des fonctions polynomiales homogènes de degré deux à deux indéterminées et à coefficients entiers. □

Remarque 4.13. Le résultat précédent montre bien qu'il y a une équivalence entre les deux définitions introduites. Par conséquent, si nous fixons une base pour notre réseau, nous ne perdons pas en généralité lorsque nous considérons les formes quadratiques binaires comme des fonctions polynomiales homogènes de degré deux à coefficients entiers. Cela nous permettra, entre autres, de redéfinir la notion d'équivalence comme nous l'avions fait dans le chapitre 3.

Bien que les définitions soient équivalentes, la définition 4.11 et la proposition 4.12 nous donnent des informations complémentaires concernant les coefficients des formes quadratiques binaires lorsqu'une base de notre réseau est précisée. Ces informations sont reprises dans le corollaire suivant.

Corollaire 4.14. *Soient Λ un réseau de dimension deux pour la base $\{e_1, e_2\}$ et f une forme quadratique binaire sur ce réseau. Alors, la forme quadratique binaire f est entièrement déterminée par les valeurs $f(e_1), f(e_2)$ et $f(e_1+e_2)-f(e_1)-f(e_2)$.*

Démonstration. Nous avions montré dans la preuve de la proposition 4.12 que pour tout élément $xe_1 + ye_2$ du réseau Λ, nous pouvons écrire

$$\begin{aligned} f(xe_1+ye_2) &= f(e_1)x^2 + B(e_1,e_2)xy + f(e_2)y^2 \\ &= f(e_1)x^2 + (f(e_1+e_2)-f(e_1)-f(e_2))xy + f(e_2)y^2. \end{aligned}$$

Les coefficients sont donc des constantes propres au réseau et à la forme quadratique binaire f et elles la déterminent totalement. □

Notation 4.15. Le corollaire précédent nous permet de réutiliser une notation du chapitre 3. En effet, lorsque nous définissons une forme quadratique binaire f sur un réseau Λ et $\{e_1, e_2\}$ une base de Λ, nous pouvons la spécifier entièrement par les coefficients

$$a = f(e_1) \quad ; \quad b = f(e_1+e_2)-f(e_1)-f(e_2) \quad ; \quad c = f(e_2).$$

Par conséquent, lorsque cela sera opportun, nous écrirons à nouveau

$$f = (a, b, c).$$

Nous redéfinissons désormais l'image d'une forme quadratique binaire.

Définition 4.16. *Soit Λ un réseau de dimension deux et f une forme quadratique binaire sur ce réseau. On définit* ***l'image*** *de f par*

$$\mathrm{Im}(f) = \{f(r) | r \in \Lambda\}.$$

Un entier n appartenant à l'image de f est appelé un entier ***représenté*** *par f.*

Au vu de la proposition 4.12, il est clair que la définition d'image est analogue à celle définie au chapitre 3. La définition d'entier représenté reste donc identique.

Nous pouvons toujours distinguer la représentation de la représentation propre.

Définition 4.17. *Soit Λ un réseau de dimension deux et f une forme quadratique binaire sur ce réseau. Un entier n est* ***proprement représenté*** *par f s'il existe un vecteur v du réseau Λ tel que v est un vecteur d'une base de Λ et $f(v) = n$.*

Proposition 4.18. *La définition de représentation propre d'un entier par un forme quadratique binaire 3.8 du chapitre 3 est équivalente à la définition de représentation propre 4.17.*

Démonstration. Munissons notre réseau Λ d'une base $\{e_1, e_2\}$. Disons que le vecteur v du réseau Λ appartienne à une base $\{v, w\}$ de Λ pour un certain vecteur w de Λ. Alors, la proposition 4.2 nous indique qu'il existe une matrice M appartenant à $\mathrm{GL}_2(\mathbb{Z})$ tel que

$$(v, w) = (e_1, e_2)M.$$

Si nous posons

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix},$$

on déduit que $v = re_1 + te_2$. Par conséquent,

$$f(v) = f(re_1 + te_2) = f(e_1)r^2 + (f(e_1 + e_2) - f(e_1) - f(e_2))rt + f(e_2)t^2.$$

Les entiers r et t sont premiers entre eux par le théorème de Bézout 2.6 et on conclut que $f(v)$ est proprement représenté par f au sens de la définition du chapitre 3.

Dans le sens inverse, si un entier n admet une représentation propre, alors il existe un couple d'entiers (r, t) premiers entre eux tel que $f(re_1 + te_2) = n$ et le vecteur $re_1 + te_2$ appartient notamment à la base $\{re_1 + te_2, se_1 + ue_2\}$ avec s et u des entiers tels que $ru - st = \pm 1$. □

Si nous munissons notre réseau d'une base, la proposition 4.12 indique que les formes quadratiques binaires au sens de la définition 4.11 sont des fonctions polynomiales homogènes de degré deux à deux indéterminées et à coefficients dans les entiers. Nous pouvons donc leur donner une forme matricielle comme nous l'avons fait au chapitre 3. Soient Λ

un réseau muni de la base $\{e_1, e_2\}$ et $f = (a, b, c)$ une forme quadratique binaire sur Λ. Nous pouvons écrire, pour tout élément $xe_1 + ye_2$ appartenant à Λ,

$$f(xe_1 + ye_2) = (x, y) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Nous redéfinissons donc notre action du groupe $\mathrm{GL}_2(\mathbb{Z})$ utilisé au chapitre 3.

Proposition 4.19. *L'action α du groupe $\mathrm{GL}_2(\mathbb{Z})$ sur les formes quadratiques binaires définies par*

$$\alpha(ax^2 + bxy + cy^2, M) = (x, y)M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M \begin{pmatrix} x \\ y \end{pmatrix}$$

est une action de groupe à droite. □

Nous définissons une fois de plus la notion d'équivalence.

Définition 4.20. *Soient Λ un réseau de dimension deux. Deux formes quadratiques binaires sont dites **équivalentes** si elles appartiennent à la même orbite sous l'action de $\mathrm{GL}_2(\mathbb{Z})$.*

Nous redonnons ci-dessous une preuve du fait que deux formes quadratiques binaires ont la même image.

Proposition 4.21. *Soit Λ un réseau pour la base $\{e_1, e_2\}$ et soient f et g deux formes quadratiques binaires équivalentes. Alors, $\mathrm{Im}(f) = \mathrm{Im}(g)$.*

Démonstration. Puisque f et g sont équivalentes, il existe une matrice M appartenant à $\mathrm{GL}_2(\mathbb{Z})$ tel que, pour tout élément $xe_1 + ye_2$ du réseau Λ,

$$g(xe_1 + ye_2) = (x, y)M^T \begin{pmatrix} f(e_1) & \frac{1}{2}B(e_1, e_2) \\ \frac{1}{2}B(e_1, e_2) & f(e_2) \end{pmatrix} M \begin{pmatrix} x \\ y \end{pmatrix},$$

où $B(e_1, e_2) = f(e_1 + e_2) - f(e_1) - f(e_2)$. Disons que la matrice M est égale à

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

Alors,

$$\begin{aligned} g(xe_1 + ye_2) &= (rx + sy, tx + uy) \begin{pmatrix} f(e_1) & \frac{1}{2}B(e_1, e_2) \\ \frac{1}{2}B(e_1, e_2) & f(e_2) \end{pmatrix} \begin{pmatrix} rx + sy \\ tx + uy \end{pmatrix} \\ &= f((rx + sy)e_1 + (tx + uy)e_2) \\ &= f(x(re_1 + te_2) + y(se_1 + ue_2)). \end{aligned}$$

Par conséquent, $\mathrm{Im}(g) \subseteq \mathrm{Im}(f)$. L'autre inclusion se prouve en considérant la matrice M^{-1} et en transformant g en f avec celle-ci. □

Remarque 4.22. Nous tenons à faire remarquer au lecteur que malgré le fait que la définition d'équivalence s'avère parfaitement identique à celle du chapitre précédent, on constate un changement de point de vue. Dans le chapitre précédent, nous avions souvent considéré que la transformée d'une forme quadratique binaire par une matrice de $\mathrm{GL}_2(\mathbb{Z})$ ou bien de $\mathrm{SL}_2(\mathbb{Z})$ consistait à changer les entrées de la matrice des coefficients de la forme quadratique binaire. Ce n'est pas fondamentalement ce qu'il se passe dans le cas présent. Transformer une forme quadratique binaire en une autre revient maintenant à changer la base de notre réseau. En effet, exemplifions en reprenant les développements faits dans la preuve de la proposition précédente. Soit Λ un réseau pour la base $\{e_1, e_2\}$ et soient f et g deux formes quadratiques binaires équivalentes telles que la transformée de f par la matrice

$$M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

soit g. Alors, nous avons montré dans la proposition précédente que pour tout élément $r = xe_1 + ye_2$ du réseau Λ,

$$g(xe_1 + ye_2) = f((rx + sy)e_1 + (tx + uy)e_2) = f(x(re_1 + te_2) + y(se_1 + ue_2)).$$

Évaluer g au point r revient à évaluer f au point $M \cdot r$ ou bien évaluer f sur le point de coordonnées (x, y) du réseau Λ, mais pour la base $(e_1, e_2)M$.

Les mêmes points du réseau peuvent toujours être atteint, mais leurs coordonnées changent. Alors que le chapitre précédent mettait en exergue l'importance des coefficients d'une forme quadratique binaire, notamment au travers du théorème 3.11, les résultats auxquels nous arriveront impliqueront quant à eux bien plus les idées liées aux changement de coordonnées des points du réseau.

La prochaine section sera consacrée à la construction du topographe d'une forme quadratique binaire.

4.3 Construction du topographe d'une forme quadratique binaire et progression arithmétique

Les réseaux que nous considérons dans cette section sont tous de dimension deux.

Dans cette section, nous allons formellement introduire les topographes d'une forme quadratique binaire. Fondamentalement, nous allons appliquer une forme quadratique binaire sur les bases relâchées et super-bases relâchées du topographe d'un réseau.

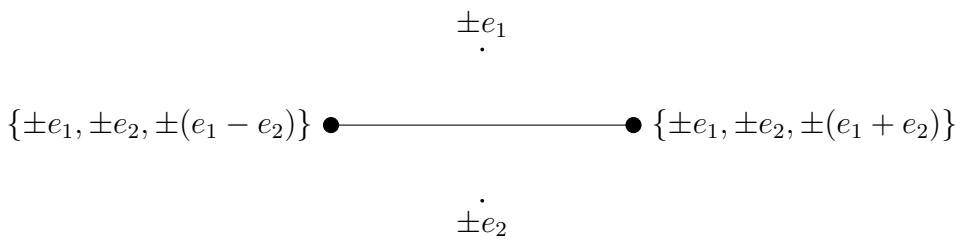
Définition 4.23. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Le* ***topographe*** *de f, noté T_f, est le topographe T auquel nous avons appliqué f aux vecteurs de ses arêtes et de ses sommets.*

Nous donnons ci-dessous un exemple.

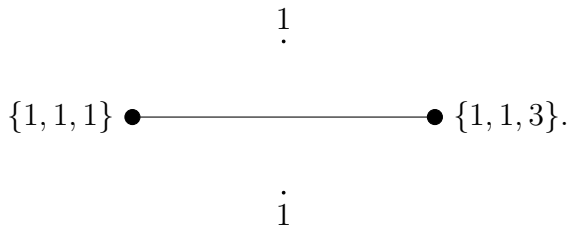
Exemple 4.24. Prenons Λ un réseau pour la base $\{e_1, e_2\}$ et f la forme quadratique binaire sur Λ telle que

$$f(e_1) = 1 \quad ; \quad f(e_1 + e_2) - f(e_1) - f(e_2) = 1; \quad f(e_2) = 1.$$

Le corollaire 4.14 indique que ces valeurs suffisent à entièrement déterminer la forme quadratique f. En l'occurrence, cette forme quadratique binaire est la forme quadratique binaire $(1, 1, 1)$ que nous avons déjà étudiée au chapitre 3. Sous la forme quadratique binaire $(1, 1, 1)$, la partie de représentation du topographe T



devient



Remarque 4.25. Tous les topographes ont la même structure. Ce sont des graphes réguliers de valence égale à trois. Par conséquent, si nous trouvons un résultat sur un topographe d'une forme quadratique binaire qui nous donne une information sur la structure du graphe sous-jacente, alors cette information est commune à tout topographe. Cette remarque sera centrale lorsque nous montrerons que les topographes n'admettent aucun cycle.

L'idée des prochains résultats est de déterminer, à partir de valeurs d'une forme quadratique binaire sur une super-base relâchée, les valeurs de cette forme quadratique binaire sur chaque super-base relâchée. Cela est possible grâce à la formule suivante.

Proposition 4.26. *[6, en p.9] Soit Λ un réseau et f une forme quadratique sur ce réseau. Pour tout vecteur r_1, r_2 du réseau Λ, la forme quadratique binaire f satisfait la formule*

$$f(r_1 + r_2) + f(r_1 - r_2) = 2(f(r_1) + f(r_2)).$$

Démonstration. Notons $B(r_1, r_2) = f(r_1 + r_2) - f(r_1) - f(r_2)$ la fonction bilinéaire symétrique associée à f. Dès lors, nous calculons que

$$\begin{aligned} f(r_1 + r_2) + f(r_1 - r_2) &= f(r_1) + f(r_2) + B(r_1, r_2) + f(r_1) + f(r_2) - B(r_1, r_2) \\ &= 2(f(r_1) + f(r_2)). \end{aligned}$$

Nous avons donc bien montré que f satisfait la formule énoncée. □

Le corollaire 4.14 nous avait montré qu'une forme quadratique binaire f sur un réseau Λ pour une base $\{e_1, e_2\}$ est entièrement déterminée par les valeurs $a = f(e_1), c = f(e_2)$ et $b = f(e_1 + e_2) - f(e_1) - f(e_2)$. La proposition précédente nous donne une autre caractérisation de f.

Corollaire 4.27. *Soit Λ un réseau et $\{e_1, e_2\}$ une base de Λ et f une forme quadratique binaire sur Λ. Alors, f est entièrement déterminé par les valeurs $f(e_1), f(e_2)$ et $f(e_1) + f(e_2) - f(e_1 - e_2)$.*

Démonstration. La proposition précédente nous indique dans le cas ou $r_1 = e_1$ et $r_2 = e_2$ que $f(e_1 + e_2) - f(e_1) - f(e_2) = f(e_1) + f(e_2) - f(e_1 - e_2)$. Par conséquent, f est aussi totalement déterminée par les valeurs $f(e_1), f(e_2)$ et $f(e_1) + f(e_2) - f(e_1 - e_2)$. □

Avec la formule de la proposition 4.26 à notre disposition, nous pouvons calculer à partir d'une super-base relâchée l'image d'une forme quadratique binaire.

Lemme 4.28. *Soit Λ un réseau et f une forme quadratique binaire sur ce réseau. Soient r_1, r_2 des vecteurs appartenant au réseau Λ. Posons*

$$f(r_1) = a \quad ; \quad f(r_2) = c \quad ; \quad f(r_1 + r_2) = d \quad ; \quad f(r_1 - r_2) = e.$$

Alors, il existe un entier b tel que

$$e = a + c - b \qquad ; \qquad d = a + c + b.$$

Démonstration. Si nous utilisons la formule de la proposition 4.26, nous voyons que

$$d + e = 2(a + c).$$

De là, on constate que

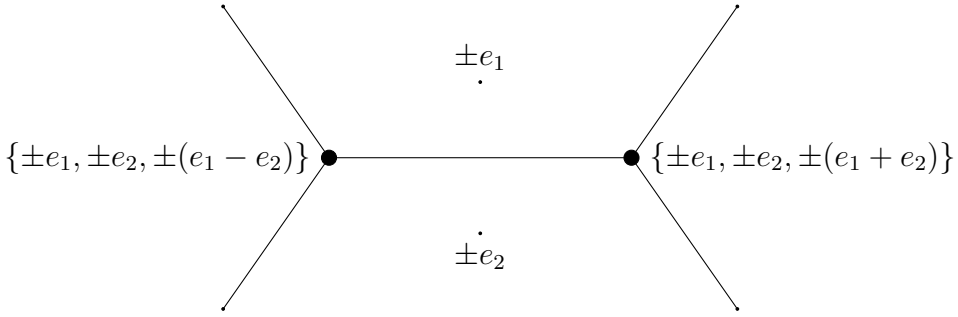
$$d = a + c - (e - a - c) = a + c + (d - a - c).$$

De plus, il est clair que

$$e = a + c + (e - a - c) = a + c - (d - a - c).$$

Nous posons donc $b = e - a - c = -(d - a - c)$ et cela prouve la proposition. □

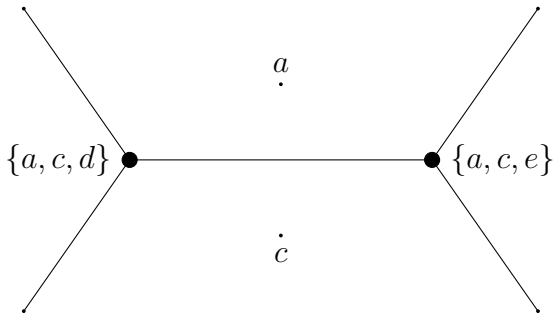
Reprenons un réseau Λ et une forme quadratique binaire f sur ce réseau et déterminons comment utiliser les résultats précédents permettent de totalement construire son topographe. Regardons une partie quelconque du topographe servant à construire le topographe autour d'une arête dont la base relâchée associée est $\{\pm e_1, \pm e_2\}$.



