

Lemmes de Siegel d'évitement

par

ÉRIC GAUDRON et GAËL RÉMOND (Grenoble)

1. Introduction. Soient n un entier ≥ 1 et Ω un sous-ensemble d'un espace vectoriel normé $(\mathbb{R}^n, \|\cdot\|)$. Pour tout entier $i \in \{1, \dots, n\}$, soit $\lambda_i(\Omega, \|\cdot\|)$ le minimum des nombres réels $r > 0$ pour lesquels il existe $\omega_1, \dots, \omega_i \in \Omega$ linéairement indépendants et de normes $\leq r$. Un des problèmes classiques de la géométrie des nombres – en grande partie résolu par Minkowski au XIX^e siècle – est de majorer $\lambda_i(\Omega, \|\cdot\|)$ en fonction du volume du compact \mathbb{R}^n/Ω et de celui de la boule unité de $(\mathbb{R}^n, \|\cdot\|)$ lorsque Ω est un réseau de \mathbb{R}^n . Dans ce texte, nous nous intéressons au cas du complémentaire d'un fermé algébrique dans un réseau. Par exemple, nous montrerons l'énoncé suivant.

THÉORÈME 1.1. *Soient $\|\cdot\|$ une norme sur \mathbb{R}^n et $\Omega \subset \mathbb{R}^n$ un réseau. Soit I un idéal de $\mathbb{Q}[X_1, \dots, X_n]$ engendré par une famille d'éléments de degré (total) $\leq M$. Soit $Z(I) = \{x \in \Omega; \forall P \in I, P(x) = 0\}$ le lieu des zéros de I dans Ω . Si $s \geq 1$ est tel qu'aucun sous- \mathbb{Z} -module de rang s n'est inclus dans $Z(I)$ alors on a $\lambda_1(\Omega \setminus Z(I), \|\cdot\|) \leq M\lambda_s(\Omega, \|\cdot\|)$.*

Une généralisation possible est de remplacer le couple $(\Omega, \|\cdot\|)$ par un fibré vectoriel adélique \overline{E} sur un corps de nombres k . Rappelons brièvement qu'un tel objet est la donnée d'un k -espace E de dimension n et de normes $\|\cdot\|_{\overline{E},v}$ sur $E \otimes_k \mathbb{C}_v$ pour toute place v de k , soumises à diverses contraintes. Une famille d'exemples est donnée par $(k^n, |\cdot|_p)$ pour $p \in [1, +\infty]$ défini par

$$|x|_{p,v} := \begin{cases} (|x_1|_v^p + \dots + |x_n|_v^p)^{1/p} & \text{si } v \mid \infty \text{ et } p \neq +\infty, \\ \max\{|x_1|_v, \dots, |x_n|_v\} & \text{sinon,} \end{cases}$$

pour tout $x = (x_1, \dots, x_n) \in \mathbb{C}_v^n$. La taille d'un élément de E peut être contrôlée au moyen des normes qu'il a en les différentes places de k . On peut alors définir des minima successifs associés à \overline{E} (notés $\lambda_i^{\text{BV}}(\overline{E})$), de

2010 *Mathematics Subject Classification*: Primary 11G50; Secondary 11H06, 14G40.

Key words and phrases: Siegel's lemma, successive minima, adelic vector bundle, combinatorial Nullstellensatz.

manière similaire au cas classique. Dans la notation, l'exposant BV représente les initiales de Bombieri–Vaaler. La précision est nécessaire car il existe plusieurs définitions différentes et, en général, non équivalentes de minima successifs de fibrés vectoriels adéliques (voir [Ga2, §2.4]). Dans ce contexte, l'analogie du problème de Minkowski est alors appelé *lemme de Siegel* dans la littérature (surtout diophantienne, voir [Ga3, §9]), expression à laquelle on peut adjoindre le mot *évitement* lorsque l'on cherche une solution dans le complémentaire d'un ensemble algébrique de E , comme dans le théorème 1.1.

Cet article est consacré à l'étude de cette dernière variante. Peu de résultats existent dans la littérature, essentiellement les travaux de Fukshansky [Fu1, Fu2, Fu3] et celui du premier auteur [Ga2]. La question a également été abordée par Soulé dans des exposés récents. À travers les théorèmes 2.2 et 2.9, qui sont les résultats principaux de notre texte, nous montrons comment il est possible de relier les minima du complémentaire $E \setminus F$ d'un ensemble algébrique F aux minima du fibré adélique \overline{E} ambiant. Le théorème 2.2 s'exprime sous la forme $\lambda_1^{\text{BV}}(\overline{E} \setminus \overline{F}) \leq m \lambda_{\dim F+1}^{\text{BV}}(\overline{E})$ où m est un nombre réel qui dépend de k , de la dimension de F et d'un majorant M des degrés d'une famille d'équations définissant F . Le théorème 2.9 propose quant à lui un énoncé *absolu* (c'est-à-dire où la dépendance en le corps de nombres disparaît) qui fait intervenir les minima successifs de Zhang. Ces deux résultats séparent les contributions aux places archimédiennes et aux places ultramétriques. Comme nous le montrerons en détail au §3, ils améliorent et généralisent les résultats connus (sauf pour la dépendance en M dans certains cas).

La méthode de [Fu1, Fu2], reprise et perfectionnée dans [Ga2], reposait sur un encadrement des cardinaux d'ensembles de points de petites hauteurs (au passage étaient redémontrés des lemmes de Siegel, aux constantes un peu moins bonnes que celles de Bombieri–Vaaler). Ici, les démonstrations sont techniquement plus simples. Dans le cas d'un corps de nombres, nous utilisons une variante du théorème d'annulation d'un polynôme en plusieurs variables sur un produit cartésien d'ensembles de cardinaux assez grands (théorème des zéros combinatoire d'Alon 2.4). La méthode généralise et raffine celle de la proposition 3.1 de [Ga2], due au second auteur (elle s'apparente à celle de [Fu3]). Pour l'énoncé absolu, nous introduisons deux définitions équivalentes des minima de Zhang qui, par essence, mènent à des minima d'évitement. Comme ni les minima de Zhang ni ceux de Bombieri–Vaaler ne sont aisément calculables, nous utilisons des lemmes de Siegel (parfois sophistiqués, comme celui de Zhang qui est issu de la géométrie d'Arakelov) pour obtenir des énoncés en termes de la hauteur du fibré adélique ambiant (corollaire 3.1). Enfin, par une variante astucieuse du théorème 2.2, nous montrons que notre approche qui contourne les en-

cadrements de cardinaux de [Ga2] est plus efficace puisqu'elle donne de meilleurs résultats.

