



HAL
open science

Variétés abéliennes et théorème de Minkowski-Hlawka

Pascal Autissier

► **To cite this version:**

Pascal Autissier. Variétés abéliennes et théorème de Minkowski-Hlawka. *Manuscripta mathematica*, 2016, 149 (3-4), pp.275-281. 10.1007/s00229-015-0791-1 . hal-01022915

HAL Id: hal-01022915

<https://hal.science/hal-01022915v1>

Submitted on 11 Jul 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Variétés abéliennes et théorème de Minkowski-Hlawka

Pascal Autissier

11 juillet 2014

Abstract : A classical theorem of Minkowski and Hlawka states that there exists a lattice in \mathbb{R}^n with packing density at least 2^{1-n} . Buser and Sarnak proved the analogue of this result in the context of complex abelian varieties. Here we give an improvement of this analogue; this shows a conjecture of Muetzel.

Résumé : Un théorème classique de Minkowski et Hlawka montre l'existence d'un réseau de \mathbb{R}^n à densité d'empilement $\geq 2^{1-n}$. Buser et Sarnak ont établi l'analogie de ce résultat dans le cadre des variétés abéliennes complexes. On donne ici une amélioration de cet analogue; cela prouve une conjecture de Muetzel.

2010 Mathematics Subject Classification : 11H31, 14K20.

1 Introduction

Un problème important de la Géométrie des Nombres est l'étude de la plus grande densité d'empilement des réseaux d'un espace euclidien E de dimension $n \geq 1$. Rappelons que si Γ est un réseau de E de premier minimum $\lambda_1(\Gamma)$, sa densité d'empilement $\Delta(\Gamma)$ est la densité de l'empilement de boules de rayon $\frac{\lambda_1(\Gamma)}{2}$ centrées en les points de Γ . Le problème en question est alors d'estimer $\Delta_n = \sup\{\Delta(\Gamma) ; \Gamma \text{ réseau de } E\}$.

La valeur exacte de Δ_n n'est établie que pour certains petits entiers n , et le comportement asymptotique de Δ_n lorsque n tend vers $+\infty$ reste mystérieux. Le fameux théorème de Minkowski-Hlawka donne l'inégalité $\Delta_n \geq \frac{1}{2^{n-1}}$ pour tout $n \geq 1$. La meilleure minoration générale connue (à la valeur de la constante c près) est due à Rogers [8] en 1947 :

Théorème (Rogers) : *En posant $c = \frac{2}{e}$, on a $\Delta_n \geq \frac{cn}{2^n}$ pour tout entier $n \geq 1$.*

La constante c a été améliorée successivement par Davenport-Rogers [4], Ball [1], Venkatesh [10]. Ce dernier obtient $\Delta_n \geq \frac{c'n}{2^n}$ pour tout n assez grand, avec $c' = 65963$. Dans le même article, il montre également le résultat suivant :

Théorème (Venkatesh) : *Il existe une infinité d'entiers $n \geq 3$ vérifiant l'inégalité $\Delta_n \geq \frac{n}{2^{n+1}} \ln \ln n$.*

À titre de comparaison, la meilleure majoration générale connue est celle de Kabatyanskii et Levenshtein [6], qui est de la forme $\Delta_n \leq C^n$ pour tout n assez grand, avec $C = 0,661$.

On s'intéresse dans ce travail à l'analogie de ce problème dans le contexte des variétés abéliennes complexes.

Soit $(A; L)$ une variété abélienne complexe de dimension $g \geq 1$, principalement polarisée. Posons $T_A = \Gamma(A; \Omega_{A/\mathbb{C}})^\vee$ et désignons par Γ_A le réseau des périodes de A (on a donc un isomorphisme $A(\mathbb{C}) \simeq T_A/\Gamma_A$ de groupes analytiques). La polarisation L induit une forme de Riemann $\langle ; \rangle$ sur T_A , *i.e.* un produit scalaire hermitien sur T_A tel que $\text{Im}\langle \gamma_1; \gamma_2 \rangle \in \mathbb{Z}$ pour tout $(\gamma_1; \gamma_2) \in \Gamma_A^2$.