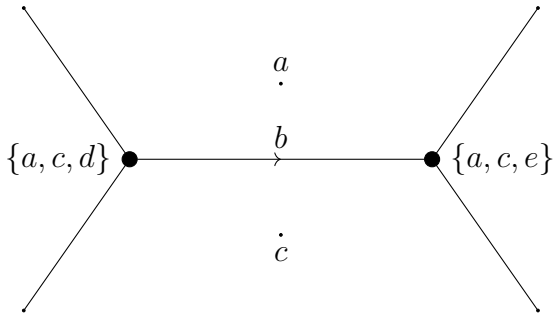
Si nous posons

$$f(e_1) = a \quad ; \quad f(e_2) = c \quad ; \quad f(e_1 + e_2) = d \quad ; \quad f(e_1 - e_2) = e,$$

nous pouvons construire la partie de topographe de Conway associée à f.



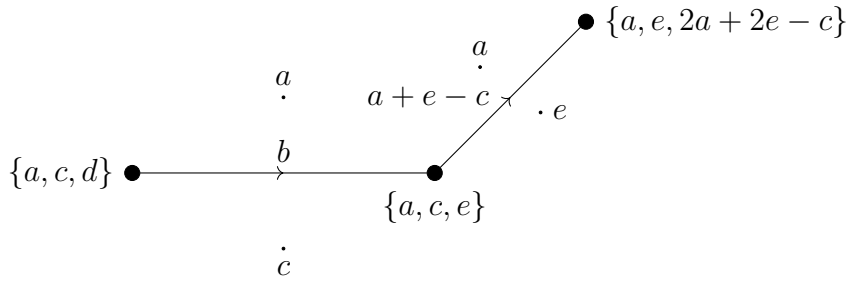
Le lemme 4.28 nous permet d'orienter l'arête de façon à garder le signe de $b = e - a - c = a + c - d$ positif. De sorte que suivre la direction de la flèche indique que $a + c + b = e$ et aller dans le sens opposé indique que $d = a + c - b$.



Nous faisons dès à présent deux commentaires cruciaux.

Remarque 4.29. Nous donner une arête orientée d'un topographe revient à se donner deux formes quadratiques binaires sur notre réseau : les formes quadratiques binaires (a, b, c) et (c, b, a) (en réalité plutôt quatre si l'on considère les signes de b). Ces formes quadratiques binaires sont bien entendu équivalentes. Nous pouvons donc vraiment voir les formes quadratiques binaires sur les topographes et plus précisément sur les arêtes des topographes. Cette façon de d'appréhender les formes quadratiques binaires sera utile non-seulement lorsque nous traiterons des groupes d'automorphismes des formes quadratiques binaires dans les prochaines sections, mais aussi lorsque nous élaborerons un algorithme décidant si un entier est proprement représenté par une forme quadratique binaire ou non.

Remarque 4.30. Orienter les arêtes nous permet de construire un topographe d'une forme quadratique. Si nous reprenons le dessin plus haut et que nous suivons les indications, nous voyons que $e = a + b + c$. L'arête en haut à droite peut être le couple $\{a, e\}$. On trouve la valeur et l'orientation de l'arête en calculant $a + e - c$. Le dessin suivant représente le cas ou $a + e - c$ est positif. Cela nous permet de déterminer la dernière valeur du sommet en haut à droite. Celle-ci vaut $2a + 2e - c$. On peut faire pareil pour chacune des arêtes. Cette façon de construire un topographe d'une forme quadratique binaire s'appelle la **règle de la progression arithmétique**[2].



La règle de la progression arithmétique sera particulièrement utile dans la prochaine section lorsque nous prouverons que les topographes sont des arbres.

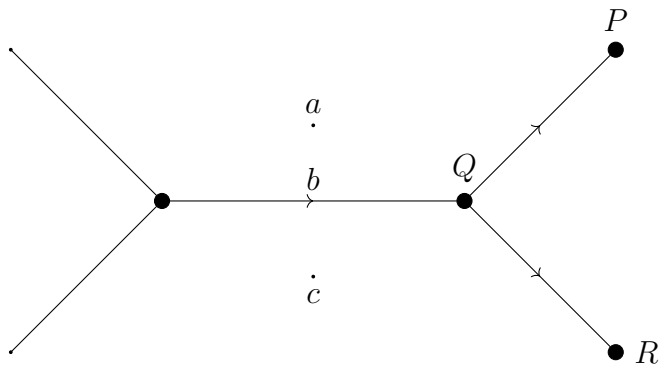
2. Cette nomination provient du fait que les nombres $d, a + c, e$ sont en progression arithmétique de raison b.

4.4 Structure d'arbres des topographes et représentation principale

Les réseaux que nous considérons dans cette section sont tous de dimension deux.

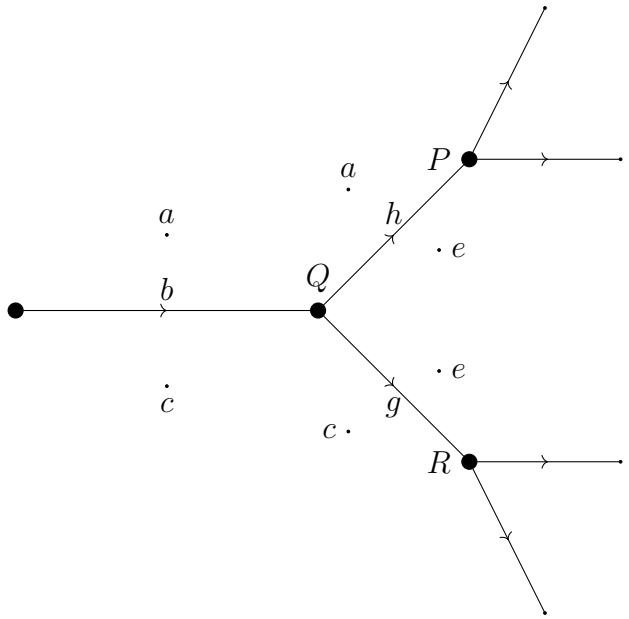
Dans cette section, nous allons montrer que le topographe d'un réseau Λ est un arbre, i.e. un graphe connexe sans cycle. Nous avons déjà démontré dans la section 4.1 que le topographe d'un réseau est connexe. Il nous reste donc seulement à montrer qu'il ne contient pas de cycle. Nous commençons par l'élaboration d'un lemme utilisant la règle de la progression arithmétique afin de nous informer sur les prochains entiers du topographe de Conway d'une forme quadratique binaire.

Lemme 4.31. *[6, Climbing lemma en p.11-12] Soit Λ un réseau et f une forme quadratique binaire sur ce réseau. Soit*



une partie du topographe de f où a, b et c sont des entiers positifs. Alors, les arêtes liant Q à P et Q à R sont orientés de Q vers P et de Q vers R.

Démonstration. Par la règle de la progression arithmétique, le sommet Q contient les valeurs a, c et $e = a + b + c$. Disons, sans perte de généralité, que l'arête reliant Q au sommet P est $\{a, e\}$. La règle de la progression arithmétique nous dit qu'il existe un entier h tel que $a + e - h = 2a + b + c - h = c$. Donc, $h = 2a + c$ est positif et l'orientation de l'arrête liant Q à P est bien de Q vers P. Il en va de même pour l'arête reliant Q à R. On déduit de la proposition 4.6 que l'arête reliant Q à R est $\{e, c\}$. En utilisant la règle de la progression arithmétique, nous savons qu'il existe un entier g tel que $c+e-g = a+b+2c-g = a$. On déduit que $g = b+2c$ est positif et en conséquence, l'orientation de l'arête liant Q à R est de Q vers R.

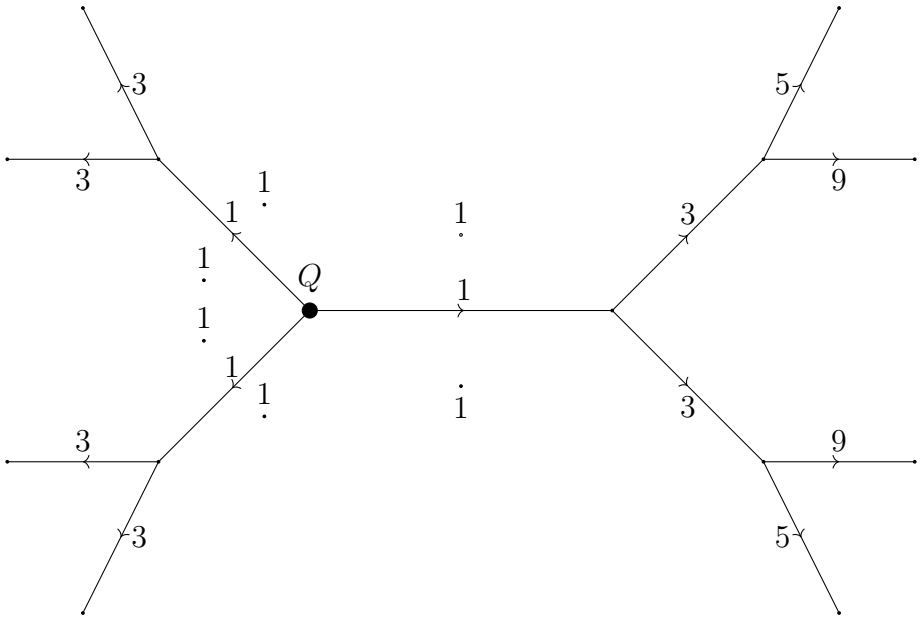


□

Nous montrons désormais que les topographes n'admettent pas de cycle.

Théorème 4.32. *[6, en p.12] Soit Λ un réseau et T un topographe de Λ. Alors, T n'admet pas de cycle.*

Démonstration. Pour démontrer ce résultat, nous allons regarder le topographe de la forme quadratique binaire $(1, 1, 1)$. Puisque la structure de graphe d'un topographe est indépendante de la forme quadratique binaire, prouver qu'un topographe d'une forme quadratique binaire bien précis n'admet pas de cycle démontrera qu'aucun topographe n'admet de cycle. À cet effet, nous représentons une certaine partie du topographe de la forme quadratique binaire $(1, 1, 1)$ et représentons bien les orientations de chaque arête.



On constate que le sommet Q du graphe est tel que les arêtes sont orientées de façon à sortir du sommet. Par conséquent, les valeurs représentées sur le topographes de $(1, 1, 1)$ ne peuvent que croître par le lemme 4.31. Ainsi, ce topographe de Conway ne possédera aucun cycle. En effet, si ce topographe présentait un cycle, alors les valeurs devraient décroître à un moment ce qui serait absurde. Il en sera de même pour tous les autres au vu de la discussion précédente. □

Puisque les topographes sont connexes 4.9 et n'admettent pas de cycle 4.32, nous obtenons directement le théorème suivant.

Théorème 4.33. *Tout topographe d'un réseau est un arbre.* □

Nous allons maintenant pouvoir alléger les dessins en introduisant la notion de représentation principale d'un topographe. Nous rappelons ci-dessous la définition de graphe planaire.

Définition 4.34. *Soit $G = (V, E)$ un graphe. Le graphe G est dit **planaire** s'il existe*

1. *une fonction $i : V \to \mathbb{R}^2$ injective ;*
2. *pour toute arête $e = \{u, v\}$ de E, il existe une fonction linéaire $\phi_e : [0, 1] \to \mathbb{R}^2$ telle que $\phi_e(0) = i(u)$ et $\phi_e(1) = i(v)$. De plus, pour tout arête e_1, e_2 distinctes de E et tout $s, t \in]0, 1[$, $\phi_{e_1}(t) \neq \phi_{e_2}(s)$.*

*Un triplet $\mathcal{R} = (G, i, \{\phi_e\}_{e\in E})$ sera appelé une **représentation** du graphe G dans le plan.*

Les représentations des graphes planaires admettent des faces, i.e. des régions connexes du plan.

Définition 4.35. *Soit $G = (V, E)$ un graphe planaire muni d'une représentation $\mathcal{R} = (G, i, \{\phi_e\}_{e\in E})$. Une **face** de la représentation $(G, i, \{\phi_e\}_{e\in E})$ est une composante connexe de l'ensemble $\mathbb{R}^2 \setminus \bigcup_{e\in E} \phi_e([0, 1])$.*

Nous allons désormais montrer que les arbres réguliers de valence trois sont des graphes planaires. Cela induira que les topographes sont des graphes planaires.

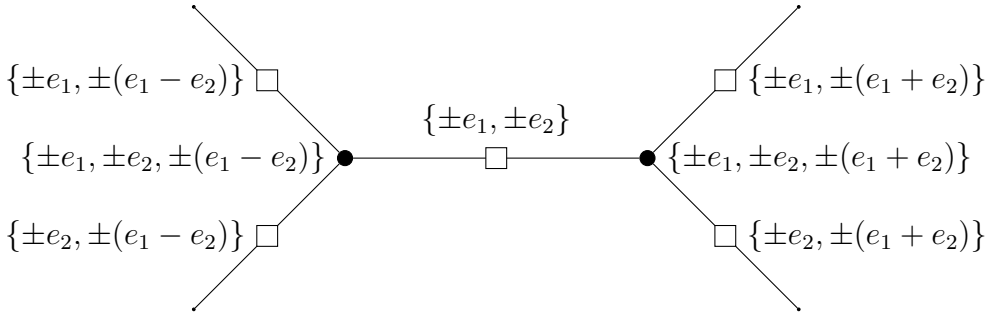
Proposition 4.36. *Tout arbre régulier de valence égale à trois est un graphe planaire.*

Démonstration. Pour montrer cela, nous allons simplement construire notre représentation. Soit $G = (V, E)$ un arbre régulier de valence égale à trois et soit la plan $\mathbb{R}^2$ d'abscisse x et d'ordonnée y. Soit v_0 un sommet arbitraire de V. Notre représentation se construit de la façon suivante. Nous plaçons v_0 au point de coordonnée $(0, 0)$. Nous plaçons ensuite les sommets adjacents sur les points de coordonnée $(-1, 1)$; $(0, 1)$; et $(1, 1)$. Nous relions ces points au point $(0, 0)$. Nous procédons désormais par induction. Pour chacun des sommets que nous rajouterons, nous devrons le lier à trois autres sommets. Un de ces sommets sera le sommet à partir duquel nous avons construit les coordonnées du point associé. Nous appellerons ce sommet le sommet parent. Les deux autres seront les sommets que nous construisons à la prochaine étape de l'induction. Ces sommets seront appelés sommets enfants. Soit v_P un sommet posé sur le point de coordonnée (x_P, m) pour m un naturel, alors les sommets enfants auront les coordonnées $(x_P + \frac{1}{(m+1)^2}, m+1)$ et $(x_P - \frac{1}{(m+1)^2}, m+1)$. Les arêtes reliant les sommets ne s'intersecteront jamais puisque les abscisses des coordonnées des points n'ayant pas le même sommet parent sur un même étage s'éloignent plus nous montons dans les étages. Et ceux partageant le même sommet parent sont toujours espacés sur l'axe des abscisses. □

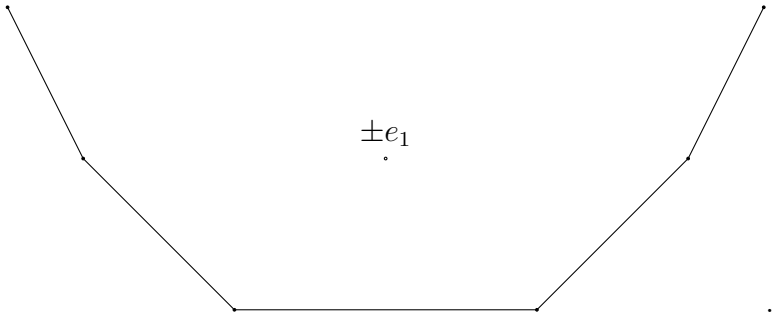
Corollaire 4.37. *Tout topographe T d'un réseau est un graphe planaire.*