2. Résultats

2.1. Soit k un corps de nombres de degré D , de discriminant absolu Δ_k/\mathbb{Q} et d'anneau des entiers \mathcal{O}_k . Soient r_1 et r_2 le nombre de places réelles et complexes de k et ω_k le nombre de racines de l'unité de k . On note $V(k)$ l'ensemble des places de k et $V_\infty(k)$ le sous-ensemble des places archimédiennes. Soit $\bar{E} = (E, (\|\cdot\|_{\bar{E},v})_{v \in V(k)})$ un fibré vectoriel adélique sur k , de dimension $n \geq 1$, au sens de [Ga1, Ga2].

DÉFINITION 2.1. Soit $i \in \{1, \dots, n\}$. Le $i^{\text{ème}}$ minimum de Bombieri–Vaaler relatif à \bar{E} , noté $\lambda_i^{\text{BV}}(\bar{E})$, est la borne inférieure de l'ensemble des nombres réels $r > 0$ tels que l'ensemble

$$E \cap \mathbf{B}_{\bar{E}}(0, r) := \left\{ x \in E; \sup_{v \in V_\infty(k)} \|x\|_{\bar{E},v} \leq r \text{ et } \sup_{v \notin V_\infty(k)} \|x\|_{\bar{E},v} \leq 1 \right\}$$

contienne i vecteurs linéairement indépendants.

Un résultat-clef de cet article est l'énoncé suivant.

THÉORÈME 2.2. Soient \bar{E} un fibré vectoriel adélique sur k et $\mathbf{S}(E^\vee)$ l'algèbre symétrique du dual de E . Soit I un idéal de $\mathbf{S}(E^\vee)$, engendré par une famille d'éléments de degré $\leq M$. Soit $Z(I)$ le lieu des zéros de I dans E . Supposons qu'aucun sous-espace vectoriel de E de dimension $s \geq 1$ ne soit inclus dans $Z(I)$. Notons $m_s(M)$ le nombre réel

$$\min_{k' \subset k} \left(s^{1-1/D'} \left(\frac{2^{r'_2} |\Delta_{k'}/\mathbb{Q}|^{1/2}}{\pi^{r'_2}} \right)^{1/D'} \min \left(M, s + \left[\frac{(M-s)\omega_{k'}}{2\omega_k} \right] \right)^{1/D'} \right)$$

(k' parcourt tous les sous-corps de k et $D' = [k' : \mathbb{Q}]$). Alors il existe $x \in E \setminus Z(I)$ tel que

$$\sup_{v \in V_\infty(k)} \|x\|_{\bar{E},v} \leq m_s(M) \lambda_s^{\text{BV}}(\bar{E}) \quad \text{et} \quad \sup_{v \notin V_\infty(k)} \|x\|_{\bar{E},v} \leq 1.$$

Si l'on choisit $k' = \mathbb{Q}$ dans la définition, on a toujours $m_s(M) \leq M$. On obtient alors un énoncé plus simple dont découle le théorème 1.1. Par ailleurs, l'hypothèse sur s est satisfaite dès que $s > \dim Z(I)$. Si l'on note X le schéma $\text{Spec } \mathbf{S}(E^\vee)$ associé à E et Y le sous-schéma fermé de X défini par I alors la condition $x \in E \setminus Z(I)$ devient $x \in (X \setminus Y)(k)$. Cet énoncé s'applique en particulier lorsque $Y = \bigcup_{i=1}^M E_i$ est l'union de sous-espaces vectoriels E_1, \dots, E_M de E , qui est le cas usuel considéré dans [Fu1, Fu2, Ga2] (voir la proposition 3.2 plus loin).

En appliquant successivement ce théorème à $Z(I) \cup kx_1 \oplus \dots \oplus kx_i$, on en déduit aisément l'existence d'une petite base de E qui évite $Z(I)$:

COROLLAIRE 2.3. *Dans les conditions du théorème 2.2, il existe une base x_1, \dots, x_n de E dont aucun des vecteurs n'est dans $Z(I)$ et telle que, pour tout $i \in \{1, \dots, n\}$, on a*

$$\sup_{v \in V_\infty(k)} \|x_i\|_{\overline{E},v} \leq m_{\max(s,i)}(M+1)\lambda_{\max(s,i)}^{\text{BV}}(\overline{E}) \quad \text{et} \quad \sup_{v \notin V_\infty(k)} \|x_i\|_{\overline{E},v} \leq 1.$$

La démonstration du théorème 2.2 repose en partie sur le théorème des zéros combinatoire d'Alon [Al] :

THÉORÈME 2.4. *Soient n un entier ≥ 1 , K un corps et $P \in K[X_1, \dots, X_n]$ de degré total $\deg P$. Choisissons $(a_1, \dots, a_n) \in \mathbb{N}^n$ tel que $a_1 + \dots + a_n = \deg P$ et tel que le monôme $X_1^{a_1} \dots X_n^{a_n}$ ait un coefficient non nul dans P . Si $S_i \subset K$ est un ensemble de cardinal $\geq a_i + 1$ pour tout $i \in \{1, \dots, n\}$ alors il existe $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$ tel que $P(s_1, \dots, s_n) \neq 0$.*

Soient $k_{\mathbf{A}}$ l'anneau des adèles de k et

$$\mathbf{B}_{\overline{E}}(0, 1) = \left\{ (x_v)_{v \in V(k)} \in E \otimes_k k_{\mathbf{A}} ; \sup_{v \in V(k)} \|x_v\|_{\overline{E},v} \leq 1 \right\}.$$

Soient vol une mesure de Haar sur $E \otimes_k k_{\mathbf{A}}$ et $\text{covol}(E)$ la mesure du quotient $(E \otimes_k k_{\mathbf{A}})/E$ associée. Le résultat suivant est une version adélique de l'inégalité de van der Corput [GL, p. 51].

