Le théorème des 15

Corentin Bernet, Sélène Corbineau
sous la direction de Gaëtan Chenevier

Mémoire de première année 2022-2023

1 Introduction

Ce mémoire a pour but de démontrer un surprenant résultat de la théorie des formes quadratiques, le théorème des 15.

On s'intéresse aux formes quadratiques définies positives à coefficients dans l'anneau $\mathbb{Z}$ des entiers, c'est-à-dire aux fonctions de $\mathbb{Z}^n$ dans $\mathbb{Z}$ de la forme $f(x_1, \dots, x_n) = \sum_{1 \leq i,j \leq n} f_{ij} x_i x_j$ où les coefficients entiers (f_{ij}) forment une matrice symétrique définie positive. Comme exemples historiques, on peut citer les formes $x^2 + y^2$, étudiée par Euler, et $x^2 + y^2 + z^2 + t^2$, étudiée par Lagrange.

On s'intéresse aux entiers *représentés* par cette forme, c'est-à-dire aux entiers qui sont dans son image. On dira qu'une forme quadratique est universelle si tous les entiers positifs sont représentés par elle. Par exemple, la forme $x^2+y^2+z^2+t^2$ est universelle (résultat démontré par Lagrange), alors que la forme $x^2 + y^2$ ne l'est pas (elle ne représente pas 7, et on connaît même précisément les entiers qu'elle représente).

Le théorème des 15 s'énonce de la façon suivante :

Théorème 1.0.1. *Une forme quadratique définie positive à coefficients dans $\mathbb{Z}$ est universelle si et seulement si elle représente tous les entiers de 1 à 15. En fait, il suffit qu'elle représente les entiers 1, 2, 3, 5, 6, 7, 10, 14 et 15.*

Ce théorème permet une vérification algorithmique de l'universalité d'une forme quadratique (définie positive, sur $\mathbb{Z}$). Cela permet à Bhargava, dont on suit la démonstration ici, de déterminer exactement les formes quadratiques universelles à quatre variables par exemple [3]. Le squelette de la preuve que l'on emploiera se pare de théorie plus poussée sur les formes quadratiques vis-à-vis de cet exposé pour montrer un résultat similaire où l'on autorise les f_{ij} avec

$i \neq j$ à être des demi-entiers, ce qui permet aux coefficients produits croisés d'être impairs. Cela a été mis en oeuvre par Bhargava et Hanke à la suite de la découverte de la preuve exposée ici. Ils ont démontré un théorème analogue au théorème des 15, dans lequel la constante 15 doit être là remplacée par 290, et la liste des entiers critiques est de longueur 28 [6].

La démonstration, annoncée mais non publiée pour la première fois par Conway et Schneeberger en 1993 [4] puis améliorée et publiée par Bhargava [3], utilise de nombreux calculs à l'ordinateur, et s'appuie sur l'étude théorique des formes quadratiques par le biais, notamment, des entiers p-adiques et des réseaux entiers. On s'intéressera donc à ces objets avant de présenter la démonstration de Bhargava.

Table des matières

2 Formes quadratiques : définitions et résultats fondamentaux

2.1 Définitions

Tout d'abord, il convient de définir la notion de forme quadratique dans un cas transverse à celui de $\mathbb{Z}$, et de comprendre comment les manipuler. Cette étude suit celle de Serre [2].

Définition 2.1.1. *Soit k un corps, V un k-espace vectoriel de dimension finie, f une forme bilinéaire symétrique. La* ***forme quadratique*** *associée à f est l'application $q : V \to k$ définie par $\forall x \in V, q(x) = f(x,x)$. On appelle (V,q) un espace quadratique. On appellera forme quadratique une forme quadratique s'obtenant à partir d'un certain f.*

On définit parfois les formes quadratiques par les axiomes suivants : q est une forme quadratique si

— $\forall \lambda \in k, \forall x \in V, q(\lambda x) = \lambda^2 q(x)$

— L'application $(x,y) \mapsto q(x+y) - q(x) - q(y)$ est une forme bilinéaire.

On récupère alors la forme bilinéaire f par une polarisation : $f(x,y) = \frac{q(x+y)-q(x)-q(y)}{2}$. L'inconvénient de cette méthode est la division par 2 dans le cas certes pathologique de la caractéristique 2.

On introduit à présent la notion de *matrice de Gram*, une représentation matricielle d'une forme quadratique agréable à manipuler.

Définition 2.1.2. *On suppose V de dimension n et on choisit une base $e = (e_1, \ldots, e_n)$. La matrice de Gram relative à e de la forme quadratique q est la matrice $M \in \mathcal{M}_n(k)$ définie par $M_{ij} = f(e_i, e_j)$ pour $1 \leq i, j \leq n$. Cette matrice est symétrique.*

Maintenant qu'on a introduit une représentation matricielle, il est tentant de parler d'équivalence de formes quadratiques, comme dans le cadre des applications linéaires. On en donne d'abord une définition algébrique :

Définition 2.1.3. *Soit q, q' deux formes quadratiques sur V. On dit que q et q' sont* équivalentes *s'il existe $u \in GL(V)$ telle que $q' = q \circ u$.*

On vérifie aisément que cette définition donne une relation d'équivalence. La question qui se pose alors est : comment se traduit l'équivalence de deux formes quadratiques sur leurs matrices de Gram ? Soit P la matrice associée à u dans la base e. On a :

$$\begin{aligned} f'(e_i, e_j) &= f(P_{1i}e_1 + \ldots + P_{ni}e_n, P_{1j}e_1 + \ldots + P_{nj}e_n) \\ &= \sum_{1 \leq k,l \leq n} P_{ki} P_{lj} f(e_k, e_l) \end{aligned}$$

On reconnaît un produit matriciel : si M, M' sont les matrices de Gram de q, q' dans la base e alors $M' = P^T M P$.

On a déjà observé la similarité avec les produits scalaires sur un espace euclidien. En fait, on peut donner un sens à une grande partie des concepts d'algèbre euclidienne dans le cadre des formes quadratiques :

Définition 2.1.4. *Soit A une partie de V, q une forme quadratique sur V. On appelle orthogonal de A le sous-espace vectoriel $A^\perp = \{x \in V \mid \forall y \in A, f(x,y) = 0\}$. On dit que q est dégénérée si $V^\perp \neq \{0\}$.*

On n'étudiera pas de formes quadratiques dégénérées, puisque le théorème des 15 traite de formes défini-positives, qui ne peuvent pas être dégénérées comme on le verra. Mentionnons tout de même qu'on pert peu de généralité en faisant cela, grâce au fait suivant :

Propriété 2.1.5. *Soit S un supplémentaire de $V^\perp$ dans V. Alors q induit sur $V^\perp$ la forme nulle, et sur S une forme non-dégénérée.*

Démonstration. i) Si $x \in V^\perp$, on a $q(x) = f(x,x) = 0$ par hypothèse.

ii) On appelle T l'orthogonal de S dans lui-même. Soit $x \in T$. Alors pour tout $y \in S$, $f(x,y) = 0$. De plus pour tout $z \in V^\perp$, $f(x,z) = 0$ par hypothèse. Comme S et $V^\perp$ sont supplémentaires, on en déduit $f(x,t) = 0$ pour tout $t \in V$. Ainsi $x \in V^\perp$, et comme $x \in S$ on a directement $x = 0$. Donc $T = \{0\}$, la forme induite sur S est non-dégénérée.