Démonstration. Par le théorème 4.33, nous savons que T est un arbre. De plus, par la propriété 4.8, nous savons que les topographes sont des graphes réguliers de valence égale à trois. Nous déduisons donc par la propriété précédente que T est planaire. □

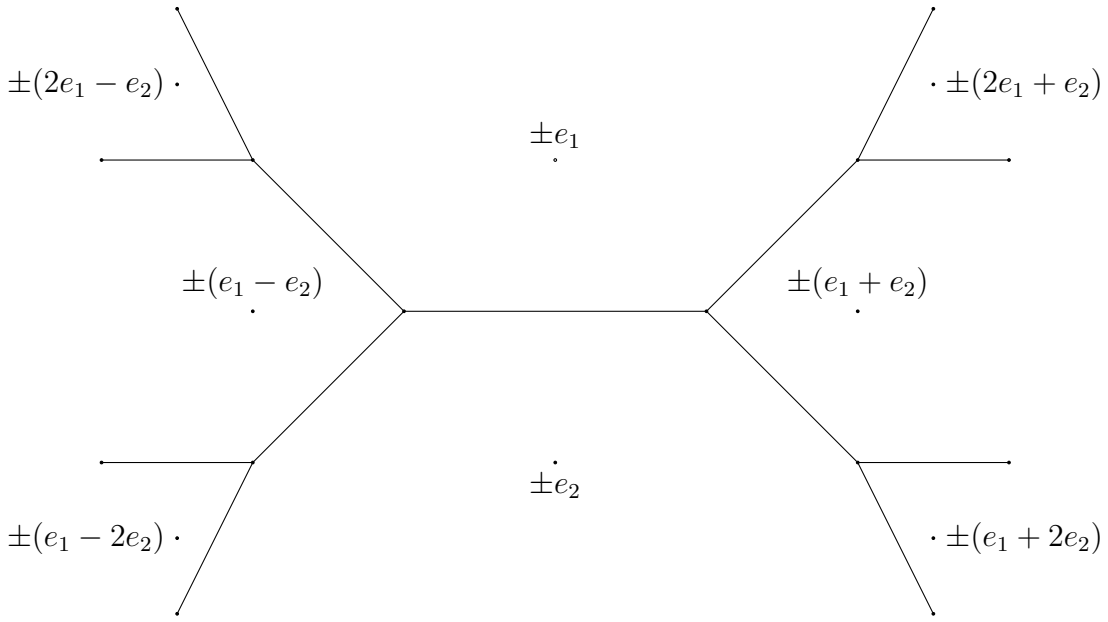
Nous pouvons désormais faire des dessins plus économes en notations. Prenons une base relâchée quelconque $\{\pm e_1, \pm e_2\}$ d'un réseau Λ. Dessinons un exemple d'une partie de topographes autour de cette base relâchée.



Nous pouvons tracer un chemin sur le graphe passant par tous les sommets et arêtes contenant $\pm e_1$. Nous montrerons plus tard que nous pouvons toujours nous arranger pour que le chemin encercle une face du graphe. Nous notons cette face $\pm e_1$ et la représentons comme suit,



Nous pouvons faire de même pour tous les autres éléments de bases de telle sorte que deux vecteurs séparés par une arête forment une base relâchée et trois vecteurs entourant un sommet donnent une super-base relâchée.

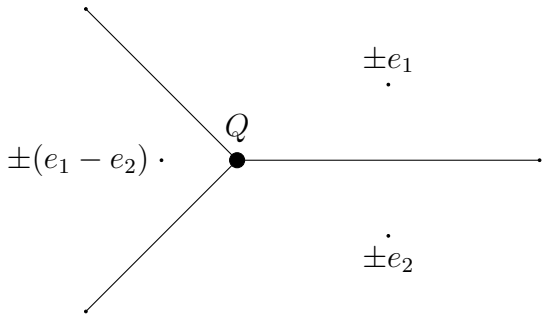


Nous appellerons ces représentations des représentations principales.

Définition 4.38. *Soit Λ un réseau et $T = (V, E)$ le topographe de ce réseau. Notons P_r le chemin du topographe T passant par chaque arête contenant le vecteur relâché $\pm r$. Une représentation $\mathcal{R} = (T, i, \{\phi_e\}_{e\in E})$ du topographe T est dite* ***principale*** *si, pour tout vecteur relâché $\pm r$ appartenant à une base relâchée du réseau Λ, le chemin P_r délimite une face de la représentation $\mathcal{R}$ du topographe T. Plus précisément, si une des deux composantes connexes de l'ensemble $\mathbb{R}^2 \setminus \bigcup_{e\in P_r} \phi_e([0, 1])$ est une face de $\mathcal{R}$.*

Nous montrons désormais que tout réseau admet un topographe principal. Pour ce faire, nous complémentons la notation 4.10.

Notation 4.39. Dans la notation 4.10, séparer deux vecteurs relâchés par une arête impliquait que l'arrête était l'union de ces deux vecteurs relâchés. Nous faisons pareil, mais dans le cas des super-bases relâchées. Le dessin suivant indique que la super-base relâchée Q est constituée des vecteurs relâchées l'encerclant.

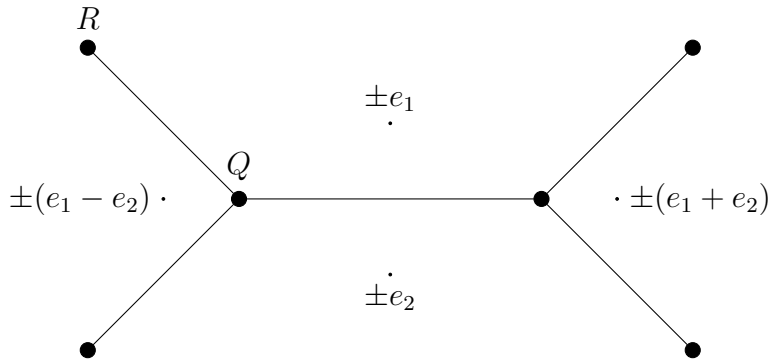


De plus, cette notation couplée à la notation 4.10 fixe les arêtes liée à Q.

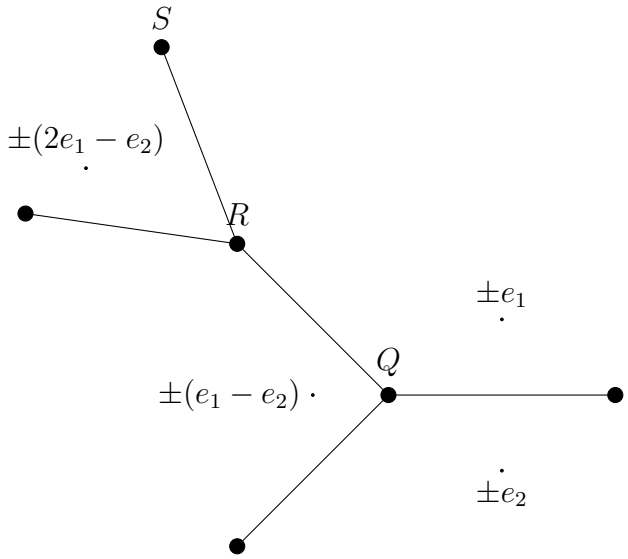
Cette notation est précieuse dans le sens où elle montre instantanément ce qu'il implique pour un topographe d'être principal. On peut arranger l'écriture des bases relâchées de telle sorte que les faces du topographes ne "contiennent" qu'un seul vecteur relâché. Nous approfondissons cette observation dans le théorème suivant.

Théorème 4.40. *Soit Λ un réseau pour la base $\{e_1, e_2\}$ et T son topographe. Alors, T admet une représentation principale.*

Démonstration. Nous allons construire une représentation principale. Nous partons de la base relâchée $\{\pm e_1, \pm e_2\}$ du réseau Λ. Par la proposition 4.6, les super-bases relâchées sont $\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\}$ et $\{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}$. Concentrons-nous sur la super-base relâchée $\{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}$. Les trois arêtes sortantes sont données par les bases relâchées $\{\pm e_1, \pm e_2\}$; $\{\pm e_1, \pm(e_1 - e_2)\}$; et $\{\pm e_2, \pm(e_1 - e_2)\}$.



La super-base du sommet R est déjà au moins constituée des vecteurs relâchés $\pm e_1, \pm(e_1 - e_2)$ et puisque nous avons déjà fixé les vecteurs relâchés de la super-base du sommet Q, la proposition 4.6 nous assure que nous n'avons qu'un unique choix de vecteur relâché pour compléter la super-base du sommet R. Nous ajoutons donc le vecteur relâché $\pm(2e_1 - e_2)$.



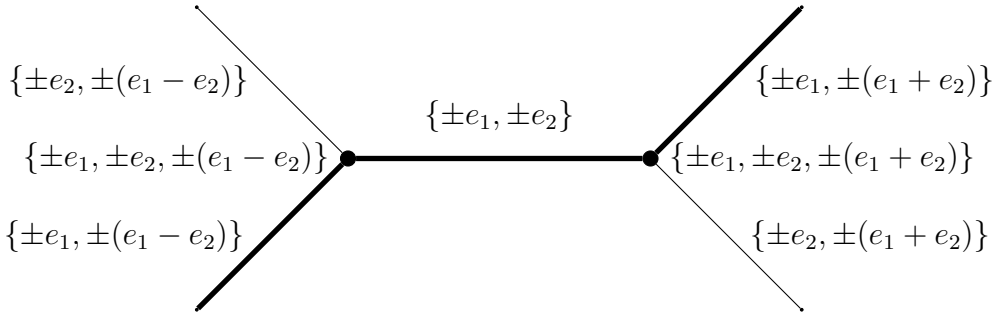
Afin de continuer la construction, nous allons pousser la notation jusqu'au bout. Nous voyons qu'une des arêtes liée au sommet R est la base relâchée $\{\pm(2e_1 - e_2), \pm(e_1 - e_2)\}$ et une autre est celle que nous avions déjà, c'est à dire la base relâchée $\{\pm e_1, \pm(e_1 - e_2)\}$. Pour la dernière arête, nous n'avons pas le choix. C'est la base relâchée $\{\pm(2e_1 - e_2), \pm e_1\}$. Par conséquent, réannoter le vecteur relâché $\pm e_1$ à droite de l'arête RS est superflu puisqu'aucun autre vecteur n'est un candidat et qu'il est déjà sur une des faces adjacentes. De deux choses l'une :

1. fixer une base relâchée à un sommet et utiliser les notations 4.10 et 4.39 est suffisant pour construire sans ambiguïté toute la représentation du topographe, car comme nous l'avons montré, nous pouvons de cette façon voyager de sommet en sommet en les construisant ;
2. cette construction nous donne bien un topographe principal puisqu'il n'y a qu'un seul vecteur relâché par face et en conséquence, le chemin constitué des bases relâchées contenant ce vecteur relâché entoure la face dans laquelle il se situe.

Puisque les topographes sont connexes, nous pouvons continuer ce procédé de sommet en sommet afin de construire l'entièreté de la représentation. De plus, cette représentation est principale, ce qui conclut notre preuve. □

La preuve du théorème précédent confirme en quelque sorte la notation que nous avons introduite plus tôt. Nous ne perdons aucune information lorsque nous l'utilisons. De plus, celle-ci force en quelque sorte la représentation du topographe à être principale. Par la suite, car nous n'utiliserons plus que des représentations principales, nous continuerons

d'utiliser cette notation. Celle-ci nous sera d'ailleurs d'une précieuse aide. Il est cependant à noter que toutes les représentations ne sont pas principales comme le montre la partie de représentation suivante. Le chemin contenant le vecteur relâché $\pm e_1$ surligné en gras sur le dessin ne peut délimiter une face de la représentation.

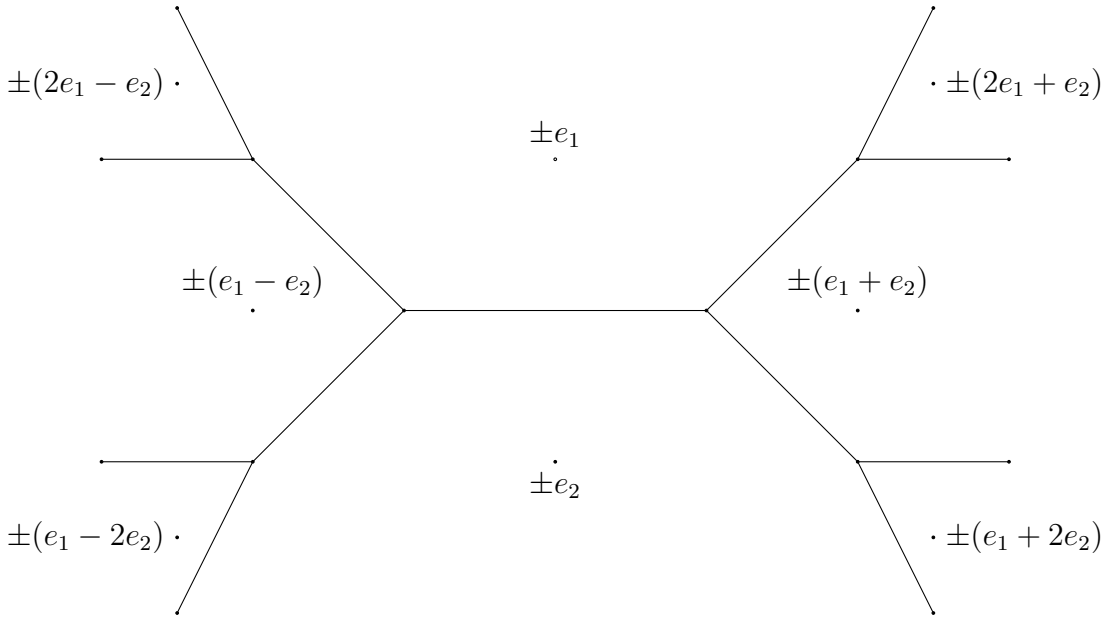


4.5 Topographe de Conway d'une forme quadratique binaire et automorphismes de topographes de Conway

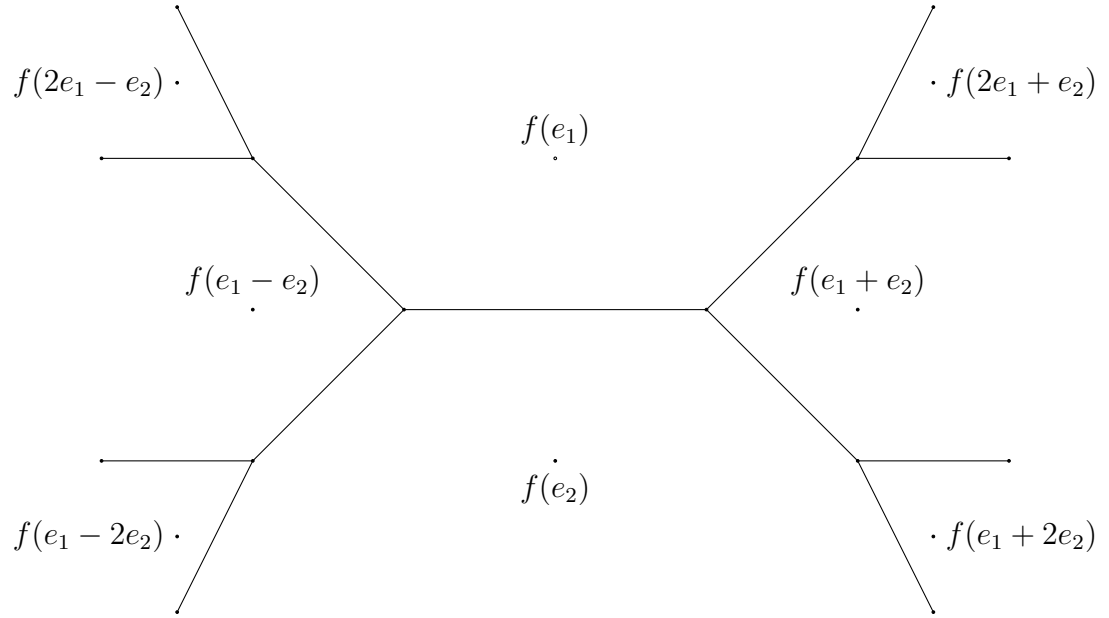
Les réseaux que nous considérons dans cette section sont tous de dimension deux.

Nous allons maintenant profiter de la structure avantageuse des représentations principales d'un topographe. Ces représentations nous permettent de définir les topographes de Conway.