PROPOSITION 2.5. *Soit \overline{E} un fibré vectoriel adélique sur k , de dimension $n \geq 1$. On a*

$$2 \left\lceil \frac{\text{vol}(\mathbf{B}_{\overline{E}}(0, 1))}{2^{nD} \text{covol}(E)} \right\rceil + 1 \leq \text{card } E \cap \mathbf{B}_{\overline{E}}(0, 1).$$

Démonstration. On se ramène au cas classique sur \mathbb{Q} au moyen du \mathbb{Q} -fibré vectoriel adélique ${}_{\mathbb{Q}}\overline{E}$ défini comme suit : l'espace vectoriel sous-jacent est E vu comme \mathbb{Q} -espace vectoriel (noté ${}_{\mathbb{Q}}E$), la norme en une place v de \mathbb{Q} est $\|x\|_{{}_{\mathbb{Q}}\overline{E},v} := \sup\{\|x_w\|_{\overline{E},w} ; w \in V(k), w|v\}$ pour $x \in {}_{\mathbb{Q}}E \otimes_{\mathbb{Q}} \mathbb{Q}_v = \prod_{w|v} E \otimes k_w$ de coordonnées $(x_w)_{w|v}$. Les boules adéliques $\mathbf{B}_{\overline{E}}(0, 1)$ et $\mathbf{B}_{{}_{\mathbb{Q}}\overline{E}}(0, 1)$ coïncident. Pour tout choix de mesure de Haar vol sur $E \otimes_k k_{\mathbf{A}} = {}_{\mathbb{Q}}\overline{E} \otimes_{\mathbb{Q}} \mathbb{Q}_{\mathbf{A}}$ on a

$$\frac{\text{vol}(\mathbf{B}_{{}_{\mathbb{Q}}\overline{E}}(0, 1))}{\text{covol}({}_{\mathbb{Q}}\overline{E})} = \frac{\text{vol}(\mathbf{B}_{\overline{E}}(0, 1))}{\text{covol}(E)}.$$

L'inégalité de van der Corput classique (sur \mathbb{Q})

$$2 \left\lceil \frac{\text{vol}(\mathbf{B}_{{}_{\mathbb{Q}}\overline{E}}(0, 1))}{2^{nD} \text{covol}({}_{\mathbb{Q}}\overline{E})} \right\rceil + 1 \leq \text{card } {}_{\mathbb{Q}}E \cap \mathbf{B}_{{}_{\mathbb{Q}}\overline{E}}(0, 1) = \text{card } E \cap \mathbf{B}_{\overline{E}}(0, 1)$$

permet alors de conclure. ■

REMARQUE 2.6. Notons $|\cdot|_v$ la valeur absolue sur le complété k_v de k en la place v qui étend la valeur absolue usuelle sur $(\mathbb{Q}, v|_{\mathbb{Q}})$ (voir [Ga1,

p. 25]). Soit $(a_v)_{v \in V_\infty(k)}$ un multiplet de nombres réels strictement positifs. Appliquée à $\overline{E} = (k, (a_v^{-1} |\cdot|_v)_{v \in V_\infty(k)}, (|\cdot|_v)_{v \notin V_\infty(k)})$ et couplée à la formule

$$\frac{\text{vol}(\mathbf{B}_{(k, (|\cdot|_v)_{v \in V(k)})}(0, 1))}{\text{covol}(k)} = \frac{2^{r_1+r_2} \pi^{r_2}}{|\Delta_{k/\mathbb{Q}}|^{1/2}} \quad (\text{voir [Ga2, p. 170]}),$$

la proposition 2.5 montre que

$$2 \left[\left(\frac{\pi}{2} \right)^{r_2} \cdot \frac{\prod_{v \in V_\infty(k)} a_v^{[kv:\mathbb{R}]}}{|\Delta_{k/\mathbb{Q}}|^{1/2}} \right] + 1 \leq \text{card}\{x \in \mathcal{O}_k; \forall v \in V_\infty(k), |x|_v \leq a_v\}.$$

Cette minoration généralise et améliore la première inégalité du lemme 5.2 de [Fu3] (et donc aussi le corollaire 1.6 du même article).

Démonstration du théorème 2.2. Soient $e_1, \dots, e_s \in E$ des vecteurs linéairement indépendants tels que, pour tout $i \in \{1, \dots, s\}$,

$$\sup_{v \in V_\infty(k)} \|e_i\|_{\overline{E},v} \leq \lambda_s^{\text{BV}}(\overline{E}) \quad \text{et} \quad \sup_{v \notin V_\infty(k)} \|e_i\|_{\overline{E},v} \leq 1.$$

Par hypothèse, le sous-espace vectoriel de E engendré par e_1, \dots, e_s n'est pas inclus dans $Z(I)$ et il existe donc $P \in I$, de degré total $\leq M$, tel que le polynôme

$$Q(X_1, \dots, X_s) := P(X_1 e_1 + \dots + X_s e_s)$$

n'est pas identiquement nul. Soit $X_1^{a_1} \dots X_s^{a_s}$ un monôme de degré maximal apparaissant dans Q . Soit k' un sous-corps de k . Soient $\xi_1, \dots, \xi_{\omega_k}$ les racines de l'unité (distinctes) de k . Pour tout $i \in \{1, \dots, s\}$, soit α_i le nombre réel ≥ 0 défini par

$$\alpha_i^{D'} = \frac{2^{r'_2} |\Delta_{k'/\mathbb{Q}}|^{1/2}}{\pi^{r'_2}} \left(1 + \left[\frac{(a_i - 1)\omega_{k'}}{2\omega_k} \right] \right).$$

Soit $B_i := \{\zeta \in \mathcal{O}_{k'}; \sup_{v \in V_\infty(k')} |\zeta|_v \leq \alpha_i\}$. Choisissons une famille B'_i de représentants de $B_i \setminus \{0\}$ modulo les racines de l'unité de k' et posons $S_i = \{0\} \cup \bigcup_{h=1}^{\omega_k} \xi_h B'_i$. Les ensembles qui composent cette union sont disjoints et on a

$$\text{card } S_i = 1 + \omega_k \text{card } B'_i = 1 + \omega_k \left(\frac{\text{card } B_i - 1}{\omega_{k'}} \right).$$