□

2.2 Premiers éléments de classification et exemples

Dans cette section, on va aborder la classification des formes quadratiques, à équivalence près. On donne pour cela un premier invariant fondamental :

Définition 2.2.1. *Soit q une forme quadratique. On appelle déterminant de q le déterminant de sa matrice de Gram, vu comme élément de $k/c(k)$, où $c(k)$ désigne l'ensemble des carrés de k.*

La notation $k/c(k)$ renvoie au monoïde quotient $(k/c(k), \times)$. La présence de 0 empêche en effet de parler de groupe quotient, mais la définition est la même, et on ne s'intéressera de toute façon pas à des formes de déterminant nul.

Cette définition n'est pas ambiguë car en passant modulo les carrés, le déterminant ne dépend pas de la base dans laquelle on calcule la matrice de Gram. En effet, soient M, M' deux matrices de Gram de q, on sait qu'il existe P inversible telle que $M' = PMP^T$. On en déduit $\det(M') = \det(P)^2 \det(M)$.

Avec cet outil, on peut démontrer un important résultat de diagonalisation, qui s'inspire de l'orthogonalisation de Gram-Schmidt :

Propriété 2.2.2. *Soit q une forme quadratique sur V. Alors q est équivalente à une forme quadratique dont la matrice de Gram est diagonale.*

Démonstration. La proposition 2.1.5 permet de supposer que q est non-dégénérée, car il suffit de diagonaliser sur l'espace S. En particulier il existe $x \in V$ tel que $q(x) \neq 0$. On complète en une base $x_1, \ldots, x_n$ de V avec $x_1 = x$, puis on pose, pour k entre 2 et n, $x'_k = x_k - \frac{f(x_k,x)}{q(x)}x$, orthogonal à x. On se place dans la base $x, x'_2, \ldots, x'_n$. La matrice de Gram de q dans cette base est une matrice par blocs, un bloc de taille 1 et un de taille $n-1$. On diagonalise le bloc de taille $n-1$ par récurrence (le cas $n = 1$ est trivial). □

Remarque. *On en déduit qu'une forme quadratique est dégénérée si et seulement si son déterminant est nul. En effet,* $\det(q) = \lambda_1 \ldots \lambda_n$ *avec λ_i les coefficients de la forme diagonale de q. $det(q)$ est nul ssi il existe i tel que λ_i est nul, auquel cas le vecteur x_i associé est orthogonal à tous les vecteurs de cette base donc à V tout entier. Réciproquement, si tous les λ_i sont non-nuls, on a $f(x,y) = \sum_i 2\lambda_i x_i y_i$. Donc si $x \in V^\perp$, on a pour tout i, $2\lambda_i x_i = 0$ donc $x = 0$.*

Par ailleurs, la preuve ci-dessus permet en fait de construire une « base orthogonale »commençant par n'importe quel vecteur de V, ce qui sera utile plus tard.

On peut maintenant aborder la classification des formes quadratiques dans des cas simples : $\mathbb{C}, \mathbb{R}, \mathbb{F}_p$. Le résultat ci-dessus permet de se restreindre à la classification des formes diagonales $x \mapsto a_1x_1^2 + \ldots + a_nx_n^2$, notée plus simplement $a_1x_1^2 + \ldots + a_nx_n^2$.

Propriété 2.2.3. *Toutes les formes quadratiques non-dégénérées sur $\mathbb{C}$ sont équivalentes.*

Démonstration. Soit $a_1x_1^2 + \ldots + a_nx_n^2$ une forme diagonale non-dégénérée, avec par conséquent $a_i \neq 0$ pour tout i. On sait que chaque a_i a une racine carrée b_i non-nulle, donc on peut la réécrire $(b_1x_1)^2 + \ldots + (b_nx_n)^2$, ce qui est évidemment équivalent à $x_1^2 + \ldots + x_n^2$. Toute forme quadratique non-dégénérée sur $\mathbb{C}$ est donc équivalente à celle-ci : elles sont toutes équivalentes. □

Le même argument tient pour tout corps quadratiquement clos, c'est-à-dire tel que pour tout $a \in k$ admette une racine carrée dans k. Le corps des nombres complexes $\mathbb{C}$ en est un exemple comme tout corps algébriquement clos, ou celui des nombres constructibles à la règle non-graduée et au compas.

En revanche, $\mathbb{R}$ n'est pas un corps quadratiquement clos, mais ses carrés sont connus, ce sont les nombres positifs. La classification ne sera donc pas non plus difficile.

Définition 2.2.4. *Si q une forme quadratique sur $\mathbb{R}^n$ s'écrit à équivalence près $a_1x_1^2 + \ldots + a_nx_n^2$, on appelle signature de q le cardinal de $\{1 \leq i \leq n \mid a_i > 0\}$.*

Propriété 2.2.5. *La signature est bien définie, et deux formes quadratiques non-dégénérées sur $\mathbb{R}$ sont équivalentes si et seulement si elles ont même signature.*

Démonstration. Pour q une forme quadratique, on appelle r_q la dimension maximale d'un sous-espace vectoriel de V sur lequel q est définie positive. Cette quantité est bien définie, et si $q' = q \circ f$, alors q' est définie positive sur V si et seulement si q est définie positive sur $f(V)$ qui est de même dimension que V. D'où $r_q = r_{q'}$. Prenons q diagonale de signature k, qui est donc définie positive sur $\mathrm{Vect}(x_1, \ldots, x_k)$. Si $\dim(V) \geq k+1$, alors V intersecte $\mathrm{Vect}(x_{k+1}, \ldots, x_n)$, donc q n'est pas définie positive sur V, et donc $r_q = k$. On en déduit que si deux formes quadratiques diagonales n'ont pas la même signature, elles ne sont pas équivalentes.

Soit $a_1x_1^2 + \ldots + a_nx_n^2$ non-dégénérée sur $\mathbb{R}$, de signature k. On peut supposer $a_1, \ldots, a_k > 0$ et $a_{k+1}, \ldots, a_n < 0$ quitte à permuter les coordonnées. On réécrit cette forme en $(\sqrt{a_1}x_1)^2 + \ldots + (\sqrt{a_k}x_k)^2 - (\sqrt{-a_{k+1}}x_{k+1})^2 - \ldots - (\sqrt{-a_n}x_n)^2$, ce qui est équivalent à $x_1^2 + \ldots + x_k^2 - x_{k+1}^2 - \ldots - x_n^2$. Deux formes quadratiques non-dégénérées de même signature sont donc équivalentes. □

On fixe à présent p un nombre premier impair et on étudie les formes quadratiques sur $\mathbb{F}_p$(on pourrait en fait regarder n'importe quel corps fini). On rappelle que la moitié de ses éléments inversibles sont des carrés.