Définition 4.41. *Soient Λ un réseau et T le topographe de ce réseau. Soit f une forme quadratique binaire sur Λ. Soit $\mathcal{R}$ une représentation principale du topographe T.*



Un ***topographe de Conway*** *de la forme quadratique binaire f est une représentation principale du topographe T auquel nous appliquons f aux vecteurs relâchés de ses arêtes et de ses sommets. Nous notons cette représentation $\mathcal{C}_{\mathcal{R},f}$.*

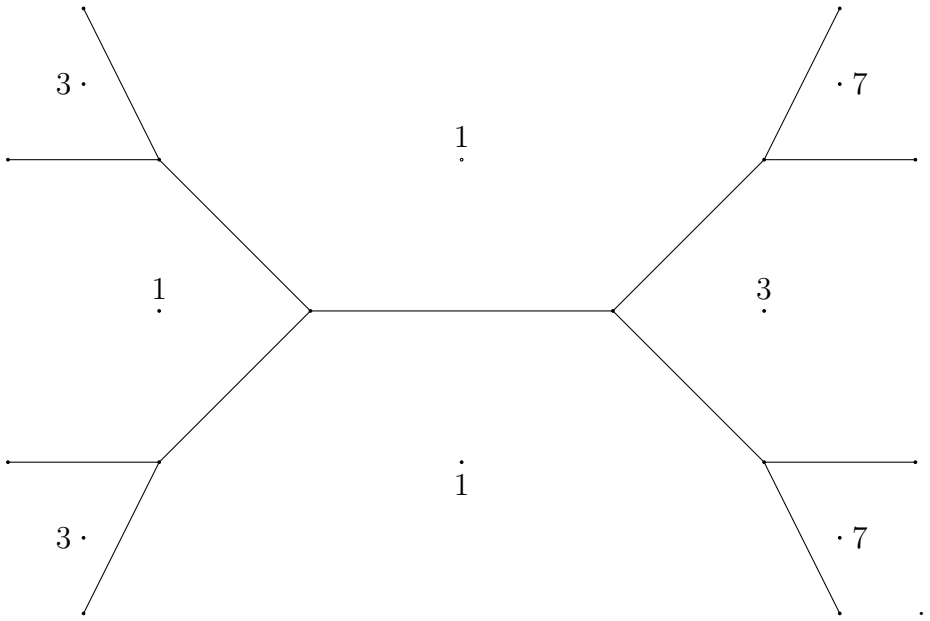


Nous donnons désormais un exemple d'un tel topographe de Conway.

Exemple 4.42. Soit Λ un réseau pour la base $\{e_1, e_2\}$ et soit f une forme quadratique binaire sur Λ telle que

$$f(e_1) = 1 \qquad ; \qquad f(e_1 + e_2) - f(e_1) - f(e_2) = 1 \qquad ; \qquad f(e_2) = 1.$$

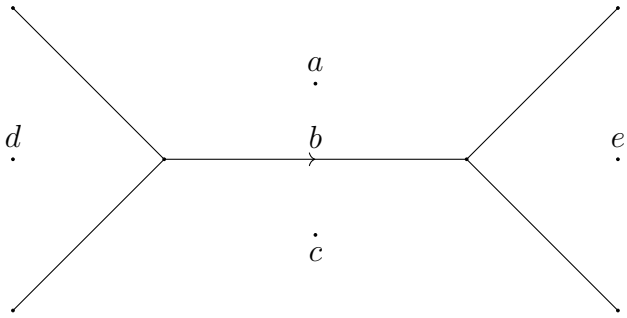
Cette forme quadratique binaire est la forme quadratique binaire $(1, 1, 1)$ dont nous avons déjà exploré les propriétés au chapitre précédent. Le topographe de Conway de la forme quadratique binaire $(1, 1, 1)$ est le graphe



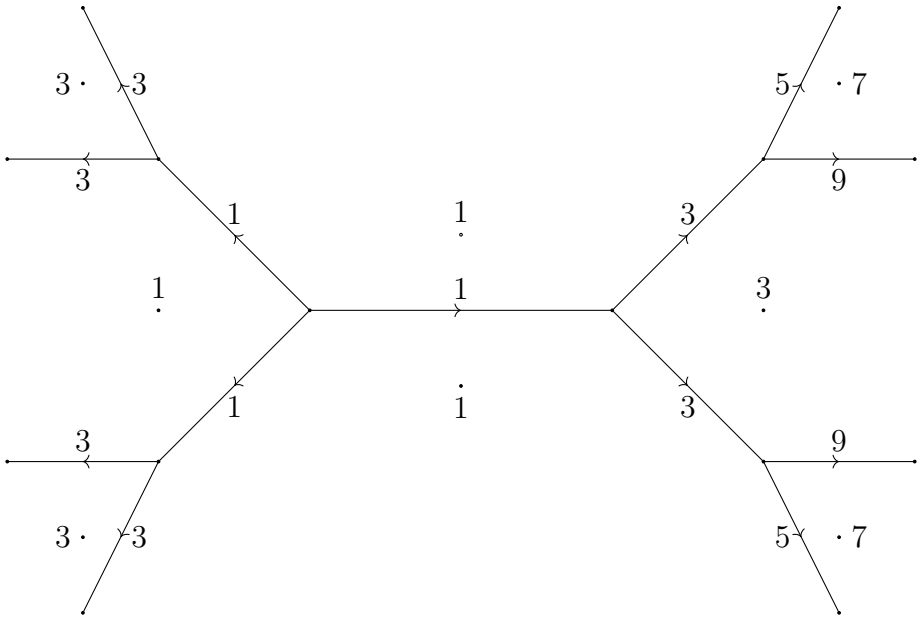
Les entiers apparaissant sur les différentes faces appartiennent donc à l'image de la forme quadratique binaire $(1, 1, 1)$. Ce sont en fait les entiers proprement représentés par la forme quadratique $(1, 1, 1)$.

Remarque 4.43. Les entiers représentés sur les topographes de Conway d'une forme quadratique binaire sont les entiers proprement représentés par cette forme quadratique binaire. Cela provient du fait que tous les vecteurs du topographe appartiennent à des bases et que chaque vecteur d'une base du réseau est dans son topographe au travers des bases relâchées.

Nous montrons désormais comment les topographes de Conway permettent de rendre les notations plus claires et surtout comment la règle de la progression arithmétique en est impactée. Il n'est plus nécessaire de noter les valeurs que prend la forme quadratique binaire sur chaque arête, celles-ci nous sont directement données par les notations 4.10 et 4.39 apportées aux faces. Dès lors, la règle de la progression arithmétique se visualise simplement dans le dessin suivant. Celui-ci indique que $a + b + c = e$ et $a + c - b = d$.



Donc, si nous reprenons la forme quadratique binaire $(1, 1, 1)$, nous obtenons cette partie de topographe de Conway.



D'ailleurs, puisque nos faces sont fixées, nous confirmons le commentaire fait dans la remarque 4.29. Sur chaque arête, nous pouvons considérer que nous avons placé une forme quadratique binaire (deux si nous ne considérons pas le sens de la flèche). L'arête centrale est la forme quadratique binaire $(1, 1, 1)$. Si nous suivons le chemin vers le nord-est, nous arrivons à la forme quadratique binaire $(1, 3, 3)$. En suivant le sens de la flèche, nous arrivons aux formes quadratiques binaires $(1, 5, 7)$ et $(7, 9, 3)$. Ces formes sont équivalentes parce que conceptuellement, nous n'avons fait qu'appliquer $(1, 1, 1)$ sur notre réseau, mais pour une autre base.

Nous passons désormais à la notion d'automorphisme. D'un point de vue purement géométrique, nous voulons que la notion d'automorphisme de topographe de Conway rejoigne celle d'isométrie du plan lorsque nous donnons assez de régularité à nos représentations principales. Si nous prenons le cas de la forme quadratique $(1, 1, 1)$, on remarque que des rotations de 120 degrés autour du sommet dont chaque arête est sortante

laisseraient le topographe de Conway inchangé. Cette observation sera approfondie dans la prochaine section 4.6. Afin de définir les automorphismes de topographes de Conway, nous aurons besoin de la définition d'automorphismes de graphes.

Définition 4.44. *Soit $G = (V, E)$ un graphe. Un **automorphisme** de G est une bijection $\psi : V \to V$ tel que pour toute arête $\{u, v\}$ de E, $\{\psi(u), \psi(v)\}$ est une arête de E.*

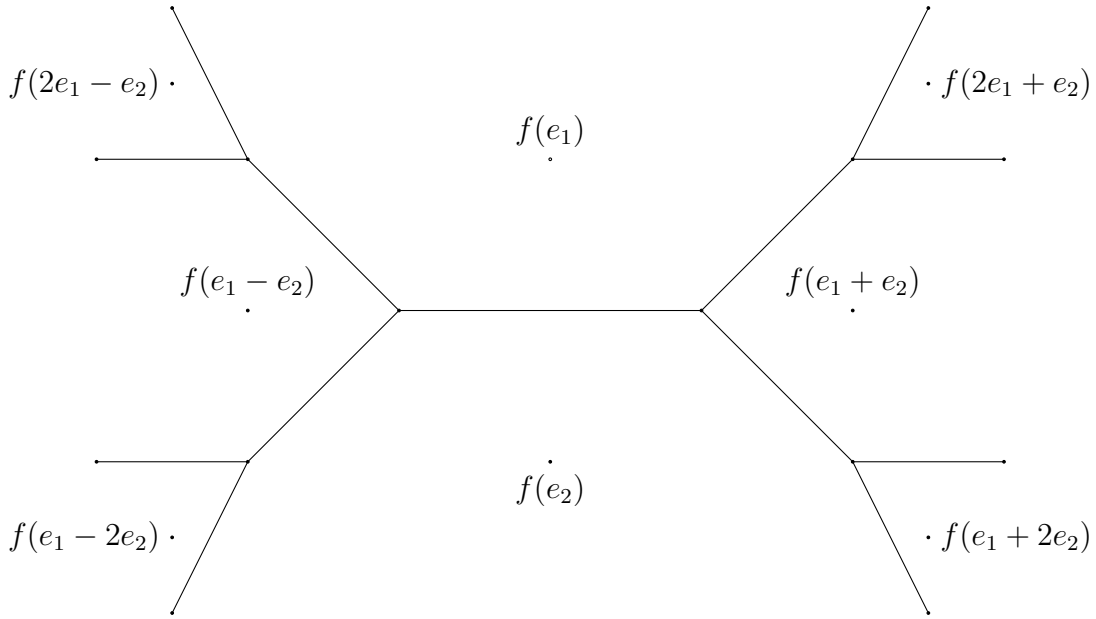
Il est clair qu'un automorphisme de graphe ne change pas le graphe. Par contre, il change sa représentation. Soient $G = (V, E)$ un graphe planaire, ψ un automorphisme de G et $\mathcal{R} = (G, i, \{\phi_e\}_{e \in E})$ une représentation de G. La représentation du graphe après l'application de l'automorphisme est $\mathcal{R}^\psi = (G, i \circ \psi, \{\phi_e\}_{e \in E})$. Les automorphismes de topographes qui nous intéressent sont ceux qui préservent la principalité des représentations.

Définition 4.45. *Soient Λ un réseau et T le topographe de ce réseau. Un automorphisme ψ de T est dit **principal** si pour toute représentation principal $\mathcal{R} = (G, i, \{\phi_e\}_{e \in E})$ de T, la représentation $\mathcal{R}^\psi = (G, i \circ \psi, \{\phi_e\}_{e \in E})$ est une représentation principale.*

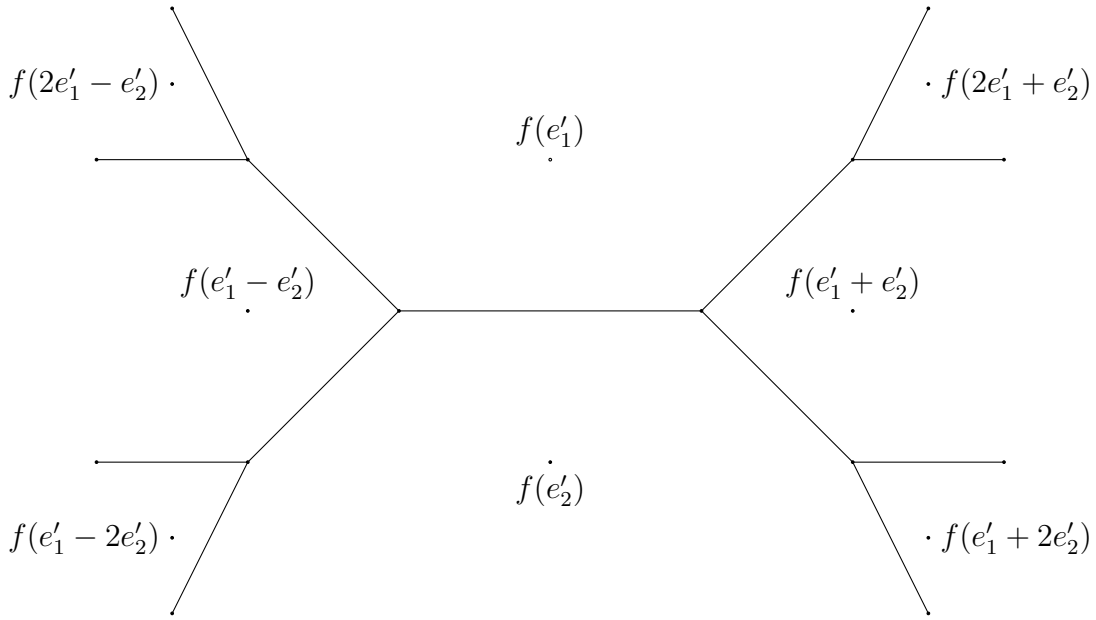
On remarque tout d'abord que l'ensemble des automorphismes principaux est non-vide puisqu'il contient l'identité. De plus, cet ensemble muni de la composition standard de morphismes de graphe est un groupe. Nous pouvons voir ce groupe comme un sous-groupe du groupe de permutations des faces de la représentation principale.

Nous allons désormais mettre en lien le comportement des topographes de Conway lorsque, pour une forme quadratique binaire f et une matrice M de $\mathrm{GL}_2(\mathbb{Z})$, nous appliquons $\alpha(f, M)$ aux vecteurs relâchés des arêtes et des sommets de la représentation principale plutôt que f.

Prenons un réseau Λ pour la base $\{e_1, e_2\}$, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et soit ψ un automorphisme principale de T. Nous dessinons le topographe de Conway de f.



Nous prenons désormais la représentation principale $\mathcal{R}^\psi$ et dessinons la même partie du plan mais pour le topographe de Conway $\mathcal{C}_{\mathcal{R}^\psi, f}$.



Nous avons donc les valeurs de f sur la super-base relâchée $\{\pm e'_1, \pm e'_2, \pm(e'_1 - e'_2)\}$. Cela définit une forme quadratique binaire équivalente g sur le réseau Λ, mais pour la base $\{e'_1, e'_2\}$. La permutation ψ induit donc une matrice M^ψ de $\mathrm{GL}_2(\mathbb{Z})$ transformant f en g. Cette observation nous conduit au théorème suivant.

Théorème 4.46. *Soit Λ un réseau pour la base $\{e_1, e_2\}$, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale et ψ un automorphisme principal. Alors, il existe une matrice M^ψ de $\mathrm{GL}_2(\mathbb{Z})$ telle que*

$$\mathcal{C}_{\mathcal{R}^\psi,f} = \mathcal{C}_{\mathcal{R},\alpha(f,M^\psi)}.$$

Démonstration. Au vu de la discussion précédente, nous devons montrer que la matrice M^ψ qui transforme la forme quadratique binaire

$$f(xe_1 + ye_2) = f(e_1)x^2 + B(e_1, e_2)xy + f(e_2)y^2$$

en la forme quadratique binaire

$$g(xe_1 + ye_2) = f(e_1')x^2 + B(e_1', e_2') + f(e_2')y^2$$

avec $B(e_1, e_2) = f(e_1 + e_2) - f(e_1) - f(e_2)$, induit l'égalité

$$\mathcal{C}_{\mathcal{R}^\psi,f} = \mathcal{C}_{\mathcal{R},\alpha(f,M^\psi)}.$$

La règle de la progression arithmétique nous assure que connaître la valeur d'une forme quadratique binaire sur une super-base relâchée suffit pour construire l'intégralité du topographe de Conway. Les deux topographes de Conway sont identiques puisque nous forçons le même sommet à avoir les mêmes valeurs grâce à l'équivalence. □

Ce théorème justifie notre définition d'automorphisme de topographe de Conway.