En utilisant la remarque 2.6 et grâce au choix de α_i , on minore le cardinal de B_i par $3 + 2[(a_i - 1)\omega_{k'} / (2\omega_k)]$ et l'on obtient $\text{card } S_i > a_i$. Le théorème 2.4 assure alors l'existence de $(x_1, \dots, x_s) \in \prod_{i=1}^s S_i$ tel que $Q(x_1, \dots, x_s) \neq 0$. Le vecteur $x = x_1 e_1 + \dots + x_s e_s$ répond aux conditions du théorème. En effet, il appartient à $E \setminus Z(I)$ et ses normes ultramétriques sont inférieures à 1 (car les éléments de S_i sont des entiers algébriques). De plus, les normes archimédiennes de x sont $\leq (\sum_i \alpha_i) \lambda_s^{\text{BV}}(\overline{E})$. La concavité de $x \mapsto x^{1/D'}$ donne

$$\sum_{i=1}^s \alpha_i \leq \left(\frac{2^{r'_2} |\Delta_{k'/\mathbb{Q}}|^{1/2}}{\pi^{r'_2}} \right)^{1/D'} s^{1-1/D'} \left(\sum_{i=1}^s \left(1 + \left[\frac{(a_i - 1)\omega_{k'}}{2\omega_k} \right] \right) \right)^{1/D'}.$$

On majore ensuite la somme des parties entières par la partie entière de la somme, ce qui fait apparaître $u(h) = h + [(M - h)\omega_{k'}/(2\omega_k)]$ avec $h := \text{card}\{i; a_i \neq 0\} \leq \min\{s, M\}$. Comme $u(h) = [(M\omega_{k'} + (2\omega_k - \omega_{k'})h)/(2\omega_k)]$ croît avec h , on trouve que la somme $\sum_i \alpha_i$ est plus petite que

$$\left(\frac{2^{r'_2} |\Delta_{k'/\mathbb{Q}}|^{1/2}}{\pi^{r'_2}} \right)^{1/D'} s^{1-1/D'} \left(\min(s, M) + \left[\frac{(M - \min(s, M))\omega_{k'}}{2\omega_k} \right] \right)^{1/D'}.$$

Pour conclure, on prend le minimum sur k' des expressions obtenues. ■

2.2. Au-delà du cadre des corps de nombres, il est possible de formuler des lemmes de Siegel sur $\overline{\mathbb{Q}}$. On parle alors de lemme de Siegel *absolu* à la suite de l'article [RT] de Roy–Thunder en 1996 qui ont donné une généralisation du théorème de Minkowski dans ce contexte. Une version plus fine se déduit du travail antérieur de Zhang ([Zh1], 1995) qui introduit des minima successifs pour la hauteur sur les variétés arithmétiques. Cette définition tout à fait générale donne même directement des minima d'évitement : pour obtenir le $i^{\text{ème}}$ minimum, on évite les sous-ensembles algébriques de dimension $i - 1$ (alors que la définition 2.1 n'évite que les sous-espaces vectoriels de dimension $i - 1$).

Précisons cette notion pour un fibré adélique \overline{E} sur $k \hookrightarrow \overline{\mathbb{Q}}$ comme ci-dessus (la variété correspondante serait ici $\mathbf{P}(E^\vee)$). Rappelons d'abord pour cela (voir [Ga1, p. 38]) que \overline{E} possède des extensions \overline{E}_K (d'espace sous-jacent $E \otimes K$) à tout surcorps K de k de degré fini. Pour $x \in E \otimes K$ et $v \in V(K)$ nous pouvons donc parler de la norme $\|x\|_{\overline{E},v}$ et de la hauteur $H_{\overline{E}}(x)$ de x définie comme le produit $\prod_{v \in V(K)} \|x\|_{\overline{E},v}^{n_v/[K:\mathbb{Q}]}$ où $n_v := [K_v : \mathbb{Q}_v]$ est le degré local en la place v . Si $x \in E \otimes \overline{\mathbb{Q}}$ nous notons $k(x)$ le corps de définition de x , c'est-à-dire le plus petit surcorps de k tel que $x \in E \otimes_k k(x)$. Par ailleurs, pour un ensemble $X \subset E \otimes \overline{\mathbb{Q}}$, notons $\text{Zar}(X)$ son adhérence pour la topologie de Zariski. La définition originale de Zhang (celle qui nous permettra d'employer son lemme de Siegel absolu) s'écrit alors comme suit.

DÉFINITION 2.7. Soit $i \in \{1, \dots, n\}$. Le $i^{\text{ème}}$ minimum de Zhang relatif à \overline{E} , noté $Z_i(\overline{E})$, est la borne inférieure de l'ensemble des nombres réels $r > 0$ tels que l'ensemble

$$\text{Zar}\{x \in E \otimes \overline{\mathbb{Q}}; H_{\overline{E}}(x) \leq r\}$$

soit de dimension au moins i .

Comme nous avons utilisé plus haut les minima au sens de Bombieri–Vaaler et non directement au sens de la hauteur, il semble naturel d'intro-

duire également deux variantes de cette définition :

$$\begin{aligned}\zeta_i^{\text{BV}}(\overline{E}) &= \inf\{r > 0; \dim \text{Zar}((E \otimes \overline{\mathbb{Q}}) \cap \mathbf{B}_{\overline{E}}(0, r)) \geq i\}, \\ \lambda_i^{\text{BV}}(\overline{E}, \overline{\mathbb{Q}}) &= \inf\{r > 0; \dim \text{Vect}_{\overline{\mathbb{Q}}}((E \otimes \overline{\mathbb{Q}}) \cap \mathbf{B}_{\overline{E}}(0, r)) \geq i\},\end{aligned}$$

où l'on note, avec un léger abus de langage, $(E \otimes \overline{\mathbb{Q}}) \cap \mathbf{B}_{\overline{E}}(0, r)$ l'ensemble

$$\left\{x \in E \otimes \overline{\mathbb{Q}}; \sup_{v \in V_\infty(k(x))} \|x\|_{\overline{E}, v} \leq r \text{ et } \sup_{v \notin V_\infty(k(x))} \|x\|_{\overline{E}, v} \leq 1\right\}.$$

La seconde notion généralise directement la définition 2.1. La première se confond quant à elle avec la définition 2.7 en vertu du lemme suivant.