Lemme 2.2.6. *Toute forme quadratique non dégénérée à plus de deux variables sur $\mathbb{F}_p$ est universelle.*

Démonstration. Il suffit de le prouver pour une forme diagonale à deux variables. Soit $ax^2 + by^2$ une telle forme, $c \in \mathbb{F}_p$. Quand x et y parcourent $\mathbb{F}_p$, ax^2 et $c - by^2$ prennent tous deux $\frac{p+1}{2}$ valeurs (le nombre de carrés) car $a, b \neq 0$, par principe des tiroirs une valeur est représentée par les deux. Donc $ax^2 + by^2$ représente c, et est universelle. □

Propriété 2.2.7. *Une forme quadratique sur $\mathbb{F}_p$ de déterminant $D \neq 0$ est équivalente à $x_1^2 + \ldots + x_{n-1}^2 + Dx_n^2$. En particulier deux formes quadratiques sur $\mathbb{F}_p$ sont équivalentes si et seulement si elles ont même déterminant.*

Démonstration. On raisonne par récurrence sur n, l'initialisation ne pose pas de problème. Soit q une forme quadratique à plus de deux variables de déterminant D. Comme vu ci-dessus q représente 1, q est donc équivalente à $x_1^2 + q'(x_2, \ldots, x_n)$ avec q' une forme quadratique sur un espace de dimension $n-1$, de déterminant D nécessairement. Alors q' est équivalente à $x_2^2 + \ldots + Dx_n^2$ par hypothèse de récurrence, ce qui conclut. □

Mais revenons au problème de départ. On souhaite une meilleure connaissance des formes quadratiques sur $\mathbb{Z}$, qui n'est pas un corps. On va donc commencer par étudier les formes quadratiques sur $\mathbb{Q}$, ce qui est déjà plus délicat que ce que l'on vient de mener, les carrés de $\mathbb{Q}$ étant nettement moins faciles à décrire que ceux de $\mathbb{C}, \mathbb{R}, \mathbb{F}_p$. Pour ce faire, on cherche des invariants en étudiant les surcorps naturels de $\mathbb{Q}$. Le corps des réels $\mathbb{R}$ en est un et nous donne la signature, mais il nous faut plus. C'est ici qu'interviennent les corps $\mathbb{Q}_p$ des nombres p-adiques.

3 Les nombres p-adiques

3.1 Définition

Dans toute la section, p désigne un nombre premier.

On commence par définir l'anneau $\mathbb{Z}_p$ des entiers p-adiques. Informellement, les entiers p-adiques sont des entiers ayant, en base p, un nombre infini de chiffres à gauche, de même que les réels ont un nombre infini de chiffres à droite.

Définition 3.1.1. *Un entier p-adique est une suite $(a_n)_{n\in\mathbb{N}^*}$ telle que pour tout n, a_n est un élément de $\mathbb{Z}/p^n\mathbb{Z}$ vérifiant $\forall k < n, a_n \equiv a_k \pmod{p^k}$.*

On définit l'addition et le produit naturellement, terme à terme. On désignera par k l'entier p-adique $(k \pmod{p^n})_{n\in\mathbb{N}^*}$, ce qui permet de plonger $\mathbb{Z}$ dans $\mathbb{Z}_p$. Il est clair que cela fait de $\mathbb{Z}_p$ un anneau intègre. On note $\mathbb{Q}_p$ son corps des fractions, appelé corps des nombres p-adiques. Listons quelques propriétés fondamentales dont les démonstrations sont présentées par Serre [2] :

Propriété 3.1.2. *Les inversibles de $\mathbb{Z}_p$ sont les $a = (a_n)$ vérifiant $a_1 \neq 0$. Si $a \in \mathbb{Z}_p$ est non-nul, on peut écrire $a = p^k u$ de façon unique, avec k un entier positif et u un inversible. De même si $a \in \mathbb{Q}_p$ non-nul, avec k un entier relatif. On note $k = v_p(a)$. La fonction v_p est un stathme euclidien sur $\mathbb{Z}_p$.*

Propriété 3.1.3. *On pose, pour $a \in \mathbb{Q}_p$, $\mid a \mid_p = p^{-v_p(a)}$ avec la convention $v_p(0) = \infty$. Alors $(\mathbb{Q}_p, \mid \cdot \mid_p)$ est un corps valué. La topologie associée est compacte, complète, ultramétrique et $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$. De plus une série à coefficients dans $\mathbb{Q}_p$ converge si et seulement si son terme général tend vers 0.*

3.2 Formes quadratiques sur $\mathbb{Q}_p$

Pour comprendre les formes quadratiques sur $\mathbb{Q}_p$, il faut d'abord connaître les carrés de ce corps, ce qui se ramène à connaître les carrés de $\mathbb{Z}_p$. Il y en a étonnamment beaucoup :

Propriété 3.2.1. *Si $p \neq 2$, $u \in \mathbb{Z}_p^\times$ est un carré si et seulement si u_1 est un carré dans $\mathbb{F}_p$. En conséquence, les carrés de $\mathbb{Q}_p$ sont les $p^{2k}u$ avec u un carré inversible et k un entier relatif.*

Démonstration. Cherchons un dévissage du groupe multiplicatif $\mathbb{Z}_p^\times$. Par le morphisme $\mathbb{Z}_p^\times \to \mathbb{F}_p^* : a \mapsto a_1$, on sait que $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^* \times (1 + p\mathbb{Z}_p)$. Si $z \in 1 + p\mathbb{Z}_p$, on a $\mid z - 1 \mid_p < 1$, ce qui permet de définir $\log(z)$ par la série entière usuelle car $\frac{(z-1)^n}{n}$ tend vers 0. C'est un isomorphisme de $1 + p\mathbb{Z}_p$ vers $p\mathbb{Z}_p$. En effet pour $z \in p\mathbb{Z}_p$ on peut aussi définir $\exp(z)$ avec la série entière, puisque $\frac{z^n}{n!}$ tend vers 0 (la formule de Legendre permet d'avoir $v_p(n!) < \frac{n}{p-1}$ donc $\mid \frac{z^n}{n!} \mid_p = p^{v_p(n!)-nv_p(z)} < p^{-n(1-\frac{1}{p-1})}$ qui tend vers 0). On vérifie que exp et log sont réciproques l'une de l'autre, d'où l'isomorphisme. On a alors $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^* \times \mathbb{Z}_p$. Or la multiplication par 2 est bijective dans le groupe additif $\mathbb{Z}_p$, donc u est un carré si et seulement si sa composante dans $\mathbb{F}_p^*$, soit u_1, est un carré. □