Définition : Le **volume d'injectivité** $V(A; L)$ de $(A; L)$ est la densité d'empilement du réseau Γ_A dans l'espace euclidien $(T_A; \text{Re}\langle ; \rangle)$. De manière équivalente, $V(A; L)$ est le plus grand volume d'une boule ouverte de T_A qui s'injecte dans A (le volume est normalisé de sorte que Γ_A soit de covolume 1).

Étant donné un entier $g \geq 1$, on note \mathcal{A}_g l'espace de modules (grossier) des schémas abéliens de dimension relative g et principalement polarisés. On cherche ici à minorer $V_g = \sup\{V(A; L) ; (A; L) \in \mathcal{A}_g(\mathbb{C})\}$. On a trivialement l'inégalité $V_g \leq \Delta_{2g}$. Buser et Sarnak [3] ont montré l'équivalent du théorème de Minkowski-Hlawka dans ce cadre :

Théorème (Buser, Sarnak) : *Pour tout entier $g \geq 1$, on a $V_g \geq \frac{1}{2^{2g-1}}$.*

On se propose ici de raffiner ce résultat pour certaines valeurs de g . On désigne par φ la fonction indicatrice d'Euler.

Théorème 1.1 : *Soit m un entier ≥ 3 ; posons $g = \varphi(m)$. On a la minoration $V_g \geq \frac{m}{4^g}$.*

Tirons quelques conséquences du théorème 1.1. Muetzel conjecture dans [7] (voir sa conjecture 2.5) l'estimation $4^g V_g \geq 2g$ lorsque g est une puissance de 2. On obtient ici une version améliorée de cet énoncé :

Corollaire 1.2 : *(α) Soit g un entier ≥ 2 qui est une puissance de 2. On a $4^g V_g \geq 3g$.
(β) Soit g un entier de la forme $g = \varphi(n)$ pour un entier $n \geq 3$. On a $4^g V_g \geq 2g + 2$.*

Ce résultat suggère que V_g admet peut-être une minoration semblable à celle de Rogers :

Question : Si g est un entier ≥ 2 , a-t-on $4^g V_g \geq 2g + 2$?

On déduit aussi de l'énoncé 1.1 un analogue (ou plutôt un raffinement, au vu de la majoration $V_g \leq \Delta_{2g}$) du théorème de Venkatesh :

Corollaire 1.3 : *Notons ici γ la constante d'Euler. Il existe un réel c et une infinité d'entiers g tels que $4^g V_g \geq e^\gamma g \ln \ln g - cg$.*

La démonstration du théorème 1.1 repose sur un argument de valeur moyenne sur un certain espace de réseaux, inspiré de la méthode classique de Minkowski-Hlawka. Plus précisément, on considère des réseaux $\Gamma \subset \mathbb{C}^g$ munis d'une action libre d'un groupe cyclique d'ordre m et tels que \mathbb{C}^g/Γ soit une variété abélienne ayant un anneau d'endomorphismes de rang $\geq \frac{g}{2}$ (voir remarque 4.1).

Je remercie Renaud Coulangeon pour m'avoir fourni la référence [10]. Je remercie également Gaël Rémond pour ses commentaires sur ce travail.

2 Rappels

Soit n un entier ≥ 1 . Munissons \mathbb{R}^n de la norme euclidienne usuelle, notée $\| \cdot \|$, et de la mesure de Lebesgue. On désigne par v_n le volume de la boule unité de \mathbb{R}^n , de sorte que $v_n = \frac{\pi^{n/2}}{(n/2)!}$.

Soit Γ un réseau de \mathbb{R}^n de covolume 1. Le premier minimum de Γ est par définition le réel $\lambda_1(\Gamma) = \min_{\gamma \in \Gamma - \{0\}} \|\gamma\|$. La densité d'empilement $\Delta(\Gamma)$ de Γ est la densité de l'empilement de boules de rayon $\frac{\lambda_1(\Gamma)}{2}$ centrées en les points de Γ . On a donc la formule $\Delta(\Gamma) = \frac{v_n}{2^n} \lambda_1(\Gamma)^n$.