LEMME 2.8. *Pour tous \overline{E} et i comme ci-dessus on a $\lambda_1^{\text{BV}}(\overline{E}, \overline{\mathbb{Q}}) = Z_1(\overline{E})$ et $\lambda_i^{\text{BV}}(\overline{E}, \overline{\mathbb{Q}}) \leq \zeta_i^{\text{BV}}(\overline{E}) = Z_i(\overline{E})$.*

Démonstration. Abrégeons $X_r = (E \otimes \overline{\mathbb{Q}}) \cap \mathbf{B}_{\overline{E}}(0, r)$. Nous avons $\text{Zar}(X_r) \subset \text{Vect}_{\overline{\mathbb{Q}}}(X_r)$ et donc $\dim \text{Zar}(X_r) \leq \dim \text{Vect}_{\overline{\mathbb{Q}}}(X_r)$. Ceci entraîne directement $\lambda_i^{\text{BV}}(\overline{E}, \overline{\mathbb{Q}}) \leq \zeta_i^{\text{BV}}(\overline{E})$. De plus X_r est stable par multiplication par les racines de l'unité, donc

$$\dim \text{Zar}(X_r) \geq 1 \Leftrightarrow X_r \text{ infini} \Leftrightarrow X_r \neq \{0\} \Leftrightarrow \dim \text{Vect}_{\overline{\mathbb{Q}}}(X_r) \geq 1.$$

On en déduit $\lambda_1^{\text{BV}}(\overline{E}, \overline{\mathbb{Q}}) = \zeta_1^{\text{BV}}(\overline{E})$. L'implication facile $x \in X_r \Rightarrow H_{\overline{E}}(x) \leq r$ donne $Z_i(\overline{E}) \leq \zeta_i^{\text{BV}}(\overline{E})$. L'implication réciproque est fautive mais nous allons établir

$$H_{\overline{E}}(x) < r \Rightarrow \exists z \in \overline{\mathbb{Q}}^\times, zx \in X_r.$$

Ceci suffira à montrer $\zeta_i^{\text{BV}}(\overline{E}) \leq Z_i(\overline{E})$ car l'inégalité stricte ne modifie pas l'infimum sur r et $\text{Zar}(\overline{\mathbb{Q}}^\times \cdot X_r) = \text{Zar}(X_r)$ par densité des racines de l'unité.

Soit donc maintenant $x \in E \otimes \overline{\mathbb{Q}} \setminus \{0\}$ tel que $H_{\overline{E}}(x) < r$. Notons $K = k(x)$ et considérons un entier naturel N . Pour $v \in V(K)$ posons $a_v = (r/\|x\|_{\overline{E}, v})^N$ si $v \in V_\infty(K)$ et $a_v = \|x\|_{\overline{E}, v}^{-N}$ sinon. De cette façon, le produit (fini) $\prod_v a_v^{[K_v:\mathbb{Q}_v]} = (r/H_{\overline{E}}(x))^{[K:\mathbb{Q}]N}$ tend vers $+\infty$ avec N . Ceci fait qu'en posant $\overline{F} = (K, (a_v^{-1}|\cdot|_v)_{v \in V(K)})$ le volume de la boule adélique $\mathbf{B}_{\overline{F}}(0, 1)$ tend également vers l'infini : il ne se calcule pas directement avec le produit ci-dessus (comme c'était le cas dans la remarque 2.6) car pour une place ultramétrique la formule $\text{vol}\{y \in K_v; |y|_v \leq a_v\} = a_v^{[K_v:\mathbb{Q}]}\text{vol}\{y \in K_v; |y|_v \leq 1\}$ n'est valable que si $a_v \in |K_v|_v$; cependant le quotient est borné uniquement en fonction de v et ceci nous donne l'assertion sur la limite. Par suite la proposition 2.5 fournit $\text{card}\{y \in K; \forall v \in V(K), |y|_v \leq a_v\} > 1$ pour N assez grand. On choisit alors $y \neq 0$ dans cet ensemble et l'on pose $z = y^{1/N} \in \overline{\mathbb{Q}}^\times$. Le résultat découle simplement du fait que pour tout $v \in V(K(z))$ on a $|z|_v = |y|_v^{1/N}$. ■

L'équivalent du théorème 2.2 est alors une simple reformulation de la définition (et le degré M n'intervient plus).

THÉORÈME 2.9. *Soient \bar{E} un fibré vectoriel adélique sur k et I un idéal de $\mathbf{S}(E^\vee \otimes \bar{\mathbb{Q}})$ de lieu des zéros $Z(I)$ dans $E \otimes \bar{\mathbb{Q}}$. Supposons $t := \dim Z(I) < \dim E$. Alors, pour tout $\varepsilon > 0$, il existe $x \in (E \otimes \bar{\mathbb{Q}}) \setminus Z(I)$ tel que*

$$\sup_{v \in V_\infty(k(x))} \|x\|_{\bar{E},v} \leq Z_{t+1}(\bar{E}) + \varepsilon \quad \text{et} \quad \sup_{v \notin V_\infty(k(x))} \|x\|_{\bar{E},v} \leq 1.$$

3. Comparaison avec les résultats antérieurs. Dans cette partie nous montrons comment le théorème 2.2 entraîne les résultats déjà connus dans la littérature [Fu1, Fu2, Fu3, Ga2], sauf en ce qui concerne la dépendance en l'entier M qui est différente dans [Ga2]. La comparaison se fait en deux temps : nous commençons avec [Fu3] qui a un majorant uniforme (indépendant de l'arithmétique de I) comme le nôtre, puis nous montrons que le théorème 2.2 entraîne aussi – et de manière plus surprenante – l'énoncé principal de [Ga2] (qui contenait déjà [Fu1, Fu2]).

3.1. Commençons par énoncer une conséquence du théorème 2.2. Pour un entier $N \geq 1$ et un sous-espace vectoriel E de k^N , le terme $H(E, |\cdot|_2)$ désigne la hauteur de E vu comme sous-fibré hermitien de $(k^N, |\cdot|_2)$, et H_n est le nombre harmonique $1 + 1/2 + \dots + 1/n$.