Reste le cas $p = 2$, où la condition s'avère plus contraignante :

Propriété 3.2.2. *Un élément $u \in \mathbb{Z}_2^\times$ est un carré si et seulement si $u_3 = 1$.*

Démonstration. La preuve est moralement la même que dans le cas $p \neq 2$, à deux détails près : l'exponentielle est cette fois définie sur $4\mathbb{Z}_2$ et à valeurs dans $1 + 4\mathbb{Z}_2$. On déduit de $1 + 4\mathbb{Z}_2 \simeq \mathbb{Z}_2$ que le groupe des carrés est d'indice 2 dans $1 + 4\mathbb{Z}_2$, et on sait qu'il est inclus dans $1 + 8\mathbb{Z}_2$, donc tout élément de $1 + 8\mathbb{Z}_2$ est un carré. Et si k est impair, on sait déjà que $k^2 \equiv 1 \pmod 8$ par disjonction de cas. D'où l'équivalence. □

On voit donc qu'il y a beaucoup de carrés dans $\mathbb{Z}_p$, ce qui aidera à démontrer l'universalité de formes quadratiques sur ce corps. Étant donnée une forme quadratique sur $\mathbb{Z}$, on peut la considérer comme à coefficients dans $\mathbb{Z}_p$, on aimerait donc relier l'universalité dans ces différents anneaux. On a miraculeusement un résultat à ce sujet, qui demande d'introduire la notion de *genre*.

Définition 3.2.3. *On dit que deux formes quadratiques à coefficients dans $\mathbb{Z}$ sont dans le même genre si elles sont équivalentes dans $\mathbb{Z}_p$ pour tout nombre premier p.*

À première vue, cette relation d'équivalence semble très restrictive, mais il n'en est rien. Par exemple, les deux formes $x^2 + 11y^2$ et $3x^2 + 2xy + 4y^2$, sont dans le même genre. Pour le voir, on écrit

$$3x^2 + 2xy + 4y^2 = \frac{1}{3}((3x + y)^2 + 11y^2)$$

. Soit p premier. Montrons que $q = 3x^2 + 2xy + 4y^2$ représente 1 dans $\mathbb{Z}_p$. Si $p \neq 2$, l'égalité ci-dessus montre que q représente $(1 + 11)/3 = 4 = 2^2$, donc que q représente 1 (en divisant x et y par 2). Si $p = 2$, on considère que q représente $(11 \cdot 9)/3 = 33$ qui est un carré, donc que q représente 1. Si $p \neq 11$, q est non dégénérée (vu son déterminant). Comme elle représente 1, la proposition 2.2.2 permet d'écrire $q \sim x^2 + ay^2$ avec a défini au carré près. Vu le déterminant de q, il est possible de prendre $a = 11$. Cela montre $q \sim x^2 + 11y^2$ dans $\mathbb{Z}_p$ avec $p \neq 11$. Si $p = 11$ alors on remarque que 3 est un carré dans $\mathbb{Z}_p$, donc que, écrivant $3 = s^2$, $q = ((3x + y)/s)^2 + 11(y/s)^2$ d'où $q \sim x^2 + 11y^2$ dans ce cas. Cela achève de montrer que $x^2 + 11y^2$ et $3x^2 + 2xy + 4y^2$ sont dans le même genre !

L'intérêt de cette relation d'équivalence résulte d'un corollaire du théorème de Hasse-Minkowski, démontré par Cassels dans [1].

Théorème 3.2.4. *Soit q forme quadratique sur $\mathbb{Z}$ et $n \in \mathbb{Z}$. Si q représente n dans $\mathbb{Z}_p$ pour tout p premier, alors il existe q' une autre forme quadratique sur $\mathbb{Z}$ telle que*

- *q et q' soient dans le même genre*
- *q' représente n dans $\mathbb{Z}$.*

En particulier, si q est unique en son genre, alors elle représente n si et seulement si elle représente n dans tous les $\mathbb{Z}_p$. L'intérêt de ce théorème est qu'être universel sur $\mathbb{Z}_p$ est facile, en tout cas lorsque $p \neq 2$. Déjà, à forme quadratique fixée il ne peut y avoir qu'un nombre fini de premiers, identifiables, qui peut poser problème :

Propriété 3.2.5. *Soit q une forme quadratique de la forme $x^2 + f(y, z)$ et p premier impair. Si $p \nmid \det q$ alors q est universelle sur $\mathbb{Z}_p$.*

Démonstration. Comme $p \nmid \det q$, il vient $p \nmid \det f$ donc f est non dégénérée sur $\mathbb{F}_p$ et est donc universelle par le lemme 2.2.6. Soit $a \in \mathbb{Z}_p$. Il existe $y, z \in \mathbb{Z}$ tels que $a - f(y, z) \equiv 1$ modulo p. Dès lors $a - f(y, z)$ est un carré de $\mathbb{Z}_p$ et q représente a. □

Pour les p posant éventuellement problème, des petits calculs permettent de s'assurer que beaucoup d'entiers sont tout de même représentés.

Propriété 3.2.6. *On reprend le cadre précédent, sans l'hypothèse sur le déterminant. Soit $0 < k < p^2$ un entier. Si q représente k dans $\mathbb{Z}/p^2\mathbb{Z}$ alors q représente tout $n \in \mathbb{Z}$ de la forme $p^{2m}u$ avec u congru à k modulo p^2.*

Démonstration. Soit n de la forme prescrite. Par hypothèse, dans $\mathbb{Z}_p$, q représente un certain $k+p^2l$. Alors, les $1+ps$ avec $s \in \mathbb{Z}_p$ étant des carrés, q représente tous les

$$(k+p^2l)(1+ps) = k + p[p^2l + s(k+p^2l)]$$

Si $p \nmid k$ alors $k+p^2l$ est un inversible, donc q représente u en prenant le bon s, puis n vu que p^{2m} est un carré. Si $p \mid k$, écrivant $k = pk'$ avec $p \nmid k'$ on écrit

$$(k+p^2l)(1+ps) = k + p^2[pl + s(k'+pl)]$$

et on conclut similairement. □

Remarquons que ce résultat est en fait assez faible : la preuve jette beaucoup d'informations et utilise seulement les carrés de la forme $1+ps$. Toutefois, il est suffisant pour notre étude, d'autant que la mise en oeuvre du résultat plus fort sous-jacent nécessite en fait la même quantité de calculs.

Le cas $p = 2$ nécessite une attention particulière. En calquant la preuve précédente et vu la caractérisation des carrés de $\mathbb{Z}_2$, on obtient :

Propriété 3.2.7. *On reprend le cadre précédent. Soit ici $0 < k < 16$, non multiple de 4. Si q représente k dans $\mathbb{Z}/16\mathbb{Z}$ alors q représente tous les $2^{2m}u$ avec u congru à k modulo 16.*

4 Formes quadratiques entières et réseaux entiers

En dernier lieu avant d'aborder la démonstration de Bhargava, nous nous intéressons aux formes quadratiques entières. Comme $\mathbb{Z}$ n'est pas un corps, leur manipulation est moins agréable. Toutefois, nous présenterons un point de vue facilitant l'usage des formes quadratiques entières : les réseaux entiers.