Définition 4.47. *Soit Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de f. Un automorphisme principal ψ est un* ***automorphisme du topographe de Conway*** *$\mathcal{C}_{\mathcal{R},f}$ si*

$$\mathcal{C}_{\mathcal{R}^\psi,f} = \mathcal{C}_{\mathcal{R},f}.$$

L'automorphisme identité Id *sera appelé automorphisme* ***trivial****.*

Proposition 4.48. *Soit Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T. Soit $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de f. L'ensemble des automorphismes du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ muni de leur composition usuelle et de l'automorphisme identité forment un groupe.*

Démonstration. Il nous suffit de regarder le comportement des automorphismes du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ sur une super-base relâchée du topographe T. En effet, nous savons qu'une représentation principale est entièrement déterminée par les vecteurs d'une super-base relâchée et la notation 4.39. Soient ϕ et ψ deux automorphismes du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$. Soit $\{\pm e_1, \pm e_2, \pm e_3\}$ une super-base relâchée de Λ. Disons que ϕ envoie le point $\{\pm e_1', \pm e_2', \pm e_3'\}$ sur la super-base relâchée $\{\pm e_1, \pm e_2, \pm e_3\}$ de sorte

que les faces $\pm e'_1, \pm e'_2, \pm e'_3$ soient envoyées respectivement sur les faces $\pm e_1, \pm e_2, \pm e_3$ de la représentation $\mathcal{R}$. Puisque ϕ est un automorphisme du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$, on déduit que $f(e_1) = f(e'_1)$, $f(e_2) = f(e'_2)$ et $f(e_3) = f(e'_3)$. Si nous effectuons le même procédé pour ψ, et envoyons les faces $\pm e''_1, \pm e''_2, \pm e''_3$ sur les faces $\pm e'_1, \pm e'_2, \pm e'_3$, alors nous constatons que $f(e'_1) = f(e''_1)$, $f(e'_2) = f(e''_2)$ et $f(e'_3) = f(e''_3)$. On déduit que $f(e_1) = f(e''_1)$, $f(e_2) = f(e''_2)$ et $f(e_3) = f(e''_3)$. L'utilisation de la règle de la progression arithmétique montre alors que

$$\mathcal{C}_{\mathcal{R}^{\psi\phi},f} = \mathcal{C}_{\mathcal{R},f}.$$

Donc, la composée de deux automorphismes du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est un automorphisme du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$.

L'inverse d'un automorphisme ψ du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est aussi un automorphisme du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ puisque si ψ envoie les faces $\pm e_1, \pm e_2, \pm e_3$ sur les faces $\pm e'_1, \pm e'_2, \pm e'_3$, alors $f(e_1) = f(e'_1)$, $f(e_2) = f(e'_2)$ et $f(e_3) = f(e'_3)$. On déduit donc par la règle de la progression arithmétique que

$$\mathcal{C}_{\mathcal{R}^{\psi^{-1}},f} = \mathcal{C}_{\mathcal{R},f}.$$

Cela conclut notre preuve. □

On déduit directement du théorème 4.46 le corollaire suivant.

Corollaire 4.49. *Soit Λ un réseau, T son topographe de Conway et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale et ψ un automorphisme de topographe de Conway. Alors, ψ induit un automorphisme de la forme quadratique binaire f.*

Démonstration. Par le théorème 4.46, il existe une matrice M^ψ telle que

$$\mathcal{C}_{\mathcal{R}^\psi,f} = \mathcal{C}_{\mathcal{R},\alpha(f,M^\psi)}.$$

Puisque ψ est un automorphisme de topographe de Conway, on déduit que

$$\mathcal{C}_{\mathcal{R},\alpha(f,M^\psi)} = \mathcal{C}_{\mathcal{R},f}$$

On remarque de cette dernière égalité que $\alpha(f, M^\psi)$ et f prennent les mêmes valeurs sur une super-base. Par conséquent, elles sont égales et on conclut que M^ψ est un automorphisme de forme quadratique binaire. □

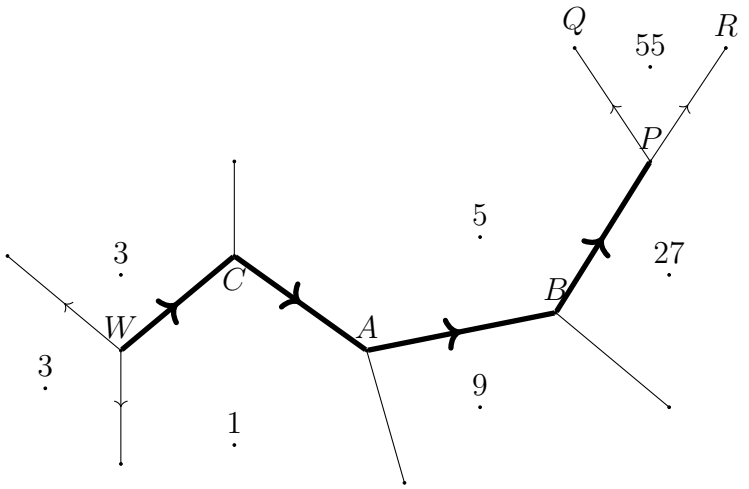
Nous pourrons donc déterminer des informations sur le groupe d'automorphismes d'une forme quadratique binaire juste en regardant les symétries de son topographe de Conway.

4.6 Puits de topographes de Conway et groupe d'automorphismes de formes quadratiques binaires définies positives

Les réseaux que nous considérons dans cette section sont tous de dimension deux.

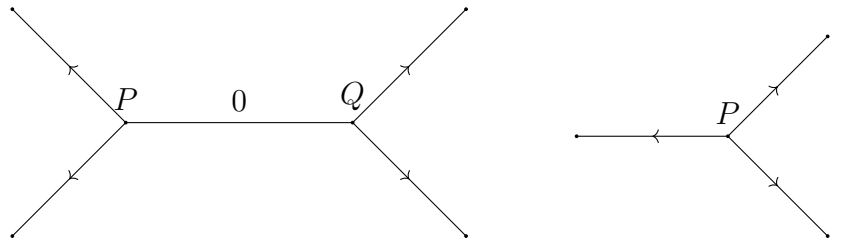
Jusqu'à présent, nous avons simplement représenté les valeurs d'une forme quadratique binaire sur un topographe. Nous allons désormais montrer les spécificités des formes quadratiques binaires définies positives et indéfinies. Dans le cas des formes quadratiques binaires définies positives, nous pourrons utiliser les résultats obtenus dans le chapitre 3 afin de donner une image concrète de leurs comportements. Cette image sera celle d'un puits. En ce qui concerne les formes quadratiques binaires indéfinies, nous verrons dans les prochaines sections que leur comportement est différent, mais pas moins intéressant puisque les images que nous pourrons leur associer seront celles d'un lac, d'une rivière voire les deux. Ces différentes images et leur nomenclature sont reprises et traduites par nos soins de la référence [6].

Nous commençons par le cas le plus simple : les formes quadratiques binaires définies positives. Nous savons par la section précédente que les topographes de Conway sont des arbres. Ils sont donc connexes. De plus, l'image d'une forme quadratique définie positive contient uniquement des entiers positifs. Nous prenons une partie d'un topographe de Conway.



Si nous partons du point P et remontons en allant dans le sens opposé des flèches, nous arrivons au sommet W. Celui-ci est tel que toutes ses arêtes sont orientés de façon à sortir de lui. Nous venons de découvrir ce que nous appellerons un puits simple. Il existe une autre variante que nous nommerons double puits. Nous définissons rigoureusement cette notion.

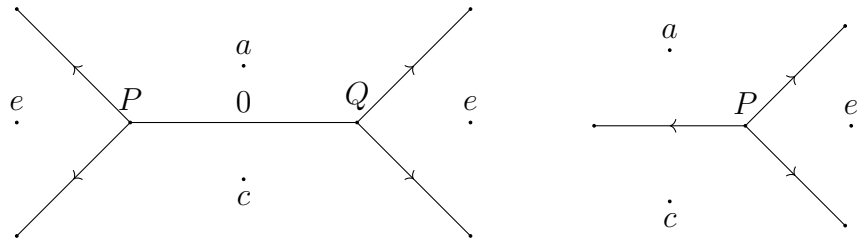
Définition 4.50. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway associé à la forme quadratique binaire f auquel nous avons orienté les arêtes en suivant la règle de la progression arithmétique. Un* ***puits simple*** *du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est un sommet P tel que chacune de ses arêtes est orientée de sorte à sortir du sommet P. Un* ***double puits*** *du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est une paire de sommets P et Q reliée par une arête 0 et tels que chaque autre arête est orientée pour sortir des sommets.*



Nous montrons ci-dessous que tout topographe de Conway d'une forme quadratique binaire définie positive admet un unique puits.

Proposition 4.51. *[11, Theorem 10.6 en p.262] Soient Λ un réseau, T son topographe et f une forme quadratique binaire définie positive pour ce réseau. Soit $\mathcal{R}$ une représentation principale de T. Alors, le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un unique puits que celui-ci soit simple ou double.*

Démonstration. Commençons par l'existence. Puisque f est définie positive, le topographe de Conway de f admet un entier minimal. Notons ce minimum par a. De tous les entiers adjacents à a sur le topographe de Conway de f, nous prenons l'entier le plus petit et nous le notons c. Il y exactement deux valeurs adjacentes à a et c. Nous notons e l'entier le plus petit des deux entiers adjacents à a et c. Puisque e est le plus petit entier des entiers adjacents à a et c, la règle de la progression arithmétique assure que l'autre entier adjacent à a et c est soit égal à e, soit plus grand. On se retrouve dans les situations suivantes.



Dans chaque cas, la règle de la progression arithmétique montre que les arêtes sont orientées pour sortir des sommets puisque $a \leq c \leq e$. Nous avons donc bien construit

un puits simple ou un double puits pour une forme quadratique binaire définie positive quelconque.

Nous allons désormais montrer que le puits est unique qu'il soit double ou simple. Supposons par l'absurde qu'il existe deux puits de quelconque nature au sein d'un même topographe de Conway. Alors, puisque tout topographe de Conway est un arbre, il existe un unique chemin reliant le(s) sommet(s) de chacun des puits. Or, par le lemme 4.31, la dernière arête menant à l'un des sommets du puits devrait être orientée de sorte à rentrer dans le puits. Par définition, cela est impossible. Par conséquent, nous avons montré que le puits est unique. □

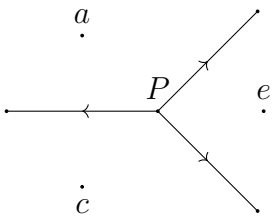
Remarque 4.52. Ce comportement particulier des topographes de Conway des formes quadratiques binaires définies positives n'est pas anodin. En réalité, c'est la notion de forme quadratique binaire réduite qui est à l'oeuvre ici. On remarque cela dans la construction même des puits : nous prenons l'entier le plus petit représenté par la forme quadratique binaire. La proposition 3.32 du chapitre 3 montrait déjà très bien l'importance de cette valeur dans la réduction d'une forme quadratique binaire définie positive. Il n'est donc pas étrange de retrouver ici cette analogie.

Regardons désormais comment nous pouvons tirer parti de la structure de puits pour déterminer le nombre d'automorphismes d'une forme quadratique binaire. Nous sommes désormais en mesure de déterminer, en regardant le topographe de Conway d'une forme quadratique binaire définie positive, le nombre d'automorphismes que celle-ci admet. Nous avons montré dans la proposition 4.51 qu'une forme quadratique binaire définie positive n'admet qu'un unique puits. Par conséquent, un automorphisme de topographe de Conway envoie un puits sur lui-même. Ce simple fait a les conséquences suivantes.

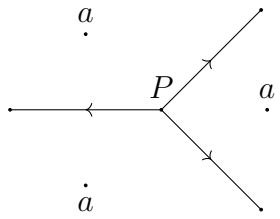
Théorème 4.53. *[11, Theorem 10.18 en p.270] Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de f. Nous avons les deux cas suivants :*

1. *si $\mathcal{C}_{\mathcal{R},f}$ admet un puits simple et un automorphisme ne stabilisant aucune face du puits, alors f est équivalente à un multiple de la forme quadratique binaire $(1,1,1)$;*
2. *si $\mathcal{C}_{\mathcal{R},f}$ admet un double puits et un automorphisme ne stabilisant aucune face du puits, alors f est équivalente à un multiple de la forme quadratique binaire $(1,0,1)$.*

Démonstration. Nous commençons par le premier cas. Admettons que $\mathcal{C}_{\mathcal{R},f}$ ait un puits simple et un automorphisme ne stabilisant aucune face du puits.

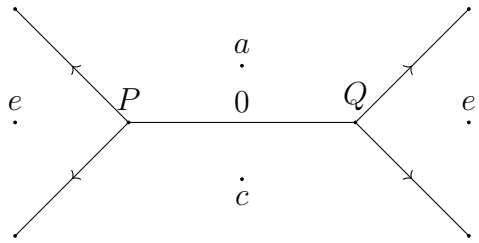


D'un point de vue purement visuel, puisque le puits est envoyé sur lui-même, cela correspond à une rotation de 120 degrés des faces soit dans le sens horlogique, soit dans le sens trigonométrique. Or, puisque le puits est envoyé sur lui-même, les entiers a, c et e doivent être égaux.



On déduit par la règle de la progression arithmétique que la forme quadratique binaire correspondante est équivalente à (a, a, a), i.e. un multiple de la forme quadratique binaire $(1, 1, 1)$. Pour une preuve plus rigoureuse, mais de facto moins visuelle, nous pouvons simplement considérer les arêtes comme des bases relâchées. L'automorphisme envoie chacune des arêtes sur une autre. Puisque les arêtes se doivent de rester les mêmes si nous appliquons f aux vecteurs de leur base relâchée associée, on déduit que $a = f(e_1) = f(e_2) = f(e_1 - e_2)$ et en utilisant la règle de la progression arithmétique que la forme f est bien équivalente à (a, a, a).

Supposons désormais que le puits soit double. Les seuls automorphismes sont représentés par des rotations de 180 degrés des faces. En effet, si nous faisons une rotation de 90 degrés, alors nécessairement $a = e = c$ et la règle de la progression arithmétique nous dit que $a = c = 0$. Par conséquent, la forme quadratique binaire f serait équivalente à $(0, 0, 0)$ qui n'est pas définie positive.



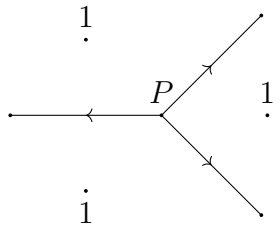
On déduit que $a = c$ et la forme quadratique binaire associée à ce topographe est équivalente à la forme quadratique binaire $(a, 0, a)$, ce qui conclut notre preuve. Une preuve plus rigoureuse revient une fois de plus à considérer les arêtes comme des bases relâchées et d'appliquer f sur les vecteurs de celles-ci. □

Nous avons donc déterminé, à partir du topographe de Conway, une propriété générale sur les formes quadratiques binaires. Nous verrons par la suite que les formes quadratiques binaires définies positives ne sont pas les seules à jouir de ce genre de propriétés.

Nous identifions désormais le groupe d'automorphisme d'un topographe de Conway de la forme quadratique binaire $(1, 1, 1)$.

Proposition 4.54. *Soit Λ un réseau pour une base $\{e_1, e_2\}$ et T son topographe. Soit $\mathcal{R}$ une représentation principale de T. Posons la forme quadratique binaire $f = (1, 1, 1)$. Le groupe d'automorphismes du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est isomorphe au groupe de permutation d'un ensemble à trois éléments S_3.*

Démonstration. Il nous suffit de regarder le comportement du topographe autour de son puits.



Pour une démonstration géométrique, nous voyons que les réflexions du topographe de Conway autour des arêtes sortantes du puits laissent le topographe inchangé. Ces éléments sont d'ordres deux. De plus, nous voyons que des rotations centrées en P d'angle 120 degrés et -120 degrés préservent aussi le topographes de Conway. Ces éléments sont d'ordre trois. Puisque le puits est nécessairement envoyé sur lui-même, ces isométries du plan et l'identité sont les seules isométries acceptables. Par conséquent, le groupe d'automorphismes de $\mathcal{C}_{\mathcal{R},f}$ est bien S_3. Pour une preuve ne nécessitant l'utilisation de la régularité de la représentation, la preuve revient à interchanger les arêtes. Puisque les arêtes sortantes du puits son identiques, il n'y a pas de restriction sur les changements d'arêtes et on conclut que le groupe d'automorphisme de ce topographe de Conway est le groupe de permutation d'un ensemble à trois éléments, c'est-à-dire S_3. □

Remarque 4.55. Dans le premier chapitre de la référence [6], J. Conway mentionne en p.22 que nous pouvons «voir» le groupe d'automorphismes [3] d'une certaine forme quadratique binaire indéfinie en déterminant les isométries de son topographe de Conway. Sa formulation est ambiguë et le lien entre les automorphismes de topographes de Conway et les automorphismes de formes quadratiques binaires reste assez obscur étant donné qu'il ne développe pas sur ce point. Dans tous les cas, la propriété précédente montre qu'il n'y pas d'isomorphisme entre ces deux groupes puisque nous avions montré dans la proposition 3.55 que le groupe d'automorphismes de $(1, 1, 1)$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Une étude plus poussée de ce lien pourrait donner des résultats intéressants sur les deux notions.