COROLLAIRE 3.1. *Soit E un sous-espace vectoriel de k^N de dimension n . Soit I un idéal de $k[X_1, \dots, X_N]$ engendré par une famille de polynômes de degré $\leq M$. Supposons que $t := \dim Z(I) < n$. Alors il existe $x \in E \cap \mathcal{O}_k^N \setminus Z(I)$ tel que*

$$H_{(k^{N+1}, |\cdot|_\infty)}(1, x) \leq n \left(\left(\frac{2}{\pi} \right)^{r_2} |\Delta_{k/\mathbb{Q}}|^{1/2} \right)^{(2n-t)/((n-t)D)} M^{1/D} H(E, |\cdot|_2)^{1/(n-t)}.$$

De plus, si $\omega_k > M$ on peut remplacer dans l'exposant $2n - t$ par n et supprimer $M^{1/D}$. De même, pour tout $\varepsilon > 0$, il existe $x \in (\mathcal{O}_{\bar{\mathbb{Q}}}^N \cap E \otimes_k \bar{\mathbb{Q}}) \setminus Z(I)$ tel que

$$H_{(k^{N+1}, |\cdot|_\infty)}(1, x) \leq \left(\exp \left(\frac{n(H_n - 1)}{2(n-t)} \right) + \varepsilon \right) H(E, |\cdot|_2)^{1/(n-t)}.$$

Démonstration. Le théorème 2.2 nous donne un élément $x \in E$ tel que $\|x\|_{(k^N, |\cdot|_\infty), v} \leq m_{t+1}(M) \lambda_{t+1}^{\text{BV}}(E, |\cdot|_\infty)$ pour tout $v \in V_\infty(k)$ et $\|x\|_{(k^N, |\cdot|_\infty), v} \leq 1$ pour tout $v \notin V_\infty(k)$. Comme les majorants sont plus grands que 1, nous pouvons remplacer la norme de x par la norme de $(1, x)$. De plus la seconde propriété se traduit par $x \in \mathcal{O}_k^N$ tandis que par produit nous avons $H_{(k^{N+1}, |\cdot|_\infty)}(1, x) \leq m_{t+1}(M) \lambda_{t+1}^{\text{BV}}(E, |\cdot|_\infty)$. Le dernier terme se compare à la hauteur $H(E, |\cdot|_2)$ via la variante adélique du second théorème de

Minkowski obtenu par Bombieri et Vaaler [BV, théorème 9] :

$$\lambda_{t+1}^{\text{BV}}(E, |\cdot|_\infty) \leq \left(\left(\frac{2}{\pi} \right)^{r_2} |\Delta_{k/\mathbb{Q}}|^{1/2} \right)^{n/((n-t)D)} H(E, |\cdot|_2)^{1/(n-t)}$$

(compte tenu à nouveau de $\lambda_i^{\text{BV}}(E, |\cdot|_\infty) \geq 1$ pour tout $i \in \{1, \dots, n\}$). En majorant $m_{t+1}(M)$ par $(t+1)^{1-1/D} (2^{r_2} |\Delta_{k/\mathbb{Q}}|^{1/2} / \pi^{r_2})^{1/D} M^{1/D}$ (qui correspond à $k' = k$) ou simplement par $t+1 \leq n$ lorsque $\omega_k > M$, on obtient les deux premiers énoncés du corollaire. Pour le dernier, nous procédons de même avec le théorème 2.9 mais nous l'appliquons directement à $(E, |\cdot|_2)$. Rien ne change pour les places ultramétriques (intégralité), mais pour une place archimédienne nous avons ici $\|x\|_{(k^N, |\cdot|_2), v} \leq Z_{t+1}(E, |\cdot|_2) + \varepsilon$. Ce majorant est encore supérieur à 1, donc nous pouvons également écrire $\|(1, x)\|_{(k^{N+1}, |\cdot|_\infty), v} \leq Z_{t+1}(E, |\cdot|_2) + \varepsilon$. La preuve continue de même mais cette fois $Z_{t+1}(E, |\cdot|_2)$ est majoré par le théorème de Zhang (voir [Zh1, théorème 5.2] ainsi que [Zh2, lemme 4.7] et [Ga3, appendice] qui explicitent la hauteur de $\mathbf{P}(E^\vee)$) :

$$Z_{t+1}(E, |\cdot|_2) \leq \exp\left(\frac{n(H_n - 1)}{2(n-t)}\right) H(E, |\cdot|_2)^{1/(n-t)}.$$

La conclusion s'ensuit (en changeant d' ε). ■

Le résultat général de [Fu3] est écrit dans le cadre très restreint du corollaire 3.1 (seulement pour la norme du maximum) mais ne donne pas des éléments entiers. En outre, la borne pour la hauteur de x comporte les mêmes quantités que celle du corollaire, mais le discriminant est à la puissance $(n+1)/(2D)$ (seulement $n/(2D)$ lorsque $\omega_k > M$) et $H(E, |\cdot|_2)$ apparaît sans l'exposant $1/(n-t)$. Lorsque l'on demande seulement $x \in (E \otimes_k \overline{\mathbb{Q}}) \setminus Z(I)$ notre estimation est plus petite que $(\sqrt{n}^n H(E, |\cdot|_2))^{1/(n-t)}$ alors que [Fu3] fournit

$$H_{(k^{N+1}, |\cdot|_\infty)}(1, x) \leq n(\exp(n(n-1)/2) + \varepsilon) H(E, |\cdot|_2).$$

3.2. Afin de comparer maintenant avec les résultats de [Ga2], écrivons une variante moins générale mais plus précise du théorème 2.2 (voir aussi [Ga2, proposition 3.1]).

PROPOSITION 3.2. *Soient $M \in \mathbb{N} \setminus \{0\}$ et \overline{E} un fibré vectoriel adélique sur k . Soient E_1, \dots, E_M des sous-espaces vectoriels stricts de E . Il existe $i \in \{1, \dots, M\}$, $\ell \in \{0, \dots, \dim E_i\}$ et $x \in E \setminus \bigcup_{j=1}^M E_j$ tels que*

$$\sup_{v \in V_\infty(k)} \|x\|_{\overline{E}, v} \leq m_{\ell+1}(M) \lambda_{\ell+1}^{\text{BV}}(\overline{E}) \quad \text{et} \quad \sup_{v \notin V_\infty(k)} \|x\|_{\overline{E}, v} \leq 1$$

(le nombre $m_{\ell+1}(M)$ est défini dans le théorème 2.2). De plus, si $\ell = 0$ on peut remplacer $m_1(M)$ par 1 et si $\ell \geq 1$ alors, pour tout $j \in \{1, \dots, \ell\}$, on a $\lambda_j^{\text{BV}}(\overline{E}_i) = \lambda_j^{\text{BV}}(\overline{E})$.