4.1 Formes quadratiques entières

Étudions les formes quadratiques entières à l'aune des sections précédentes. N'étant pas dans un corps, en tentant de calquer l'étude précédente on doit prendre des définitions *ad hoc*. Ainsi *la* matrice de Gram de la forme donnée par $\sum a_{ij}x_ix_j$ sera définie comme $(a_{ij})_{i,j}$. On dira que deux formes quadratiques entières sont équivalentes s'il existe un changement de variable « entier »transformant l'une en l'autre : si leurs matrices de Gram sont M_1, M_2 cela revient à l'existence de $P \in \mathrm{GL}_n(\mathbb{Z})$ telle que $M_1 = P^T M_2 P$. Notons que cela préserve la notion de genre et que deux formes quadratiques équivalentes représentent les mêmes entiers, quitte à multiplier un vecteur antécédent $X \in \mathbb{Z}^n$ par P ou P^{-1}.

Remarquons également que sous cette relation d'équivalence, le déterminant est un invariant d'équivalence. En effet, si les formes données par M_1 et M_2 sont équivalentes et notant P matrice de passage on a $\det M_1 = (\det P)^2 \det M_2$. Or comme $P \in \mathrm{GL}_n(\mathbb{Z})$, $\det P = \pm 1$, d'où égalité des déterminants.

4.2 Réseaux

Avant d'attaquer la preuve de Bhargava, il nous faut aborder un dernier outil qui offre un point de vue différent sur les formes quadratiques entières : les réseaux entiers, classe particulière de réseaux de $\mathbb{R}^n$. Ceux-ci jouent pour les formes quadratiques entières le rôle dévolu aux espaces vectoriels pour les formes quadratiques générales. Les notions de cette section sont tirées du livre [5] de Ebeling d'après Hirzebruch.

Définition 4.2.1. *On appelle* ***réseau*** *de $\mathbb{R}^n$ un sous-groupe engendré par une base de $\mathbb{R}^n$. Si $(e_1, \ldots, e_n)$ est une base de $\mathbb{R}^n$, le réseau associé est $\mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$. On considère $(\mathbb{R}^n, \cdot)$ espace euclidien canonique ; on appelle alors* ***réseau entier*** *un réseau L vérifiant $\forall x, y \in L, x \cdot y \in \mathbb{Z}$.*

À un réseau L on associe une forme quadratique entière définie positive q à équivalence près de la manière suivante. Si N est une matrice dont les colonnes sont une base de L alors on considère q associée à la matrice définipositive (entière) $N^T N$. Cela représente la matrice de Gram du produit scalaire canonique en la base choisie de L. Si M est une autre telle matrice, en exprimant les vecteurs de la base associée M en fonction de ceux de N on obtient $P \in \mathrm{GL}_n(\mathbb{Z})$ telle que $M = NP$. (On sait P inversible car l'on peut aussi exprimer à partir de combinaisons entières N à partir de M, ce qui fournit un inverse). Dès lors la forme qu'on associerait via M est donnée par la matrice de Gram

$$M^T M = P^T (N^T N) P$$

et est donc équivalente à q. Cela assure la bonne définition de l'association à équivalence près. D'ailleurs, quitte à fixer N et prendre P décrivant $\mathrm{GL}_n(\mathbb{Z})$, on voit que l'ensemble des formes quadratiques entières définies positives obtenues via des bases de L décrit exactement la classe d'équivalence de q. Aussi, étant donné q une forme quadratique entière définie positive, la sachant équivalente sur $\mathbb{R}^n$ au produit scalaire canonique on peut écrire sa matrice de Gram comme $M^T M$, avec M inversible. Le réseau engendré par les colonnes de M représente alors la classe de q.

Vu cette association et sachant le déterminant un invariant d'équivalence vu la sous-section précédente, on définit le *déterminant* d'un réseau entier L, $\det L$, comme celui de n'importe laquelle de ses formes associées. Comme $\det L = (\det N)^2$ où N est une matrice dont les colonnes sont les vecteurs d'une base de L, on remarque que $\det L$ s'interprête comme le carré du volume d'une maille

élémentaire. Le déterminant d'un réseau est plus communément dénommé *discriminant* de celui-ci, le terme déterminant étant réservé à la racine du discriminant. Nous avons opté pour cette convention afin d'adopter un vocabulaire commun aux réseaux et formes quadratiques.

Dans notre étude, cette analogie permet une nouvelle comparaison entre formes quadratiques : l'inclusion des réseaux associés. En effet si deux réseaux sont inclus l'un dans l'autre, les images des formes quadratiques sont aussi incluses l'une dans l'autre, ce qui sera pratique dans les études d'universalité.

4.3 Sur-réseaux

Il y a deux manières d'envisager l'inclusion de réseaux. On peut étudier les sur-réseaux de même rang (on appelle rang de L l'entier $\dim(\mathrm{Vect}(L))$), ou les sur-réseaux de rang supérieur. Ces deux études sont fondamentalement différentes, et on introduit maintenant un objet aidant à la première :

Définition 4.3.1. *Soit L un réseau entier. On appelle* ***réseau dual*** *de L le réseau $L^{\#} = \{x \in \mathbb{R}^n, \forall y \in L, x \cdot y \in \mathbb{Z}$. Ainsi, si L' est un sur-réseau entier de L de même rang, on a nécessairement $L' \subseteq L^{\#}$ (qui lui n'est en général pas entier).*

Propriété 4.3.2. *On a l'égalité* $\det(L^{\#}) = \frac{1}{\det(L)}$

Démonstration. On remarque que $L^{\#}$ est le réseau engendré par la base duale de la base de L (la base duale de (e_i) est la base (f_i) telle que $e_i \cdot f_j = \delta_{ij}$, avec δ le symbole de Kronecker. En effet, si B est la matrice de la base de L, c'est-à-dire $L = B\mathbb{Z}^n$, on a $x \in L^{\#} \iff B^T x \in \mathbb{Z}^n \iff x \in (B^T)^{-1}\mathbb{Z}^n$. Comme on a $\det(L) = \det(B)^2$, on a l'égalité. □

Propriété 4.3.3. *Soit L un réseau entier. Les sur-réseaux de L inclus dans $L^{\#}$ sont en bijection avec les sous-groupes du quotient $L^{\#}/L$, qui est un groupe abélien de cardinal* $\det(L)$.