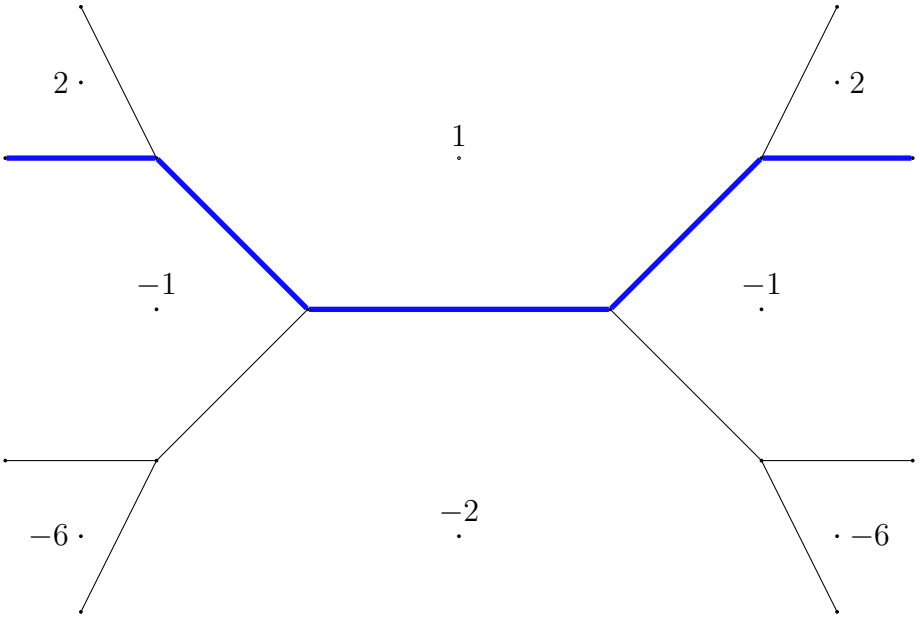
3. Ici, le groupe d'automorphisme comprend les matrices de déterminant négatif ce qui n'est pas le cas dans notre définition 3.50.

La prochaine section traitera du cas des formes quadratiques binaires indéfinies ne représentant pas 0.

4.7 Rivières de topographes de Conway et formes quadratiques binaires indéfinies ne représentant pas zéro

Les réseaux que nous considérons dans cette section sont tous de dimension deux.

Nous allons désormais nous intéresser aux formes quadratiques binaires indéfinies dont le discriminant n'est pas un carré. Nous commençons par aborder la notion de rivière. Une rivière sur un topographe de Conway est une suite d'arêtes chacune séparant une face positive et une face négative. Prenons, par exemple, la forme quadratique binaire $f(xe_1 + ye_2) = x^2 - 2y^2$ pour un réseau Λ muni de la base $\{e_1, e_2\}$. Représentons une partie de son topographe de Conway. Nous représentons la rivière via l'ajout d'une ligne grasse en bleu.

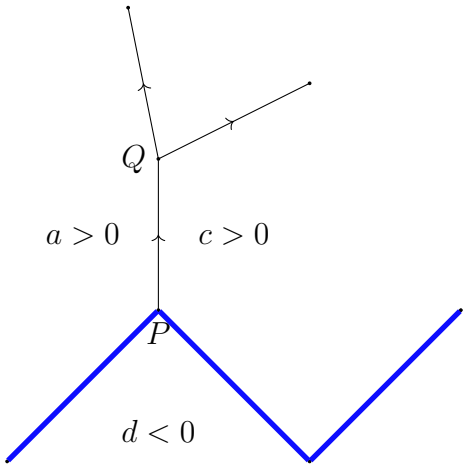


Définition 4.56. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soient $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Une suite d'arêtes du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est une* ***rivière*** *si chaque arête sépare une face positive d'une face négative.*

Nous aurons par la suite besoin du lemme suivant qui est une conséquence directe du lemme 4.31 appliqué à la théorie des rivières.

Lemme 4.57. *[6, en p.20] Soient Λ un réseau, T son topographe et f une forme quadratique binaire indéfinie sur ce réseau. Soient $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f admettant une rivière. Les chemins sortant de la rivière longent des faces dont les valeurs augmentent en valeur absolue.*

Démonstration. Prenons une rivière arbitraire.

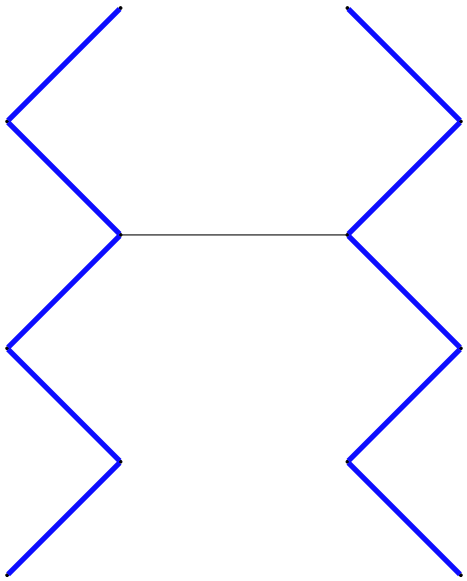


Disons sans perte de généralité que l'arête PQ sépare des faces positives. Alors, puisque les faces de l'autre côté de la rivière sont négatives, nous déterminons que l'orientation de l'arête PQ sort de P pour aller vers Q. Nous déduisons qu'en suivant le chemin commençant à l'arête PQ, les valeurs des faces augmentent par le lemme 4.31. De façon similaire, si nous suivons un chemin partant dans les faces négatives, celles-ci continueront de prendre des valeurs de plus en plus basses. Nous déduisons donc les valeurs augmentent en valeur absolue plus nous nous éloignons d'une rivière. □

Théorème 4.58. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire indéfinie sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T. Alors, tout topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ de la forme quadratique binaire f admet une unique rivière.*

Démonstration. L'existence est triviale puisque la forme quadratique binaire f admet des entiers positifs et négatifs dans son image. Le topographe de Conway étant connexe, il existe un chemin reliant une face positive à une face négative. Ce chemin entre en contact avec des faces positives et négatives. Par conséquent, il existe au moins une arête séparant une face positive d'une face négative.

Nous montrons désormais son unicité. Supposons qu'il existe deux rivières distinctes au sein d'un même topographe de Conway. Alors, puisque le topographe de Conway de contient pas de cycle, il existe un unique chemin les reliant.

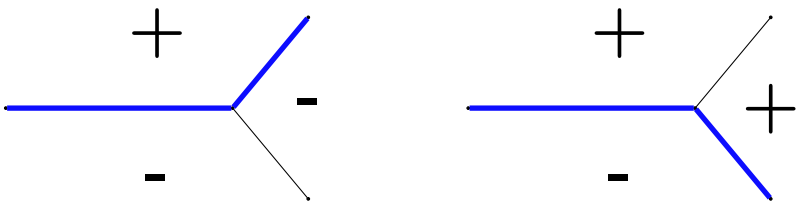


Partons de la rivière de gauche sur le dessin et suivons le chemin en noir qui nous guide vers la rivière de droite. La valeur absolue des valeurs que nous rencontrerons sera de plus en plus grande grâce au lemme 4.57. Cependant, cela est une contradiction puisque ces valeurs absolues devraient décroître en arrivant vers la rivière de droite par le lemme 4.57. On déduit qu'il n'existe qu'une seule rivière, concluant notre preuve. □

Nous donnons désormais une précision sur la taille d'une rivière d'un topographe de Conway d'une forme quadratique binaire ne représentant pas proprement l'entier 0.

Lemme 4.59. *[11, Proposition 11.6 en p.284] Soient Λ un réseau, T son topographe et f une forme quadratique binaire indéfinie ne représentant pas proprement l'entier 0 sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. La rivière du topographe de Conway T_f est infinie, i.e. la suite d'arêtes constituant la rivière est infinie.*

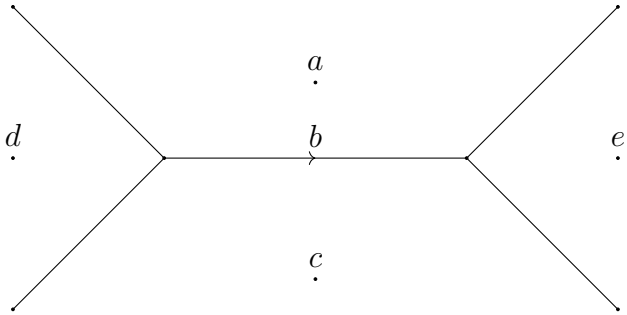
Démonstration. Pour démontrer ce résultat, on prend un bout de rivière et on regarde les différentes possibilités.



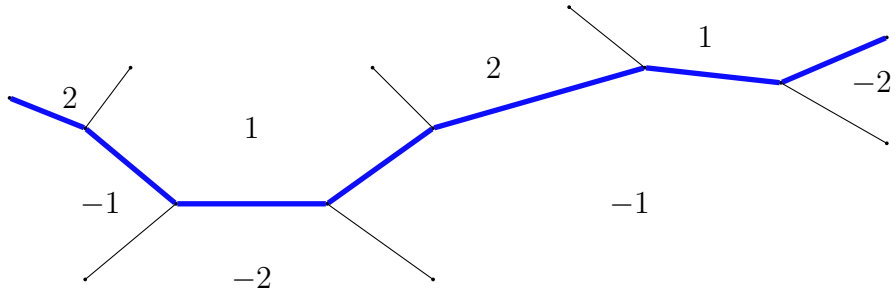
Puisque f ne représente jamais proprement l'entier 0, la rivière ne passe jamais par une face nulle. Par conséquent, elle continue indéfiniment. □

Remarque 4.60. Nous verrons que les formes quadratiques binaires représentant proprement l'entier 0 ont des propriétés différant quelque peu de celles ne représentant pas proprement l'entier 0. Essentiellement, une rivière pourra s'arrêter sur une face 0. Nous nommerons ces faces des "lacs".

Nous allons désormais pouvoir donner des précisions les automorphismes des topographes de Conway des formes quadratiques binaires indéfinies ne représentant pas l'entier 0. Plus précisément, nous allons voir que les faces longeant les rivières prennent des valeurs de façon périodique. Pour ce faire, nous rappelons qu'une forme quadratique binaire est entièrement déterminée par les valeurs qu'elle prend sur une super-base relâchée d'un réseau Λ. De plus, le coefficient b d'une forme quadratique binaire (a, b, c) est l'entier donnant l'orientation de l'arête séparant les faces a et b



Lorsque nous nous déplaçons d'arêtes en arêtes, nous passons de formes quadratiques binaires en formes quadratiques binaires équivalentes. De facto, les discriminants des formes quadratiques binaires sur lesquelles nous arrivions sont tous identiques. Cette observation a des implications sur les formes quadratiques binaires se situant sur une rivière. Reprenons la forme quadratique $f(xe_1 + ye_2) = x^2 - 2y^2$ pour un réseau Λ muni de la base $\{e_1, e_2\}$. Longeons la rivière assez longtemps pour remarquer la périodicité.



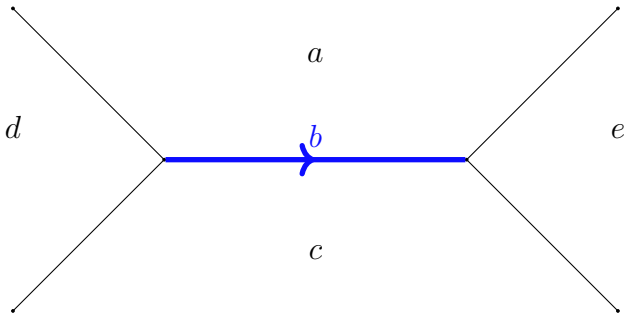
On remarque que les faces positives alternent entre les valeurs 1 et 2 tandis que les valeurs négatives alternent entre -1 et -2. Ce comportement est assez général et est propre aux formes quadratiques binaires indéfinies.

Théorème 4.61. *[6, en p.21] Soient Λ un réseau, T son topographe et f une forme quadratique binaire indéfinie. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Alors, il n'existe qu'un nombre fini de valeurs possibles pour les faces longeant la rivière et celles-ci apparaissent de façon périodique.*

Démonstration. Nous commençons par montrer que le nombre de valeurs possiblement prises par une des faces longeant la rivière est fini. Pour ce faire, reprenons la formule de discriminant d'une forme quadratique binaire. Nous savons que pour une forme quadratique binaire (a, b, c), son discriminant vaut

$$d = b^2 - 4ac.$$

De plus, les formes quadratiques binaires que nous considérons sont indéfinies et donc de discriminant positif. Si nous suivons une rivière, nous voyons que les coefficients a et c sont de signe opposé.



On déduit que $ac < 0$ et $|b| < d$. De plus, $d = |b|^2 + 4|ac|$ et par conséquent, on remarque que $0 < |ac| \leq \frac{d}{4}$. Par conséquent, il n'existe qu'un nombre fini de coefficients entiers a, b et c tels que $d = b^2 - 4ac$.

Nous montrons désormais que la rivière est périodique. Puisqu'il n'existe qu'un nombre fini de coefficients possibles pour les faces longeant la rivière, il n'existe qu'un nombre fini de formes quadratiques binaires pouvant être sur la rivière. Notons X l'ensemble des formes quadratiques binaires apparaissant sur une arête de la rivière de $\mathcal{C}_{\mathcal{R},f}$. Nous savons que X est un ensemble fini. De plus, fixer une forme quadratique binaire sur une arête suffit à construire l'intégralité du topographe de Conway. Par conséquent, fixer une arête revient à se donner un élément τ du groupe de permutations des éléments de X et se déplacer sur une arête adjacente sur la rivière revient à appliquer τ sur la forme quadratique binaire. Puisque X est un ensemble fini, le groupe de permutations est d'ordre fini et il en va de même pour l'élément τ. Par conséquent, il existe un naturel n tel que $\tau^n = \mathrm{Id}$. Nous déduisons donc que les formes quadratiques binaires sur les arêtes de la rivière apparaissent de façon périodique. □

Puisque les faces adjacentes aux rivières prennent des valeurs de façon périodique, cela montre que si un entier est proprement représenté, alors il est représenté proprement une infinité de fois. Cela vaut aussi dans le contexte de simples représentations.

Corollaire 4.62. *[11, Corollary 11.14 en p.286] Soient Λ un réseau, T son topographe et f une forme quadratique binaire indéfinie ne représentant pas proprement l'entier 0. Soit n un entier représenté par f. Alors, il existe une infinité d'éléments r du réseau Λ tels que $f(r) = n$.*

Démonstration. Afin de démontrer ce corollaire, nous allons montrer que celui-ci vaut si nous considérons un entier proprement représenté n. Au vu du lemme 3.9, cela suffira pour démontrer le résultat. Puisque la rivière est périodique, Les mêmes valeurs se répètent périodiquement dans le topographe de Conway de f. De là, le lemme 4.59 assure que la rivière d'un topographe de Conway d'une forme quadratique binaire indéfinie ne représentant pas proprement l'entier 0 est infinie. On déduit que la face dotée de la valeur n apparaît une infinité de fois ce qui est suffisant pour conclure. □

Remarque 4.63. Ce corollaire est à mettre en perspective avec la théorie des automorphismes de formes quadratiques binaires que nous avions mis en place dans la section 3.6 au chapitre 3 dans le cas des formes quadratiques binaires définies positives. Dans le cas des discriminants positifs, nous pouvons toujours montrer que le nombre de classes propres est fini. Par conséquent, le théorème 3.52 peut être adapté afin de montrer que le groupe d'automorphismes des formes quadratiques binaires indéfinies ne représentant pas zéro est infini. S'il n'est pas clair que la théorie des automorphismes de topographes de Conway donnent des informations précises sur le groupe d'automorphismes des formes quadratiques binaires indéfinies ne représentant pas zéro, elle donne tout de même une bonne intuition du comportement de celui-ci.

Nous déterminerons dans la prochaine section le comportement des formes quadratiques binaires semi-définies, i.e. des formes quadratiques binaires de discriminant égal à zéro.

4.8 Lacs de topographes de Conway et formes quadratiques binaires semi-définies et indéfinies représentant zéro

Les réseaux que nous considérons dans cette section sont tous de dimension deux.

Nous commençons par donner la définition d'une forme quadratique binaire semi-définie. Nous scindons ces formes quadratiques binaires en deux cas. Les formes quadratiques binaires semi-définies positives et négatives.