Soit g un entier ≥ 1 . On considère maintenant \mathbb{C}^g muni du produit scalaire hermitien standard (\mathbb{C} -linéaire à gauche par convention) noté $\langle ; \rangle$, et de la mesure de Lebesgue.

Soit Γ un réseau (de rang $2g$) de \mathbb{C}^g tel que $\text{Im}\langle \gamma; \gamma' \rangle \in \mathbb{Z}$ pour tout $(\gamma; \gamma') \in \Gamma^2$. Le tore \mathbb{C}^g/Γ est alors une variété abélienne complexe, et la forme de Riemann $\langle ; \rangle$ induit une polarisation L sur \mathbb{C}^g/Γ . Posons $\Gamma' = \{\gamma' \in \mathbb{C}^g \mid \forall \gamma \in \Gamma \text{ Im}\langle \gamma; \gamma' \rangle \in \mathbb{Z}\}$; c'est un réseau de \mathbb{C}^g contenant Γ . Si $\Gamma' = \Gamma$, alors la polarisation L est principale et Γ est de covolume 1.

Pour des précisions sur les polarisations, on pourra consulter [2] pages 69-74.

3 Préliminaires

Soient m un entier ≥ 3 et $\zeta \in \overline{\mathbb{Q}}$ une racine m -ième primitive de l'unité. On pose $g = \varphi(m)$ et on plonge $K = \mathbb{Q}(\zeta)$ dans \mathbb{C}^g via les g plongements complexes de K . On désigne par E le sous-espace vectoriel réel de \mathbb{C}^g engendré par K . Observons que E est en fait un sous-anneau de \mathbb{C}^g identifié à $K \otimes_{\mathbb{Q}} \mathbb{R}$, et que $\mathbb{C}^g = E \oplus iE$.

Pour tout $z = (z_1; \dots; z_g) \in \mathbb{C}^g$, on note $\bar{z} = (\bar{z}_1; \dots; \bar{z}_g)$ son conjugué complexe. Remarquons que K , O_K et E sont stables par cette conjugaison (car $\bar{\zeta} = \zeta^{-1}$). En outre, le produit scalaire hermitien standard $\langle ; \rangle$ sur \mathbb{C}^g est à valeurs réelles sur E^2 , donc fait

de E un espace euclidien. Plus précisément, on a $\langle a; b \rangle = \text{Tr}(a\bar{b})$ pour tout $(a; b) \in K^2$, où $\text{Tr} : K \rightarrow \mathbb{Q}$ désigne la trace.

Notons G le sous-groupe (cyclique d'ordre m) de O_K^* engendré par ζ . On définit une action \mathbb{R} -linéaire de G sur $\mathbb{C}^g = E \oplus iE$ par $g * (x + iy) = gx + i\bar{g}y$ pour tout $(g; x; y) \in G \times E^2$. Cette action est libre sur $\mathbb{C}^g - \{0\}$.

Lemme 3.1 : *Soient $g \in G$ et $z \in \mathbb{C}^g$. On a $\|g * z\| = \|z\|$.*

Démonstration : Écrivons $z = x + iy$ avec x et y dans E . On a alors $\|z\|^2 = \|x\|^2 + 2\text{Re}(i\langle y; x \rangle) + \|y\|^2 = \|x\|^2 + \|y\|^2$. En utilisant l'égalité $|\sigma(g)| = 1$ pour tout plongement $\sigma : K \hookrightarrow \mathbb{C}$, on obtient $\|gx\|^2 = \|x\|^2$. On en conclut que $\|g * z\|^2 = \|gx + i\bar{g}y\|^2 = \|gx\|^2 + \|\bar{g}y\|^2 = \|x\|^2 + \|y\|^2 = \|z\|^2$. \square

Désignons par I la codifférente de O_K , c'est-à-dire l'idéal fractionnaire défini par $I = \{a \in K \mid \text{Tr}(aO_K) \subset \mathbb{Z}\}$. On sait que $\{b \in K \mid \text{Tr}(bI) \subset \mathbb{Z}\} = O_K$ et que I est un réseau de E . En outre, on voit aisément que I est stable par conjugaison complexe.