Démonstration. Le premier énoncé est un résultat classique d'algèbre des groupes, la projection canonique induit cette bijection. Il n'y a donc qu'à démontrer que $L^{\#}/L$, automatiquement abélien car quotient de groupes abéliens, est de cardinal $\det(L)$. On remarque d'abord que si $L \subseteq L'$ sont deux réseaux de rang n, $\mid L'/L \mid^2 = \frac{\det(L)}{\det(L')}$. En effet, en se plaçant dans une maille de L, les classes d'équivalences de L' modulo L sont exactement les mailles de L' qui se trouvent dans la maille de L, c'est-à-dire le rapport des volumes. En appliquant à $L' = L^{\#}$, on a directement $\mid L^{\#}/L \mid = \det(L)$ □

On aura aussi besoin de regarder des sur-réseaux de rang supérieur. Si L est un sous réseau de L' et que le rang de L est strictement inférieur au rang de L', remarquons que la notion de dual de L est en fait définie sur le sous-espace $\mathrm{Vect}\, L$. On n'aura besoin dans la preuve du théorème des 15 que de réseaux de dimension $n+1$ si L est de dimension n et on montre le résultat suivant :

Propriété 4.3.4. *On considère L de rang n et un sur-réseau L' de rang $n+1$. Alors il existe un vecteur non-nul dans L' orthogonal à L. En particulier il en existe un de norme minimale.*

Démonstration. On prend un vecteur u dans L' qui n'est pas dans $\mathrm{Vect}(L)$. On a $L + \mathbb{Z}u \in L'$, on va donc chercher le vecteur orthogonal dans $L + \mathbb{Z}u$. Considérons u' le projeté orthogonal de u sur $\mathrm{Vect}(L)$. Pour tout x dans L, on a $u' \cdot x = u \cdot x$, on en déduit $u' \in L^{\#}$ car $u' \in \mathrm{Vect}(L)$ et $u' \cdot x$ est toujours entier pour $x \in L$ vu que L' est entier.

On remarque maintenant que si B est la matrice de la base de L dans $\mathrm{Vect}(L)$, BB^T est à coefficients entiers, donc $(B^T)^{-1}B^{-1}$ est à coefficients rationnels, ce qui signifie que les colonnes de $(B^T)^{-1}$ (la base de $L^{\#}$) s'expriment comme combinaison rationnelle des colonnes de B. En particulier il existe un entier m tel que $mu' \in L$. On a alors $mu - mu' \in L'$ et pas dans L sinon $u \in \mathrm{Vect}(L)$, en particulier il est non nul. De plus $(mu - mu') \cdot x = 0$ pour tout x dans L, donc est dans l'orthogonal de L : on a fini. □

5 Escalades

Nous démontrons maintenant le théorème des 15. Le coeur de la preuve repose sur la notion d'*escalade.*

Définition 5.0.1. *Pour L un réseau entier, on appelle* ***truand*** *de L le plus petit $n > 0$ non représenté par L s'il existe. On le note $t(L)$. Si L' un réseau entier peut s'écrire (à isomorphisme près) $L + \mathbb{Z}u$ avec $u \notin \mathrm{Vect}\, L$ de norme n on dit que L' est une* ***escalade*** *de L. On dit plus généralement que L' est une escalade si elle est obtenue par escalades successives du réseau trivial.*

Cette définition encapsule l'idée d'ajout de vecteur. La condition $u \notin \mathrm{Vect}\, L$ assure que u concaténé à une base de L forme une base de L', ce qui permet d'exprimer aisément une matrice de Gram de L' à partir d'une de L. Remarquons que si une forme quadratique représente $x > 0$ alors elle représente les $n^2 x$. de la sorte un truand est nécessairement sans facteur carré : si t est le truand et $t = d^2 s$ avec $d > 1$, alors s est représenté et donc t également. On parlera abusivement d'une matrice symétrique définie positive comme d'une escalade si le réseau associé en est une.

Il se trouve que l'on peut déterminer exactement les escalades, ce qui nous permettra ensuite de montrer le théorème des 15 en s'y ramenant.

5.1 Escalades de petite dimension

Le truand de $\{0\}$ est 1 donc l'unique escalade de $\{0\}$ est $\mathbb{Z}$ à isomorphisme près. Prenant $e = 1$ pour base de $\mathbb{Z}$, une escalade E de $\mathbb{Z}$ admet (e, u) pour partie génératrice avec u de norme 2. Elle admet donc une matrice de Gram de la forme

$$\begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}$$

avec $a \in \mathbb{Z}$. Comme la matrice doit être positive il vient $|a| \leq 1$ et quitte à changer u en $-u$ on peut supposer $a \geq 0$. Ainsi E admet comme matrice de Gram une des deux matrices $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. Dans le second cas, changeant u en $u - e$, on obtient pour matrice de Gram I_2 ! Les deux matrices obtenues définissent manifestement des réseaux non isomorphes qui sont les escalades de $\mathbb{Z}$.

Un raisonnement similaire permet de calculer explicitement les escalades de ces deux réseaux : celles-ci sont données par les matrices de Gram suivantes :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$$

À défaut d'être universels, ces réseaux représentent une grande quantité d'entiers. Tous sauf le dernier sont en effet uniques en leur genre et des vérifications p-adiques à l'aide des outils donnés par les propositions 3.2.6 et 3.2.7 permettent d'aboutir à la table 1. Pour vérifier le caractère unique en leur genre de ces réseaux, et plus généralement dans ce mémoire, on se réfère aux données tabulées par Brandt, Intrau et Schiemann, publiées par Nebe [7].

Pour le dernier réseau, on peut trouver des sous-réseaux de matrices de Gram

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 1 & 2 & 8 \end{pmatrix}, \begin{pmatrix} 2 & -2 & 2 \\ -2 & 5 & 2 \\ 2 & 2 & 8 \end{pmatrix}, \begin{pmatrix} 3 & 0 & 0 \\ 0 & 5 & 4 \\ 0 & 4 & 5 \end{pmatrix}$$

. On vérifie que la première de ces trois matrices est unique en son genre et que les deux autres constituent un genre. Une analyse locale permet alors de compléter la table 1 jointe en annexe.

5.2 La quatrième escalade

Le fait que les escalades de taille 3 représentent beaucoup d'entiers va *in fine* assurer que leurs escalades sont pour la plupart universelles.

Considérons par exemple les escalades de L le réseau associé à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ cette matrice représente tous les entiers pas de la forme $9^x(9y+6)$ et est de truand 6. Soit une escalade L' de L ; comme $\operatorname{Vect} L \subset \operatorname{Vect} L'$, on considère v une base de l'orthogonal de L dans L'. Soit $m > 0$ sa norme.

Soit t l'*éventuel* truand de L'. Alors t est sans facteur carré et est non représenté par L. De la sorte $t \equiv 6 \pmod 9$ et est sans facteur carré. Si $m \not\equiv 0, 6$ et $m \geq t$ alors remarquons que $t - m$ est représenté par L puisque $t - m \not\equiv 0, 6$. De la sorte on a $u \in L$ de norme $t-m$ et $u+v$ est de norme t, ce qui est absurde. Ainsi, si $m \not\equiv 0, 6$ et L' n'est pas universelle alors $t < m$.