Définition 4.64. *Soit Λ un réseau et f une forme quadratique binaire sur ce réseau.*

La forme quadratique binaire f est dite ***semi-définie positive*** *si elle représente uniquement des entiers positifs et s'il existe un élément non trivial r du réseau Λ tel que $f(r) = 0$.*

La forme quadratique binaire f est dite ***semi-définie négative*** *si elle représente uniquement des entiers négatifs et s'il existe un élément non trivial r du réseau Λ tel que $f(r) = 0$.*

Le fait que ces formes quadratiques binaires représentent l'entier zéro pour des éléments non nuls donne beaucoup d'informations sur leur comportement. Plus spécifiquement, nous allons montrer à partir du topographe de Conway de telles formes quadratiques binaires qu'elles sont toutes équivalentes à une forme quadratique binaire du type $(a, 0, 0)$ pour un entier a. De plus, nous montrerons qu'elles ont toutes un discriminant égal à zéro.

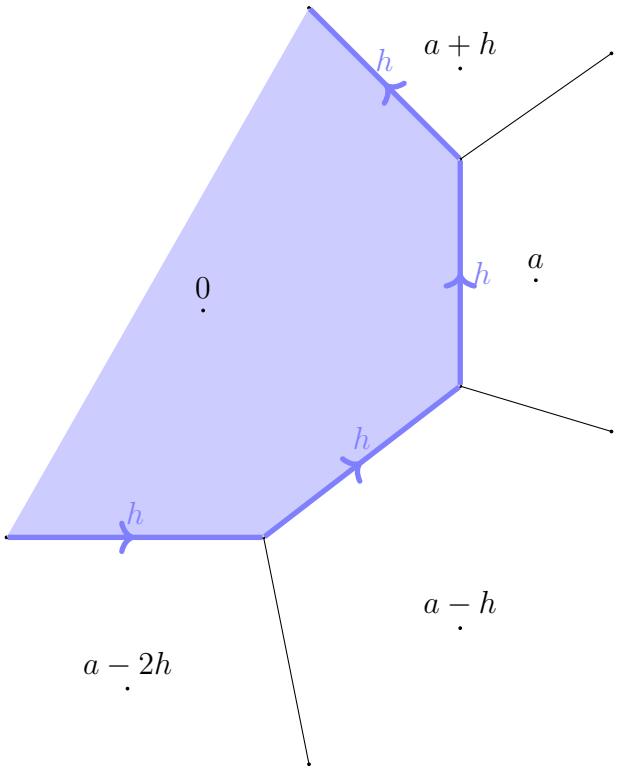
Nous définissons dans un premier temps le terme de «lac».

Définition 4.65. *[6, Semidefinite forms en p.23] Soit Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de ce topographe et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Un* ***lac*** *est une face du la représentation $\mathcal{C}_{\mathcal{R},f}$ étiqueté par l'entier zéro.*

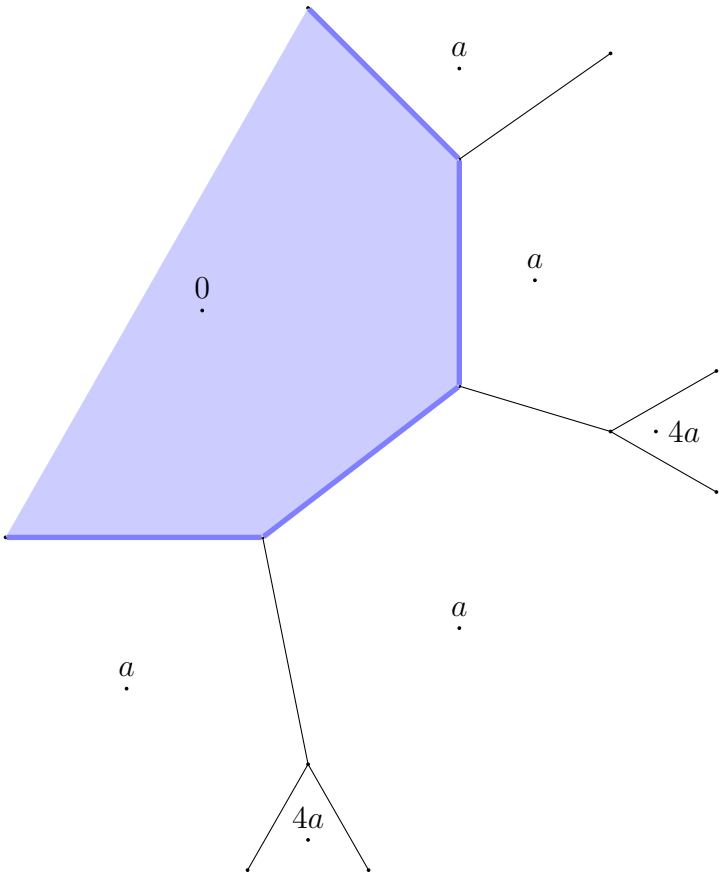
Théorème 4.66. *Soit Λ un réseau, T son topographe et f une forme quadratique binaire semi-définie sur ce réseau. Soit $\mathcal{R}$ une représentation principale de ce topographe et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Alors, le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un unique lac.*

Démonstration. Nous commençons par l'existence. Puisque les formes quadratiques binaires semi-définies admettent une représentation non triviale de zéro, elles en admettent une représentation propre par le lemme 3.9. Par conséquent, une face du topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ est étiquetée par l'entier zéro. L'unicité découle du lemme 4.31. Nous savons que s'éloigner du lac augmentera en valeur absolue les valeurs des faces. Par conséquent, il ne peut exister un autre lac sous peine que la valeur absolue des valeurs de ces faces diminue. Cela conclut notre preuve. □

Nous pouvons donc à partir de ce résultat donner un exemple de topographe de Conway.



On constate dans un premier temps que toutes les arêtes doivent porter les mêmes valeurs. En effet, cela provient de la règle de la progression arithmétique. Si nous prenons une face a avec a un entier positif et que nous suivons l'orientation de l'arête, nous arrivons à la face $a+h$. Celle-ci est positive et $a+h$ est supérieur à a. Par conséquent, toujours par la règle de la progression arithmétique, on déduit que l'arête séparant la face $a+h$ du lac doit être étiquetée par h. De plus, les formes quadratiques binaires définies positives ne représentent que des entiers positifs et zéro, h doit nécessairement être égal à zéro sous peine d'avoir des faces négatives autour du lac. On déduit donc que les topographes de Conway ont la forme suivante,



Ces observations nous donne le corollaire suivant.

Corollaire 4.67. *Soit Λ un réseau et f une forme quadratique binaire semi-définie sur ce réseau. Alors, f est équivalente à une forme quadratique binaire du type $(a, 0, 0)$ pour un entier a.*

Démonstration. On regarde un topographe de la forme quadratique binaire f. Les formes quadratiques binaires sur les arêtes longeant le lac sont de la forme $(a, 0, 0)$. On en déduit le résultat par la remarque 4.29. □

On en déduit aussi le corollaire suivant concernant le discriminant de telles formes quadratiques binaires.

Corollaire 4.68. *Soit Λ un réseau pour une base $\{e_1, e_2\}$ et f une forme quadratique binaire sur ce réseau. La forme quadratique binaire f est semi-définie si et seulement si son discriminant est nul.*

Démonstration. Si f est une forme quadratique binaire semi-définie, alors elle est équivalente à une forme quadratique binaire du type $(a, 0, 0)$ par le corollaire 4.67. Par conséquent, son discriminant est égal à zéro puisque deux formes quadratiques binaires équivalentes partagent le même discriminant par la proposition 3.13.

Réciproquement, si $f = (a, b, c)$ admet un discriminant nul, alors nous remarquons que $b^2 = 4ac$. La forme quadratique binaire f peut donc s'écrire comme

$$f(xe_1 + ye_2) = ax^2 + bxy + \frac{b^2}{4a}y^2$$

pour $xe_1 + ye_1$ un élément de Λ. Nous remarquons que

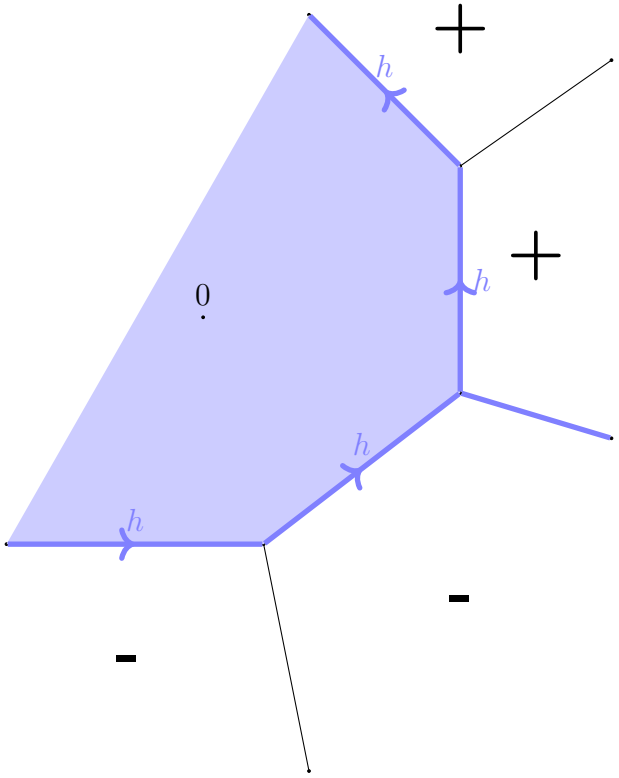
$$ax^2 + bxy + \frac{b^2}{4a}y^2 = a(x + \frac{b}{2a}y)^2.$$

Par conséquent, la forme quadratique binaire f représente zéro. Par exemple au point de coordonnées $(-b, 2a)$. On déduit l'existence d'un lac dans les topographes de f. De plus, on remarque que f n'admet dans son image que des entiers positifs ou négatifs (dépendamment du signe de a) et l'entier zéro. Nous avons donc montré que f est semi-définie. □

Nous passons désormais à l'analyse des formes quadratiques indéfinies représentant zéro. Nous commençons par un lemme concernant le comportement des rivières. De façon générale, une rivière est soit infinie, soit elle commence et se termine en se jetant dans un lac.

Théorème 4.69. *[11, Proposition 11.6 en p.284] Soient Λ un réseau, T son topographe et f une forme quadratique binaire indéfinie représentant proprement l'entier 0 sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Alors, la rivière commence et prend fin dans un lac.*

Démonstration. Si la forme quadratique binaire f représente l'entier zéro, alors, le lemme 4.66 assure que le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un lac.



en suivant les arêtes longeant le lac, nous allons tomber sur une arête sortant du lac séparée par une face positive et une face négative. Par conséquent, nous venons de trouver le début de la rivière. Par le le théorème 4.61, nous savons que les faces longeant la rivière sont en nombre fini et qu'elles apparaissent de façon périodique. Par conséquent, si nous suivons la rivière, nous allons nous retrouver sur une face zéro et donc un lac. □

Nous sommes désormais en mesure d'énoncer et de démontrer un théorème de classification des formes quadratiques binaires en fonction de leurs topographes de Conway. Ce théorème sera le sujet de la prochaine section.

4.9 Théorème de classification des formes quadratiques binaires

Les réseaux que nous considérons dans cette section sont tous de dimension deux.

Pour conclure ce chapitre, nous allons donner un théorème de classification des formes quadratiques binaires en fonction de leurs topographes de Conway. Les différentes structures de topographes de Conway que nous avons analysé sont en fait liées au discriminant des formes quadratiques binaires.

Théorème 4.70 (Caractérisation des formes quadratiques binaires)**.** *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Alors,*

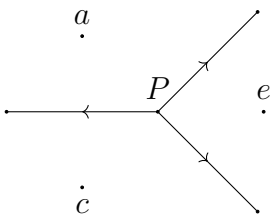
1. *le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un puits si et seulement si le discriminant de f est négatif et f est définie positive ;*
2. *le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet une rivière infinie si et seulement si le discriminant de f est positif et non-carré ;*
3. *le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un unique lac si et seulement si le discriminant de f est nul ;*
4. *le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet deux lacs si et seulement si le discriminant de f est positif et carré ;*
5. *le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ n'admet que des lacs si et seulement si f est la forme quadratique binaire triviale.*

Nous allons démontrer ce théorème au travers de plusieurs propositions. Nous démontrons les assertions dans leur ordre d'apparition.

Proposition 4.71. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un puits si et seulement si le discriminant de f est négatif et f est définie positive.*

Démonstration. [4] Si f est définie positive, la proposition 4.51 indique que $\mathcal{C}_{\mathcal{R},f}$ admet un puits.

Supposons désormais que $\mathcal{C}_{\mathcal{R},f}$ admette un puits simple ou double.



Alors, nous déduisons que $c \leq a + e$ et nous arrivons à l'inégalité

$$0 \leq c - e \leq a.$$

En mettant le tout au carré, nous obtenons l'inégalité

$$0 \leq c^2 - 2ce + e^2 \leq a^2.$$

4. La deuxième partie de cette preuve peut être trouvée dans la référence [11] la proposition 10.8 en p.264

Au vu du corollaire 4.14, le discriminant d de f vaut

$$\begin{aligned} d = (e-a-c)^2 - 4ac &= a^2 + 2ac + c^2 - 2ae - 2ce + e^2 - 4ac \\ &= a^2 - 2ac + c^2 - 2ce + e^2 - 2ae. \end{aligned}$$

L'inégalité précédente nous permet de dire que

$$d \leq a^2 + a^2 - 2ac - 2ae \leq 2a(a - (c+e)).$$

Par la règle de la progression arithmétique, nous savons aussi que $a \leq c + e$. Par conséquent, $a - c - e$ est négatif et nous déduisons que d est négatif. Par conséquent f est définie positive. □

Remarque 4.72. Cette proposition rend compte que la théorie de la réduction développée dans la section 3.4 au chapitre 3 est une particularité des formes définies positives. Les autres types de formes quadratiques binaires n'admettent pas de théorie de la réduction aussi efficace que celle des formes quadratiques binaires définies positives.

Nous démontrons désormais la deuxième assertion. Pour ce faire, nous aurons besoin du lemme suivant.

Lemme 4.73. *[11, proposition 11.2 en p.282] Soit Λ un réseau pour la base $\{e_1, e_2\}$ et $f = (a, b, c)$ une forme quadratique binaire de discriminant d carré. Alors, f représente l'entier 0.*

Démonstration. Supposons que $d = b^2 - 4ac$ soit un carré. Si $a = 0$, alors $f(0e_1 + 1e_2) = 0$. Si $a \neq 0$, alors nous évaluons f sur l'élément $(\sqrt{d} - b)e_1 + 2ae_2$ du réseau Λ. On calcule que

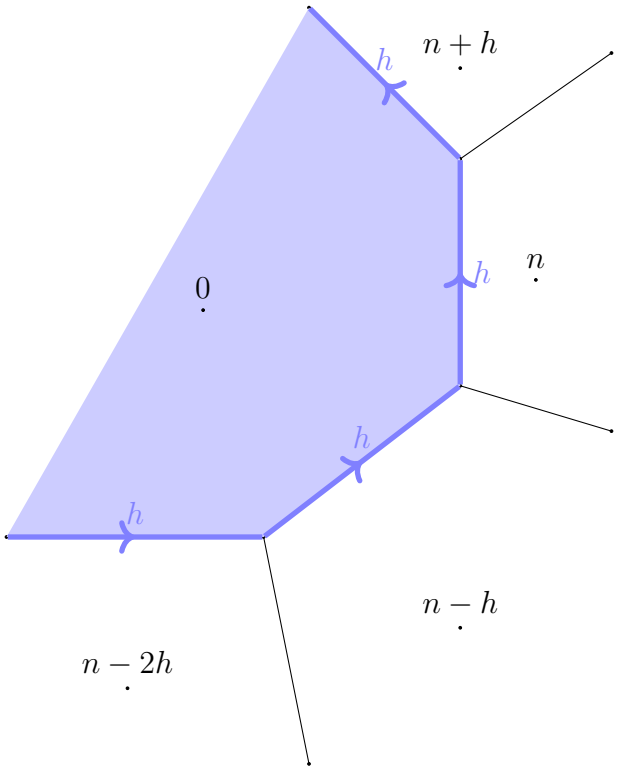
$$\begin{aligned} f(\sqrt{d} - be_1 + 2ae_2) &= a(\sqrt{d} - b)^2 + b(\sqrt{d} - b)(2a) + c(2a)^2 \\ &= a(d - 2b\sqrt{d} + b^2) + a(2b\sqrt{d} - b^2) + a(4ac) \\ &= a(d - b^2 + 4ac) \\ &= 0. \end{aligned}$$

Par conséquent, f représente zéro. □

Proposition 4.74. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet une rivière infinie si et seulement si le discriminant de f est positif et non-carré.*

Démonstration. Supposons que $\mathcal{C}_{\mathcal{R},f}$ contiennent une rivière infinie. Alors, la rivière ne commence et ne termine pas dans un lac. Par conséquent, f ne représente pas l'entier zéro. En effet, si f représentait zéro, alors la rivière passerait inévitablement par un lac et puisque les faces autour des rivières apparaissent de façon périodique par le théorème 4.61, cela induirait que la rivière est finie ce qui est absurde. Par conséquent, le lemme 4.73 indique que le discriminant de f n'est pas un carré. De plus, il est clair que le discriminant de f est positif puisque son topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet une rivière.