Lemme 3.2 : *Soit $f : E \rightarrow E$ une application \mathbb{R} -linéaire symétrique. Soit r un réel > 0 . Considérons le réseau*

$$\Gamma = rI + \left(rf + \frac{i}{r}\text{Id} \right) (O_K) = \left\{ ra + rf(b) + \frac{i}{r}b ; (a; b) \in I \times O_K \right\} \text{ de } \mathbb{C}^g.$$

(α) *Le tore \mathbb{C}^g/Γ est une \mathbb{C} -variété abélienne principalement polarisée.*

(β) *Soit $x \in E$. Si f est l'application $\begin{matrix} E \rightarrow E \\ y \mapsto x\bar{y} \end{matrix}$, alors f est symétrique, et Γ est stable sous l'action de G .*

Démonstration : (α) Vérifions que $\langle ; \rangle$ est une forme de Riemann. Soient $(a; a'; b; b') \in I^2 \times O_K^2$; posons $\gamma = ra + rf(b) + \frac{i}{r}b$ et $\gamma' = ra' + rf(b') + \frac{i}{r}b'$. On a alors

$$\text{Im}\langle \gamma; \gamma' \rangle = \langle b; a' \rangle + \langle b; f(b') \rangle - \langle a; b' \rangle - \langle f(b); b' \rangle = \text{Tr}(ba') - \text{Tr}(a\bar{b}') \in \mathbb{Z} . \quad (*)$$

Le quotient \mathbb{C}^g/Γ est donc une variété abélienne polarisée.

Montrons que la polarisation est principale. Posons $\Gamma' = \{\gamma' \in \mathbb{C}^g \mid \forall \gamma \in \Gamma \text{ Im}\langle \gamma; \gamma' \rangle \in \mathbb{Z}\}$. Le réseau Γ est d'indice fini dans Γ' , ce qui implique $\Gamma' \subset \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$. Soit $\gamma' \in \Gamma'$; il existe donc $(a'; b') \in K^2$ tel que $\gamma' = ra' + rf(b') + \frac{i}{r}b'$.

Pour tout $b \in O_K$, on a $\text{Tr}(a'b) = \text{Im}\langle rf(\bar{b}) + \frac{i}{r}\bar{b}; \gamma' \rangle \in \mathbb{Z}$ par un calcul similaire à (*), donc $a' \in I$. De même, on a $\text{Tr}(b'a) = -\text{Im}\langle r\bar{a}; \gamma' \rangle \in \mathbb{Z}$ pour tout $a \in I$, ce qui donne $b' \in O_K$. D'où $\gamma' \in \Gamma$. On a bien prouvé que $\Gamma' = \Gamma$, *i.e.* que la polarisation est principale.

(β) On suppose maintenant que f est l'application qui à $y \in E$ associe $x\bar{y}$. Soit $(y; z) \in E^2$. En écrivant par coordonnées les vecteurs x , y et z de \mathbb{C}^g , on trouve

$$\langle y; f(z) \rangle = \langle f(z); y \rangle = \sum_{k=1}^g x_k \bar{z}_k \bar{y}_k = \langle f(y); z \rangle .$$

Ainsi f est-elle symétrique. Soient $g \in G$ et $(a; b) \in I \times O_K$; on pose $\gamma = ra + rf(b) + \frac{i}{r}b$. On a $g * \gamma = g(ra + rx\bar{b}) + \frac{i}{r}\bar{g}b = rga + rf(\bar{g}b) + \frac{i}{r}\bar{g}b \in \Gamma$. D'où la G -stabilité de Γ . \square

On choisit un domaine fondamental F du réseau I dans E , et un domaine fondamental F' de O_K . Désignons par ν la mesure de Lebesgue sur E , normalisée de sorte que la boule unité dans E soit de volume v_g . Avec cette normalisation, la mesure image de $\nu \times \nu$ par l'application $h : \begin{matrix} E^2 \rightarrow \mathbb{C}^g \\ (x; y) \mapsto x + iy \end{matrix}$ s'identifie à la mesure de Lebesgue usuelle sur \mathbb{C}^g .