Si $m \equiv 6 \pmod 9$, supposons que $t \geq 4m$. On remarque que $t-m$ et $t-4m$ sont deux multiples de 9 et que, m étant de valuation 3-adique 1, ces nombres sont distincts modulo 27. Ainsi l'un d'entre eux n'est pas multiple de 27 mais vu les nombres représentés par L, il est représenté par ce réseau, via $u \in L$. Quitte à considérer $u + v$ ou $u + 2v$ on conclut à l'absurde, donc que si t existe et $m \equiv 6$ alors $t < 4m$.
Si $9 \mid m$, le raisonnement ci-dessus ne s'adapte pas de manière satisfaisante : cela laisse l'opportunité d'existence d'une *escalade pathologique.*

Calculant les escalades de L, puis un m convenables pour chaque, puis appliquant ce qu'il vient d'être démontré, on conclut que toutes les escalades de L sont universelles ! Ces calculs sont réalisables par ordinateur. Au cas où une escalade de L ne serait pas pathologique mais aurait un petit truand on la qualifie d'escalade *difficile*. Une escalade ni pathologique ni difficile est qualifiée de *facile*.

Des raisonnements semblables s'appliquent sur toutes les escalades de taille 3 (voir table 1) sauf sur

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

pour lesquels on obtient des escalades pathologiques. En outre,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

donnent lieu à des escalades difficiles, regroupées figure 5. Celles-ci ratent *de*

facto un seul entier en dessous du seuil de vérification. On remarque qu'alors leurs escalades sont automatiquement universelles. En effet, si L est une escalade difficile susmentionnée de L_0, et L' escalade L, alors le raisonnement appliqué entre L_0 et L reste valide entre L et L' ! C'est dû au fait que L représente tout entier représenté par L_0. Cela assure l'existence du même plafond M pour les truands de L' que celui obtenu pour L. Or, L représentant tout sauf un entier k en dessous de M, on a $k = t(L)$. De la sorte k est représenté par L', et tout entier $k \neq \ell \leq M$ est représenté par L donc L'. On conclut que L' est universelle ! En fait, cela vaut si l'on suppose seulement que L' est un surréseau entier de L représentant son truand.

On introduit alors la notion de réseau *quasi-universel* : ce sont les réseaux non-universels dont tous les sur-réseaux entiers représentant leur truand sont universels. De la sorte, les escalades difficiles des escalades de taille 3 sont toutes quasi-universelles.

Les escalades pathologiques sont détaillées figures 3 et 4. On remarque que certaines escalades pathologiques sont également obtenues comme escalades faciles d'une autre escalade de rang 3. Celles-ci sont alors universelles. Pour les autres L, regroupés figure 4, on cherche un sous-réseau unique en son genre L_0 de L tel qu'un argument comme l'argument général, dans son cas non-pathologique, s'applique. On se réfère pour cela aux données de Nebe et aux propriétés 3.2.6 et 3.2.7, qui ne s'appliquent qu'après des calculs. Il est faux en général alors que L est une escalade de L_0, mais ce n'est pas essentiel. Cela permet de montrer que la plupart des réseaux pathologiques sont universels, excepté

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 1 & 5 \end{pmatrix}$$

Pour le premier, l'argumentaire qui vient d'être développé doit être sensiblement raffiné. Pour les autres, on remarque que l'argument donné pour les escalades difficiles précédemment s'adapte et assure que ces escalades sont quasi-universelles.

Pour traiter

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 7 \end{pmatrix}$$

qui est universelle, l'argument employé est plus subtil que pour les autres matrices pathologiques. On remarque en fait qu'en la considérant comme escalade de $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ on peut appliquer l'argument non-pathologique si l'on suppose que l'éventuel truand est impair. De même, avec le sous-réseau vu dans la figure 4, on peut appliquer à nouveau cet argument si l'on suppose l'éventuel

truand pair. La conjonction de ces deux preuves et deux vérifications permettent d'aboutir à l'universalité.

De la sorte on connait exactement les escalades : elles sont de dimension au plus 5 et on peut, si on le souhaite, les énumérer. Cette énumération, déjà faite pour mener à bien les calculs précédents, va à travers les quelques propriétés techniques suivantes nous permettre de conclure.

Propriété 5.2.1. *Soit L une escalade non universelle. Supposons de plus qu'elle admette un sur-réseau entier L' représentant son truand, et que L' soit lui-aussi non-universel. Alors L' a un rang strictement supérieur à celui de L.*

Démonstration. Considérons le cas où $\det L$ est sans facteur carré. Supposons par l'absurde L' du même rang que L. Comme vu dans la preuve de la propriété 4.3.3, on a $\det L = \det(L')|L'/L|^2$, donc $|L'/L|^2 > 1$ est un diviseur carré de $\det L$. Comme celui-ci n'en a pas par hypothèse, on conclut par l'absurde. Reste le cas où $\det L$ admet en effet un facteur carré. Examinant les tables, il vient qu'à équivalence près on peut supposer que L est donnée par

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

Supposons être dans le premier cas, les autres étant similaires, si ce n'est un peu plus calculatoires. Dans celui-ci $\det L = 9$. Comme alors $9 = \det(L')|L'/L|^2$, on déduit que $|L'/L| = 3$ et $\det L' = 1$. Soit $u \in L'$ représentant 7, le truand de L. Comme $|L'/L| = 3$, on a $3u \in L$ par Lagrange. De la sorte on déduit que L représente $9 \cdot 7 = 63$. Consultant les tables, on est tentés de regarder modulo 8 ce fait. On remarque alors que L ne saurait représenter 63, ce qui conclut. □

On aboutit alors au désiré :

Théorème 5.2.2 (théorème des 15)**.** *Tout réseau entier représentant les entiers de $I = \{1, 2, 5, 6, 7, 10, 14, 15\}$ est universel.*

Démonstration. On remarque que I est en fait l'ensemble des truands des escalades non universelles.

Soit L représentant tout I. Comme $\{0\} \subseteq L$ et que les escalades sont de dimension au plus 5, on peut considérer $L' \subseteq L$ escalade de dimension maximale. Si $L = L'$, vu I, il vient que L est universel. Supposons $L \neq L'$. Si L' est universel, L l'est également ; supposons dorénavant L' non universelle. Si L' est quasi-universel, comme son truand est dans I donc représenté par L sur-réseau entier de L', L est universel.