Démonstration. Soit (e_1, \dots, e_n) une base de E telle que, pour tout $j \in \{1, \dots, n\}$, on a $\sup\{\|e_j\|_{\overline{E},v}; v \in V_\infty(k)\} = \lambda_j^{\text{BV}}(\overline{E})$ et $\sup\{\|e_j\|_{\overline{E},v}; v \notin V_\infty(k)\} \leq 1$. Soit ℓ le plus grand entier tel que le k -espace vectoriel V_ℓ engendré par e_1, \dots, e_ℓ est inclus dans $\bigcup_{i=1}^M E_i$. Si $\ell = 0$ alors $x = e_1$ satisfait aux conditions de la proposition. Si $\ell \geq 1$, il existe $i \in \{1, \dots, M\}$ tel que $V_\ell \subset E_i$. En particulier, on a $\lambda_j^{\text{BV}}(\overline{E}) \leq \lambda_j^{\text{BV}}(\overline{E}_i) \leq \lambda_j^{\text{BV}}(\overline{V}_\ell) = \lambda_j^{\text{BV}}(\overline{E})$ pour tout $j \in \{1, \dots, \ell\}$, ce qui montre la dernière assertion de la proposition. Quant à la première assertion, il s'agit simplement d'appliquer le théorème 2.2 à l'ensemble algébrique $\bigcup_{i=1}^M E_i \cap V_{\ell+1}$ de $V_{\ell+1}$ (muni des métriques induites par celles de \overline{E}). ■

Pour simplifier l'analyse et supprimer des complications techniques (comme introduire le *défaut de pureté* de \overline{E}) sans intérêt ici, nous supposerons jusqu'à la fin de ce paragraphe que les fibrés adéliques considérés sont *hermitiens* (voir [Ga2, définition 2.3]). Il existe une constante minimale $c(n, k) > 0$, dite *constante d'Hermite généralisée*, qui dépend d'un entier n et d'un corps de nombres k , pour laquelle on a $\lambda_1^{\text{BV}}(\overline{E}) \cdots \lambda_n^{\text{BV}}(\overline{E}) \leq c(n, k)^n H(\overline{E})$ pour tout fibré adélique hermitien \overline{E} sur k de dimension n . En notant V_n le volume de la boule unité de l'espace euclidien $(\mathbb{R}^n, |\cdot|_2)$ pour la mesure de Lebesgue, on sait d'après un théorème de Vaaler [Va] que

$$c(n, k) \leq \left(\frac{2^{r_1+r_2} |\Delta_{k/\mathbb{Q}}|^{1/2}}{V_n^{r_1/n} V_{2n}^{r_2/n}} \right)^{1/D},$$

ce qui entraîne immédiatement la borne $c(n, k) \leq \sqrt{n} |\Delta_{k/\mathbb{Q}}|^{1/(2D)}$ car $V_n^{-1} = \pi^{-n/2} \Gamma(1 + n/2) \leq (n/(2\pi))^{n/2}$ si $n \geq 2$.

COROLLAIRE 3.3. *Reprenons les notations et hypothèses de la proposition 3.2. Posons $H = c(n, k)H(\overline{E})^{1/n}$ et $n_i = \dim E_i$ pour $1 \leq i \leq M$. Alors il existe $x \in E \setminus \bigcup_{i=1}^M E_i$ tel que $\sup_{v \notin V_\infty(k)} \|x\|_{\overline{E},v} \leq 1$ et*

$$\begin{aligned} & \sup_{v \in V_\infty(k)} \|x\|_{\overline{E},v} \\ & \leq H \max_{1 \leq i \leq M} \left\{ 1, m_{n_i+1}(M) \left(\frac{H^{n_i}}{H(\overline{E}_i)} \right)^{\frac{1}{n-n_i}}, m_{n_i}(M) \left(\frac{H}{\lambda_1^{\text{BV}}(\overline{E}_i)} \right)^{\frac{n_i-1}{n-n_i+1}} \right\}. \end{aligned}$$

Démonstration. La proposition 3.2 majore le membre de gauche ci-dessus par $m_{\ell+1}(M) \lambda_{\ell+1}^{\text{BV}}(\overline{E})$ avec $\ell \leq n_i$ pour un certain $i \in \{1, \dots, M\}$. Lorsque $\ell = 0$, on a même une majoration par $\lambda_1^{\text{BV}}(\overline{E})$ qui est plus petit que H et le corollaire est démontré. Lorsque $\ell \geq 1$, nous utilisons la dernière assertion de la proposition 3.2 :

$$\begin{aligned} \lambda_{\ell+1}^{\text{BV}}(\overline{E}) &= \left(\frac{\lambda_1^{\text{BV}}(\overline{E}) \cdots \lambda_\ell^{\text{BV}}(\overline{E})}{\lambda_1^{\text{BV}}(\overline{E}_i) \cdots \lambda_\ell^{\text{BV}}(\overline{E}_i)} \cdot \lambda_{\ell+1}^{\text{BV}}(\overline{E})^{n-\ell} \right)^{\frac{1}{n-\ell}} \\ &\leq \left(\frac{\lambda_1^{\text{BV}}(\overline{E}) \cdots \lambda_n^{\text{BV}}(\overline{E})}{\lambda_1^{\text{BV}}(\overline{E}_i) \cdots \lambda_\ell^{\text{BV}}(\overline{E}_i)} \right)^{\frac{1}{n-\ell}} \leq \left(\frac{H^n}{\lambda_1^{\text{BV}}(\overline{E}_i) \cdots \lambda_\ell^{\text{BV}}(\overline{E}_i)} \right)^{\frac{1}{n-\ell}}. \end{aligned}$$