Regardons le réseau Γ du lemme 3.2 avec $f = 0$: ce réseau $\Gamma = h(rI \times \frac{1}{r}O_K)$ est de covolume $\nu(rF)\nu(\frac{1}{r}F')$ d'une part, et de covolume 1 d'autre part. On en déduit que $\nu(F)\nu(F') = 1$.

Lemme 3.3 : Soient $b \in O_K - \{0\}$, $z \in \mathbb{C}^g$ et $r \in \mathbb{R}_+^*$. Soit $\chi : \mathbb{C}^g \rightarrow \mathbb{C}$ une application telle que la fonction $E \rightarrow \mathbb{C}$ qui à x associe $\chi(x + z)$ soit intégrable et à support compact. On a l'égalité

$$\int_F \sum_{a \in I} \chi(ra + rxb + z) d\nu(x) = \frac{1}{r^g} \int_E \chi(x + z) d\nu(x) \quad .$$

Démonstration : L'application $\psi : E \rightarrow \mathbb{C}$ qui à x associe $\sum_{a \in I} \chi(ra + rx + z)$ est I -périodique, et la multiplication par b induit un revêtement $E/I \rightarrow E/I$. La formule de changement (linéaire) de variable donne $\int_{E/I} \psi(bx) d\nu(x) = \int_{E/I} \psi(x) d\nu(x)$. On en déduit que

$$\int_F \psi(xb) d\nu(x) = \sum_{a \in I} \int_F \chi(ra + rx + z) d\nu(x) = \int_E \chi(rx + z) d\nu(x) = \frac{1}{r^g} \int_E \chi(x + z) d\nu(x) \quad .$$

D'où le résultat. \square

4 Démonstration du théorème 1.1

On conserve les notations de la partie 3. Soit ε un réel vérifiant $0 < \varepsilon < m$. On va prouver l'existence d'une \mathbb{C} -variété abélienne principalement polarisée $(A; L)$ telle que $V(A; L) > \frac{m - \varepsilon}{4g}$. Lorsque $z \in \mathbb{C}^g$, on pose $\chi(z) = 1$ si $v_{2g} \|z\|^{2g} \leq m - \varepsilon$ et $\chi(z) = 0$ sinon. Pour tout réel $r > 0$, on pose

$$J(r) = \frac{\nu(F')}{r^g} \sum_{b \in O_K - \{0\}} \int_E \chi\left(x + \frac{i}{r}b\right) d\nu(x) \quad .$$

$J(r)$ est une somme de Riemann, donc $J(r)$ converge vers $\int_E \int_E \chi(x + iy) d\nu(x) d\nu(y) = m - \varepsilon$ lorsque r tend vers $+\infty$. En particulier, il existe un réel $r_0 > 0$ vérifiant $J(r_0) < m$

et $v_{2g}(r_0\lambda_1(I))^{2g} > m - \varepsilon$.

On définit une application $N : \mathbb{R}^g \rightarrow \mathbb{N}$ par la formule

$$\forall x \in \mathbb{R}^g \quad N(x) = \sum_{b \in O_K - \{0\}} \sum_{a \in I} \chi\left(r_0a + r_0x\bar{b} + \frac{i}{r_0}b\right) .$$

Grâce au lemme 3.3, on a la relation $\int_F N(x) d\nu(x) = \frac{J(r_0)}{\nu(F')}$. Il existe donc un $x_0 \in F$ tel que $N(x_0) \leq \frac{J(r_0)}{\nu(F)\nu(F')} < m$.

Notons $f : E \rightarrow E$ l'application $y \mapsto x_0\bar{y}$ et posons $\Gamma = r_0I + \left(r_0f + \frac{i}{r_0}\text{Id}\right)(O_K)$. D'après le lemme 3.2, le quotient $A = \mathbb{C}^g/\Gamma$ est une variété abélienne naturellement munie d'une polarisation L principale.

Il reste à minorer $V(A; L)$. Soit $\gamma = r_0a + r_0f(b) + \frac{i}{r_0}b \in \Gamma - \{0\}$. Si $b \neq 0$, le lemme 3.1 permet d'obtenir $m\chi(\gamma) = \sum_{g \in G} \chi(g * \gamma) \leq N(x_0) < m$, ce qui implique $v_{2g}\|\gamma\|^{2g} > m - \varepsilon$.