Supposons être dans le cas où L n'est ni universelle ni quasi-universelle. On montre que celui-ci ne peut arriver par l'absurde. Par la proposition précédente,

L' n'a pas de surréseau entier strict de même rang. Soit $u \in L$ représentant $t(L')$. On a $u \notin L'$ et $L' + \mathbb{Z}u$ est un réseau entier. Ainsi $u \notin \text{Vect}\, L'$. Cela assure que $L' + \mathbb{Z}u$ est une escalade de L' dans L. Or c'est absurde par maximalité de la dimension de L'. Cela conclut. □

Il suit que tout réseau universel admet comme sous-réseau une escalade universelle ou quasi-universelle. Or celles-ci sont de rang au moins 4. Les escalades universelles étant de dimension au moins 4 au vu de notre étude, il suit que tout réseau universel est de dimension au moins 4. On retrouve un théorème de Conway :

Théorème 5.2.3 (Conway)**.** *Aucune forme quadratique ternaire n'est universelle.*

6 Méthodes de calcul

Dans cette annexe, on détaille les méthodes permettant d'obtenir les tables précédentes, c'est-à-dire comment énumérer les escalades dans une forme plus facile à manipuler, et comment reconnaître deux formes équivalentes.

On pourrait énumérer les escalades brutalement, en ajoutant le truand dans le coin inférieur droit de la matrice de Gram et en bornant les autres coefficients par Cauchy-Schwarz, mais on va préférer borner plus précisément les coefficients non-diagonaux, et trouver ensuite une borne sur la norme du vecteur ajouté. On a alors des meilleures bornes et moins de calculs : le programme donne moins de matrices, il y a donc moins d'équivalences à chercher à la main.

Prenons d'abord le cas où l'escalade de taille 3 est diagonale. On ajoute un vecteur dont la norme est le truand, ce qui donne une nouvelle ligne (d, c, b, a) à la matrice de Gram. En faisant la transvection $e_4 \mapsto e_4 - e_i$ suffisamment de fois, on peut diminuer la valeur de d, c, b de sorte à ce que $|d|$ soit inférieur à la moitié du premier coefficient diagonal, et ainsi de suite. Ensuite on les rend positifs en changeant le vecteur associé en son opposé. Comme le premier coefficient est toujours 1, on peut garantir $d = 0$ et borner très efficacement c et b.

Continuons en prenant l'exemple de l'escalade de $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Son truand est 7, on peut donc écrire $7 = x^2 + 2y^2 + 2z^2 + aw^2 \pm 2wz \pm 2wy \geq x^2 + 2y^2 + 2z^2 + aw^2 - w^2 - z^2 - w^2 - y^2 \geq (a-2)w^2$. On a $w \neq 0$ car 7 n'est pas représenté par l'escalade de dimension 3, on en déduit $a \leq 9$. Par une méthode similaire, on arrive toujours à borner les coefficients b et c, puis a par $t + b^2 + c^2$ où t vaut le truand.

Regardons maintenant le cas où le réseau de départ n'est pas diagonal, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}$. Un changement de variables similaire permet de ramener le vecteur (c, b) dans n'importe quelle maille du réseau engendré par $(2, 1)$ et $(1, 4)$ (resp. $(1, 5)$). On peut donc ramener (c, b) dans la maille décrite par $t(2, 1) + s(1, 4)$ avec $0 \leq t, s \leq 1$ (resp. $t(2, 1) + s(1, 5)$). Une vérification manuelle sur chacun des points entiers montre ensuite que l'on peut finalement ramener (c, b) dans le pavé défini par les conditions $0 \leq c \leq 1, 0 \leq b \leq 4$ (resp. $0 \leq b \leq 5$).

Mentionnons que cette méthode d'énumération, simple et exhaustive, énumère plusieurs fois certaines classes d'équivalences de réseaux. Afin de synthétiser les résultats, nous avons regroupé les escalades d'intérêt par déterminant et tenté, parmi les escalades de même déterminant, de les montrer équivalentes, ce qui s'obtenait par quelques transvections dans chaque cas.

7 Bibliographie

Références

[1] John William Scott Cassels. *Rational Quadratic Forms*. Academic Press Inc. (London) Ltd., 1978. isbn : 978-0-486-46670-5.

[2] Jean-Pierre Serre. *Cours d'arithmétique*. 1994. isbn : 978-2-13-041835-1.

[3] Manjul Bhargava. « On the Conway–Schneeberger fifteen theorem ». In : *Quadratic forms and their applications (Dublin, 1999)*. American Mathematical Society, 2000, p. 27-37.

[4] John Horton Conway. « Universal quadratic forms and the fifteen theorem ». In : *Quadratic forms and their applications (Dublin, 1999)*. American Mathematical Society, 2000, p. 23-26.

[5] Wolfgang Ebeling. *Lattices and Code. A Course Partially Based on Lectures by Friedrich Hirzebruch*. Springer Spektrum Wiesbaden, 2013. isbn : 978-3-658-00359-3.

[6] Manjul Bhargava et Jonathan Hanke. *Universal quadratic forms and the 290-theorem*.

[7] Gabriele Nebe. *The Brandt-Intrau-Schiemann Table of Odd Ternary Quadratic Forms*. url : `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_1.html`.

Escalade	Représente tout sauf peut-être	Truand	Déterminant
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$4^n(8k+7)$	7	1
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$4^n(16k+14)$	14	2
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	$9^n(9k+6)$	6	3
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$4^n(8k+7)$	7	4
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	$4^n(16k+10)$	10	6
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$	$4^n(16k+14)$	14	8
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}$	$4^n(8k+7)$	7	9
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$	$25^n(25k+10,15)$	10	10
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$	$49^n(49k+21,35,42)$ et $12k+7,10$	7	7

FIGURE 1 – Escalades de taille 3

Escalade	Déterminant
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$	50
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 5 & 1 \\ 0 & 1 & 1 & 5 \end{pmatrix}$	43
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 5 & 1 \\ 0 & 1 & 1 & 9 \end{pmatrix}$	83
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 5 & 2 \\ 0 & 1 & 2 & 8 \end{pmatrix}$	67

FIGURE 2 – Escalades difficiles des précédentes, échouant la vérification finale pour 15 seulement (par classes d'équivalences)

Escalade	Est une escalade facile de
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 2 \\ 0 & 0 & 2 & 5 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 3 \\ 0 & 0 & 3 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 2 & 5 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$

FIGURE 3 – Escalades pathologiques visibles comme escalades faciles

Escalade	Nouveau réseau de rang 3	Déterminant	Conclusion
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix}$	8	universel
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 7 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 7 \end{pmatrix}$	24	universel
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 2 & 13 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 13 \end{pmatrix}$	96	universel
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 4 & 0 \\ 0 & 1 & 0 & 4 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 4 & 0 \\ 1 & 0 & 4 \end{pmatrix}$	24	universel
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 4 & 0 \\ 0 & 1 & 0 & 7 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 10 \end{pmatrix}$	45	universel, raisonnement spécial
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	21	échec de la vérif. en 10
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 1 & 5 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$	33	échec de la vérif. en 10

FIGURE 4 – Escalades pathologiques restantes (par classes d'équivalences)