Si $\ell = n_i$ on minore le produit $\lambda_1^{\text{BV}}(\overline{E}_i) \cdots \lambda_\ell^{\text{BV}}(\overline{E}_i)$ par $H(\overline{E}_i)$ (voir [Ga2, proposition 2.18]), ce qui fournit le terme $(H^{n_i}/H(\overline{E}_i))^{1/(n-n_i)}$ du majorant dans le corollaire. Si $\ell < n_i$ on minore ce même produit simplement par $\lambda_1^{\text{BV}}(\overline{E}_i)^\ell$. On obtient alors

$$\lambda_{\ell+1}^{\text{BV}}(\overline{E}) \leq H \left(\frac{H}{\lambda_1^{\text{BV}}(\overline{E}_i)} \right)^{\frac{\ell}{n-\ell}} \leq H \left(\frac{H}{\lambda_1^{\text{BV}}(\overline{E}_i)} \right)^{\frac{n_i-1}{n-n_i+1}}$$

car $x \mapsto x/(n-x)$ croît et $\lambda_1^{\text{BV}}(\overline{E}_i) = \lambda_1^{\text{BV}}(\overline{E}) \leq H$. On conclut avec $m_{\ell+1}(M) \leq m_{n_i}(M)$. ■

Si, dans ce corollaire, on majore $m_{n_i+1}(M)$ et $m_{n_i}(M)$ par M , il devient évident que le théorème 1.1 de [Ga2] en découle sauf pour la dépendance en M qui était de l'ordre de $M^{1/(n-t)}$ où $t = \max_i n_i$. Nous pourrions aussi écrire une majoration en $M^{1/D}$ comme dans le corollaire 3.1 en augmentant la valeur de H . Mentionnons qu'une majoration de la forme du théorème 2.2 doit présenter une dépendance en M au moins de l'ordre de $M^{1/(nD)}$. Pour le voir, on évite simplement les droites engendrées par les vecteurs de $E \cap \mathbf{B}_{\overline{E}}(0, R) \setminus \{0\}$ (pour R assez grand) et on utilise la proposition 2.5.

3.3. Les méthodes présentées dans cet article s'appliquent également pour des fibrés vectoriels adéliques sur un corps de fonctions. Donnons simplement un exemple.

Soient p un nombre premier et k une extension finie de $k_0 := \mathbb{F}_p(T)$, de degré $D = [k : k_0]$. On munit k de sa collection de valeurs absolues normalisées comme dans [Ga1, p. 25] et on note $n_v := [k_v : (k_0)_{v_0}]$ le degré local en une place v de k au-dessus de v_0 , place de k_0 . Les minima successifs de Bombieri–Vaaler n'existent plus dans ce cadre mais, étant donné un fibré adélique \overline{E} sur k , de dimension n , et $i \in \{1, \dots, n\}$, on peut définir, à la suite de Thunder, le $i^{\text{ème}}$ minimum $\lambda_i(\overline{E})$ de \overline{E} comme

$$\inf \{ |r|_{\mathbf{A}} ; r \in k_{\mathbf{A}}, \dim \text{Vect} \{x \in E ; \forall v \in V(k), \|x\|_{\overline{E},v} \leq |r_v|_v \} \geq i \}$$

où $r = (r_v)_{v \in V(k)}$ et $|r|_{\mathbf{A}} = \prod_{v \in V(k)} |r_v|_v^{n_v/D}$.

THÉORÈME 3.4. *Soient \overline{E} un fibré vectoriel adélique sur k et $s \geq 1$ un entier. Soit I un idéal de $\mathbf{S}(E^\vee)$, engendré par une famille d'éléments de degré $\leq M$. Supposons qu'aucun sous-espace vectoriel de E de dimension s ne soit inclus dans $Z(I)$. Alors il existe $x \in E \setminus Z(I)$ tel que la hauteur*

normalisée de x vérifie

$$H_{\overline{E}}(x) := \prod_{v \in V(k)} \|x\|_{\overline{E},v}^{n_v/D} \leq M \lambda_s(\overline{E}).$$

Cette borne est significativement plus simple que celles de [Fu3], en général exponentielles en M .

Références

- [Al] N. Alon, *Combinatorial Nullstellensatz*, in: Recent Trends in Combinatorics (Mátraháza, 1995), Combin. Probab. Comput. 8 (1999), 7–29.
- [BV] E. Bombieri and J. Vaaler, *On Siegel’s lemma*, Invent. Math. 73 (1983), 11–32; Addendum, ibid. 75 (1984), 377.
- [Fu1] L. Fukshansky, *Integral points of small height outside of a hypersurface*, Monatsh. Math. 147 (2006), 25–41.
- [Fu2] L. Fukshansky, *Siegel’s lemma with additional conditions*, J. Number Theory 120 (2006), 13–25.
- [Fu3] L. Fukshansky, *Algebraic points of small height missing a union of varieties*, J. Number Theory 130 (2010), 2099–2118.
- [Ga1] É. Gaudron, *Pentes des fibrés vectoriels adéliques sur un corps global*, Rend. Sem. Mat. Univ. Padova 119 (2008), 21–95.
- [Ga2] É. Gaudron, *Géométrie des nombres adélique et lemmes de Siegel généralisés*, Manuscripta Math. 130 (2009), 159–182.
- [Ga3] É. Gaudron, *Géométrie des nombres adélique et formes linéaires de logarithmes dans un groupe algébrique commutatif*, Habilitation à diriger des recherches, tel-00585976, 2009.
- [GL] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland Math. Library 37, North-Holland, Amsterdam, 1987.
- [RT] D. Roy and J. L. Thunder, *An absolute Siegel’s lemma*, J. Reine Angew. Math. 476 (1996), 1–26; Addendum and erratum, ibid. 508 (1999), 47–51.
- [Va] J. D. Vaaler, *The best constant in Siegel’s lemma*, Monatsh. Math. 140 (2003), 71–89.
- [Zh1] S. Zhang, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. 8 (1995), 187–221.
- [Zh2] S. Zhang, *Heights and reductions of semi-stable varieties*, Compos. Math. 104 (1996), 77–105.

Éric Gaudron, Gaël Rémond
 Université Grenoble I
 Institut Fourier, UMR 5582
 BP 74
 38402 Saint-Martin-d’Hères Cedex, France
 E-mail: Eric.Gaudron@ujf-grenoble.fr
 Gael.Remond@ujf-grenoble.fr

Reçu le 5.5.2011
 et révisé le 21.10.2011

(6690)