Et si $b = 0$, on a directement $v_{2g}\|\gamma\|^{2g} \geq v_{2g}(r_0\lambda_1(I))^{2g} > m - \varepsilon$.

On a donc montré que $V(A; L) = \frac{v_{2g}}{4^g}\lambda_1(\Gamma)^{2g} > \frac{m - \varepsilon}{4^g}$. D'où le résultat. \square

Remarque 4.1 : Considérons le sous-corps totalement réel $K' = \mathbb{Q}(\zeta + \zeta^{-1})$ de K . Soit $b \in O_{K'}$; notons $j(b) : \mathbb{C}^g \rightarrow \mathbb{C}^g$ la multiplication par b . Le réseau Γ du lemme 3.2.β est alors stable par $j(b)$. Cela induit un endomorphisme $j(b) : \mathbb{C}^g/\Gamma \rightarrow \mathbb{C}^g/\Gamma$. On vient ainsi de construire un morphisme injectif d'anneaux $j : O_{K'} \hookrightarrow \text{End}(\mathbb{C}^g/\Gamma)$.

En posant $W_{K'} = \sup\{V(A; L) ; (A; L) \in \mathcal{A}_g(\mathbb{C}) \text{ et } O_{K'} \text{ s'injecte dans } \text{End}(A)\}$, la démonstration ci-dessus prouve en fait l'inégalité $W_{K'} \geq \frac{m}{4^g}$.

5 Démonstration des corollaires

Démonstration de 1.2 : (α) Il suffit d'appliquer le théorème 1.1 avec $m = 3g$.

(β) Si n est pair sans être une puissance de 2, on a $4^g V_g \geq n \geq 2g + 2$. Si n est impair, on a $\varphi(2n) = g$ donc $4^g V_g \geq 2n \geq 2g + 2$. \square

Démonstration de 1.3 : Soit x un réel ≥ 3 . Prenons m égal au produit des nombres premiers $p \leq x$, et posons $g = \varphi(m)$. D'après le théorème de Mertens (voir [9] page 17), on a $\frac{m}{g} = \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^\gamma \ln x + O(1)$. Les estimations de Tchébychev donnent $\ln g \leq \ln m = O(x)$, ce qui implique $\ln \ln g \leq \ln x + O(1)$. On en conclut que $4^g V_g \geq m \geq e^\gamma g \ln \ln g + O(g)$. \square

Références

- [1] *K. Ball* : A lower bound for the optimal density of lattice packings. International Math. Research Notices **10** (1992), 217-221.
- [2] *C. Birkenhake, H. Lange* : Complex abelian varieties (second edition). Grundlehren der math. Wissenschaften **302** (2004).
- [3] *P. Buser, P. Sarnak* : On the period matrix of a Riemann surface of large genus. Inventiones Math. **117** (1994), 27-56.
- [4] *H. Davenport, C.A. Rogers* : Hlawka's theorem in the geometry of numbers. Duke Math. Journal **14** (1947), 367-375.
- [5] *P. Gaborit, G. Zémor* : On the construction of dense lattices with a given automorphisms group. Annales de l'Institut Fourier **57** (2007), 1051-1062.
- [6] *G.A. Kabatyanskiï, V.I. Levenshtein* : Bound for packings on a sphere and in space. Problems of Information Transmission **14** (1978), 1-17.
- [7] *B. Muetzel* : A new lower bound for Hermite's constant for symplectic lattices. International J. of Number Theory **8** (2012), 1067-1080.
- [8] *C.A. Rogers* : Existence theorems in the geometry of numbers. Annals of Math **48** (1947), 994-1002.
- [9] *G. Tenenbaum* : Introduction à la théorie analytique et probabiliste des nombres. Cours spécialisés de la S.M.F. **1** (1995).
- [10] *A. Venkatesh* : A note on sphere packings in high dimension. International Math. Research Notices **7** (2013), 1628-1642.

Pascal Autissier. I.M.B., université de Bordeaux, 351, cours de la Libération, 33405 Talence cedex, France.

pascal.autissier@math.u-bordeaux1.fr