Supposons désormais que le discriminant de f soit positif et non-carré. Puisque le discriminant n'est pas un carré, le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ n'admet pas de lac. En effet, supposons par l'absurde que ce topographe de Conway admette un lac. Prenons une forme quadratique binaire équivalente à f sur une des arête du lac.



Disons que cette forme quadratique binaire est $(n, h, 0)$ pour n, h des entiers. Alors, le discriminant de cette forme est égal à h^2 et est un carré. Des formes quadratiques binaires équivalentes partagent le même discriminant par la proposition 3.13. Or cela contredit notre hypothèse de départ. On déduit que le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ n'admet pas de lac et puisque f est indéfinie, elle admet une rivière par le théorème 4.58. De plus, par le lemme 4.59, cette rivière est infinie puisque f ne représente pas zéro. Cela conclut notre preuve. □

Remarque 4.75. Nous revenons sur la théorie de la réduction de ce type de formes quadratiques binaires. Dans ce cas, il est possible de montrer qu'il existe plusieurs formes

quadratiques réduites. Cette particularité se répercute dans le topographe de Conway. Celui-ci est généré par une rivière cyclique infinie. Il est aussi possible de montrer que les formes quadratiques binaires réduites pour une classe d'un déterminant positif sont "adjacentes" et forment des "cycles". Afin de vraiment montrer l'analogie avec la périodicité des rivières, il nous faudrait approfondir la théorie de la réduction pour les formes quadratiques binaires indéfinies. Cela nous emmènerait malheureusement trop loin pour notre propos. Pour une exposition de cette théorie, nous nous rapportons au chapitre trois de la référence [3].

Regardons le troisième point.

Proposition 4.76. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un unique lac si et seulement si le discriminant de f est nul.*

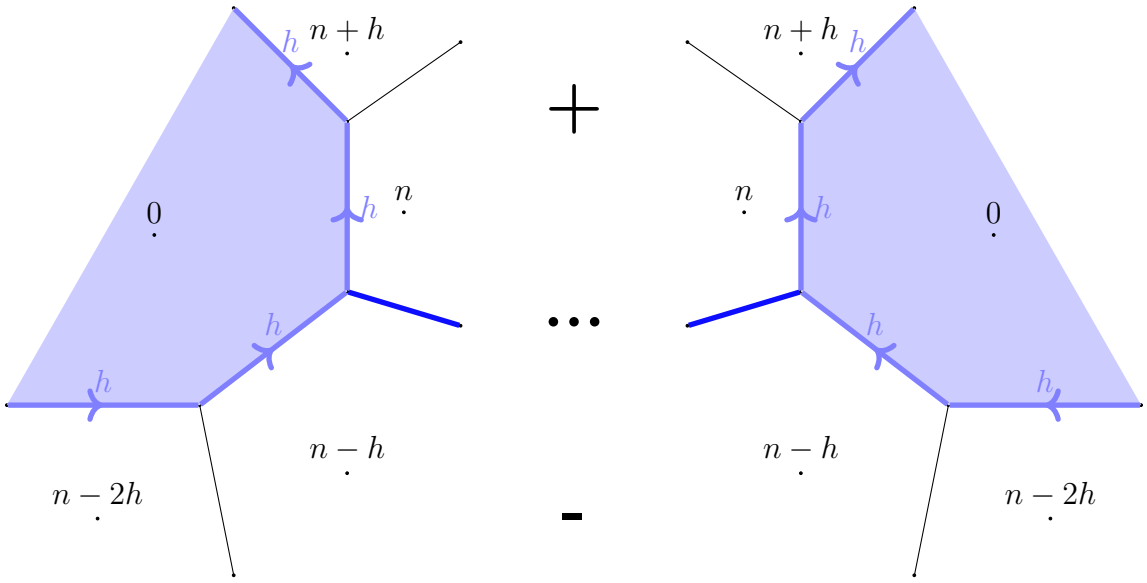
Démonstration. Supposons par l'absurde que le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un unique lac, mais que f ait un discriminant non-nul. Puisque les formes définies n'admettent pas de lac, nous pouvons aussi supposer que le discriminant est positif. La forme quadratique binaire f serait donc indéfinie et représenterait zéro. Or, par le théorème 4.69, nous savons que les topographes de Conway de formes quadratiques binaires indéfinies représentant zéro admettent deux lacs. C'est une contradiction. On déduit donc que le discriminant de f est nul.

Si maintenant le discriminant de f est nul. Alors, nous savons par le corollaire 4.68 que f est semi-définie. Par conséquent, nous pouvons conclure par le théorème 4.66 que le topographe $\mathcal{C}_{\mathcal{R},f}$ admet un unique lac. □

Nous passons à la quatrième assertion. C'est la dernière qui demandera du travail.

Proposition 4.77. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet deux lacs si et seulement si le discriminant de f est positif et carré.*

Démonstration. Si le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet deux lacs, on remarque que les formes quadratiques binaires sur les arêtes du lac ont un discriminant carré. Prenons la forme quadratique binaire $(n, h, 0)$ pour des entiers n, h. On constate que cette forme quadratique binaire est de discriminant carré. Des formes quadratiques binaires partagent le même discriminant par la proposition 3.13. Par conséquent, f a un discriminant carré.



Supposons que le discriminant de la forme quadratique f soit carré. Nous savons par le lemme 4.73 que f représente zéro. Par conséquent le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet un lac. Or, nous savons aussi par le théorème 4.61 que les faces longeant la rivière apparaissent de façon périodique. Par conséquent, la face étiquetée par un zéro réapparaît. Par conséquent, le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ admet au moins deux lac. Il n'en existe pas d'autre car cela impliquerait l'existence d'autres rivières. Or, nous savons par le théorème 4.58 qu'un topographe de Conway d'une forme indéfinie n'admet qu'une rivière. □

Finalement, nous démontrons la dernière assertion.

Proposition 4.78. *Soient Λ un réseau, T son topographe et f une forme quadratique binaire sur ce réseau. Soit $\mathcal{R}$ une représentation principale de T et $\mathcal{C}_{\mathcal{R},f}$ un topographe de Conway de la forme quadratique binaire f. Le topographe de Conway $\mathcal{C}_{\mathcal{R},f}$ n'admet que des lacs si et seulement si f est la forme quadratique binaire triviale.*

Démonstration. Si f n'admet que des lacs, alors il existe une super-base sur laquelle f vaut zéro pour chaque vecteur. On déduit du corollaire 4.14 que f est la forme quadratique binaire triviale. La réciproque étant trivial, cela conclut notre preuve. □

Nous venons donc de démontrer notre théorème de classification des formes quadratiques binaires en fonction des éléments présents sur ses topographes de Conway. Ce théorème met en évidence des propriétés qui passent inaperçues lorsque nous regardons simplement le discriminant d'une forme quadratique binaire. La présence de lacs montre la dégénérescence d'une forme quadratique binaire et les puits et rivière représentent les notions de réductions. Ce théorème conclut le chapitre et notre exposé sur les formes quadratiques binaires.

Annexe A

Réalisation et efficacité de l'algorithme

Dans cet annexe, nous donnons l'algorithme décidant si un entier est proprement représenté par une forme quadratique binaire. Ce code est réalisé en Python. Nous donnons d'abord les idées permettant de réaliser l'algorithme. Comme mentionné, cet algorithme provient principalement d'une bonne utilisation des topographes de Conway et plus spécifiquement de la règle de la progression arithmétique.

Nous nous donnons une structure d'arbre. Les noeuds des arbres seront des objets (a, b, c) représentant des formes quadratiques binaires avec a, b et c des entiers. Comme mentionné notamment dans le corollaire 4.14, ces éléments suffisent à construire l'entièreté du topographe. Les faces de ce topographe seront les éléments a et c de nos objets algorithmique.

```
class TreeNode:
    def __init__(self, a, b, c):
        self.a = a
        self.b = b
        self.c = c
        self.children = []

    def add_child(self, child_1):
        self.children.append(child_1)
```

Listing A.1 – Définition de la classe des formes quadratiques binaires

Avec la règle de la progression arithmétique, nous pouvons construire les formes quadratiques binaires voisines vues comme des arêtes dans le topographe. Pour fonctionner correctement, celui-ci doit retenir l'ensemble des noeuds qu'il a déjà analysé et il ne doit pas recréer de branche à partir de ceux-ci. Cela est réalisé grâce à l'usage d'une variable en dehors de la fonction retenant ces informations.

```
traveled = set()
def build_topograph_children(root):
    if root is None:
        return

    a = root.a
    b = root.b
```

```
    c = root.c

    if c <= 2 * a + b + c:
        child = TreeNode(a, 2 * a + b, a + b + c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if c > 2 * a + b + c:
        child = TreeNode(a, -2 * a - b, a + b + c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if a <= a + b + 2 * c:
        child = TreeNode(a + b + c, b + 2 * c, c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if a > a + b + 2 * c:
        child = TreeNode(a + b + c, -b - 2 * c, c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if c <= 2 * a - b + c:
        child = TreeNode(a, 2 * a - b, a - b + c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if c > 2 * a - b + c:
        child = TreeNode(a, -2 * a + b, a - b + c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if a <= a - b + 2 * c:
        child = TreeNode(a - b + c, -b + 2 * c, c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    if a > a - b + 2 * c:
        child = TreeNode(a - b + c, b - 2 * c, c)
        if (child.a, child.b, child.c) not in traveled:
            root.add_child(child)

    return root
```

Listing A.2 – Création des noeuds enfants

La création des formes quadratiques binaires voisines est rendu possible simplement grâce à la règle de la progression arithmétique. Nous devons rester prudent lors du choix de quelles formes quadratiques binaires sont réellement les enfants, mais cela revient à de simples conditions «si» et à une analyse du signe du deuxième coefficient des noeuds enfants.

Maintenant que nous pouvons créer les formes quadratiques adjacentes, il nous faut un algorithme pour à la fois construire l'arbre et déterminer si un certain entier est proprement représenté par la forme quadratique binaire d'origine. Celui-ci se base sur le théorème 3.11. Celui-ci nous dit qu'un entier est proprement représenté par une forme quadratique binaire si et seulement s'il existe une forme quadratique binaire proprement équivalente ayant pour premier coefficient ledit entier. Il nous suffira donc de regarder les objets $self.a$ et $self.c$ pour nous en assurer. Cette partie est assurée par le code suivant. Celui-ci prend comme entrée un entier n et une forme quadratique binaire f. Celui-ci rend la valeur $True$ si l'entier est proprement représenté et $False$ dans le cas contraire.

```
def search(n, form):

    traveled.add((form.a, form.b, form.c))
    form = build_topograph_children(form)

    if form.a == n or form.c == n:
        return True

    elif len(form.children) == 0:
        return False

    else:
        for child in form.children:
            if abs(child.a) <= abs(n) and abs(child.c) <= abs(n) and
               search(n, child):
                return True

        return False
```

Listing A.3 – Création du topographe et détection de l'entier

Ce code fonctionne récursivement et est un algorithme dit «depth-first search», c'est-à-dire qu'il parcours l'arbre d'enfant en enfant en premier. Le problème principal est que l'arbre dans lequel nous cherchons n'est pas donné, nous devons le construire et nous devons avoir une condition assez forte sur les noeuds enfants pour déterminer si nous continuons de chercher plus loin. Pour cette condition, nous utilisons la proposition 4.31. Celle-ci nous dit que les valeurs des faces augmenteront en valeur absolue si nous partons d'un puits, d'une rivière ou d'un lac. Par conséquent, nous devons changer la forme quadratique binaire de départ. Nous devons la transformer en une forme quadratique binaire se situant sur une arête d'un puits, d'une rivière ou d'un lac. De cette façon, dès que nous dépassons des faces plus grandes en valeur absolue que notre entier, nous pouvons stopper la recherche dans cette branche. Pour les formes quadratiques binaires définies positives, nous avons un algorithme de réduction. Pour les autres types de formes quadratiques binaires, la question est plus complexe. Le code suivant prend en entrée une forme quadratique binaire définie positive.

```
def reduction_def(form):
    a=form.a
```

```
    b=form.b
    c=form.c
    while not (abs(b)<= a and a <= c):
        if a < abs(b) and b > 0:
            t =b
            b = -2*a + b
            c = c-t+a
        if a < abs(b) and b < 0:
            t = b
            b = 2*a + b
            c = c-t + a
        if c < a :
            t = a
            a = c
            c= t
    return TreeNode(a,b,c)
```

Listing A.4 – Algorithme de réduction des formes quadratiques binaires définies positives

Nous demanderons donc aux utilisateurs du code de réduire eux-même les formes quadratiques binaires jusqu'à une forme quadratique binaire d'une arête, d'un lac, ou d'une rivière. L'auteur s'excuse de ne pas avoir pu élaboré un algorithme de réduction pour ces cas là.

Enfin, nous donnons une fonction rendant une phrase dans le cas ou l'entier est proprement représenté et dans le cas contraire.

```
def Answer(n, form):
    if (form.b)**2 - 4*form.a*form.c <0 :
        form =reduction_def(form)
        if search(n, form):
            print("Oui, c'est un entier proprement represente !")
        else:
            print("Non, il n'est pas proporement represente !")
    else :
        if search(n, form):
            print("Oui, c'est un entier proprement represente !")
        else:
            print("Non, il n'est pas proporement represente !")
```

Nous faisons désormais un commentaire sur l'efficacité du code. D'un point de vue complexité, le code construit un arbre et recherche en même temps dedans. Il le fait de façon récursive. Le principale problème de cette méthode est que lorsque nous cherchons si un grand nombre est proprement représenté, on procède à un grand nombre de récursions. Cependant, Python et ensuite Windows refuse d'excéder un certain nombre de récursions et d'allouer plus de mémoire vive. Une façon de régler ce problème serait d'écrire le code de façon itérative. Cela semble compliqué étant donné que nous devons construire l'arbre et chercher dedans. La construction itérative d'un arbre dans ce cas-ci semble quelque

peu compromise. Cela nécessiterait une borne sur la boucle. Pour donner un ordre d'idée, nous avons pu déterminer que 7581 ou encore 8281 sont des entiers proprement représentés. Cependant, lorsque les nombres deviennent trop grand, le code ne compile plus et rend «Process finished with exit code -1073741571 (0xC00000FD)» ce qui correspond au problème de mémoire dont nous venons de parler.

Malgré ces quelques défauts, sans la théorie des topographes, nous n'aurions pas pu développer cet algorithme. S'il est vrai que la récursion et la structure d'arbre présentent des inconvénients, il n'en reste pas moins que, si plus de mémoire était allouée, le code fonctionnerait efficacement.

Bibliographie

[1] August Lösch, *The economics of locations*, Yale University Press, New Haven, 1971.

[2] David A. Cox, *Primes of the form x^2+ny^2*, Second, Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc, Hoboken, NJ, 2013.

[3] Duncan A. Buell, *Binary Quadratic Forms*, Springer-Verlag, New York, 1989.

[4] Enrico M. Vitale, *Algèbre linéaire*, Louvain-la-neuve, Notes de cours LMAT1131, 2019, p159-160.

[5] H. Davenport, *The Higher Arithmetic*, Eighth, Cambridge University Press, Cambridge, 2008.

[6] John H. Conway, *The sensual (quadratic) form*, Carus Mathematical Monographs, vol. 26, Mathematical Association of America, Washington, DC, 1997.

[7] John U. Marshall, *The Löschian numbers as a problem in number theory*, Geographical Analysis, Vol. 7, 1975, p. 421-426.

[8] J. W. S. Cassels, *An introduction to the geometry of numbers*, Classics in Mathematics, Springer-Verlag, Berlin, 1997.

[9] Kenneth Ireland et Michael Rosen, *A classical introduction to Modern Number Theory*, Second, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[10] Leonard E. Dickson, *Introduction to the Theory of Numbers*, Dover Publications. Inc, New York, 1929.

[11] Martin H. Weissman, *An Illustrated Theory of Numbers*, American Mathematical Society, Providence, RI, 2017.

[12] Michael Goldberg, *A class of multi-symmetric polyhedra*, Tohoku mathematical journal, First series, Vol. 43, 1937, p.104-108.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Faculté des sciences
Place des sciences, 2 bte L6.06.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/sc**