Minoration de la hauteur de Néron-Tate pour les points et les sous-variétés : variations sur le problème de Lehmer

Nicolas Ratazzi

Thèse de Doctorat de l'Université Paris 6

Spécialité :

Mathématiques

présentée par :

M. Nicolas Ratazzi

pour obtenir le grade de docteur de l'Université Paris 6

Sujet :

Minoration de la hauteur de Néron-Tate pour les points et les sous-variétés : variations sur le problème de Lehmer

Soutenue le 25 mai 2004 devant le jury composé de :

M. Francesco AMOROSO	(Caen)	
M. Daniel BERTRAND	(Paris 6)	
M. Jean-Benoît BOST	(Paris 11, Orsay)	
M. Carlo GASBARRI	(Rome 2)	Rapporteur
M. Marc HINDRY	(Paris 7)	Directeur
M. Michel LAURENT	(CNRS, Marseille)	Rapporteur

Remerciements

Je tiens avant tout à remercier mon directeur de thèse Marc Hindry. Il a pleinement répondu à mes attentes d'encadrement et d'autonomie. Il a notamment toujours manifesté son intérêt pour mes recherches, même si celles-ci ne correspondent pas exactement au sujet qu'il m'avait proposé. Par ailleurs, il a fait preuve d'une disponibilité tout à fait remarquable, ayant toujours un moment à me consacrer lorsque j'en ressentais le besoin. C'est toujours avec beaucoup de gentillesse et une grande clarté qu'il a répondu à mes questions.

Je suis très heureux que Carlo Gasbarri et Michel Laurent aient accepté de rapporter ma thèse, tâche ingrate qu'ils ont néanmoins effectuée avec diligence. Je suis honoré qu'ils aient tous deux accepté de faire le déplacement à Paris pour assister à ma soutenance.
Je souhaite également exprimer ma reconnaissance à Francesco Amoroso, Daniel Bertrand et Jean-Benoît Bost pour avoir accepté de faire partie de mon jury de thèse.

Je tiens ici à indiquer ma gratitude envers Sinnou David. C'est son cours de DEA de l'année scolaire 2000/2001 sur la géométrie diophantienne (et entre autres choses sur le problème de Lehmer sur $\mathbb{G}_m^n$) qui, avec le livre de Marc Hindry et Joseph Silverman sur le même sujet, m'a définitivement donné envie de faire ma thèse dans ce domaine. Par ailleurs, il a toujours accepté de répondre chaleureusement à mes questions et c'est lui qui m'a encouragé à écrire l'article correspondant au chapitre 3 de cette thèse.

Bien que je n'aie pas encore réussi à exploiter ses idées, je voudrais également remercier Jean-Benoît Bost pour le temps qu'il a accepté de me consacrer, essayant de me faire comprendre sa vision des choses concernant les liens que pourraient avoir le théorème de l'indice de Hodge arithmétique avec les problèmes d'approximations diophantiennes.

C'est à l'occasion d'un exposé à Grenoble et d'une discussion avec Gaël Rémond que j'ai eu l'idée (et compris l'intérêt) d'écrire l'article correspondant au chapitre 5 de cette thèse. Par la suite Gaël Rémond a toujours répondu avec précision à mes différentes questions concernant ses travaux. Je tiens à le remercier ici.

Pascal Autissier a également toujours accepté de répondre à mes questions sur la theorie d'Arakelov. Par ailleurs je suis très heureux des récentes discussions stimulantes que nous avons pu avoir concernant les problèmes de Lehmer.

C'est au magistère de l'École Normale Supérieure de Paris que j'ai réellement commencé

à prendre goût pour la recherche. C'est également là que j'ai rencontré certains de mes meilleurs amis, Philippe Gravejat, Julien Marché, Benoit Daniel, Sébastien Gouezel, Alexis Devulder, Denis Conduché, Laurent Mazet et Thomas Bourdel. Je souhaite les saluer ici, notamment pour les moments de détente (non mathématiques !) que nous avons pu passer ensemble. Un petit clin d'oeil également à Tanguy Rivoal pour les discussions diverses que nous avons eues et pour m'avoir introduit dans l'antre de l'Arbre Sec. Par ailleurs, je regretterai l'ambiance très détendue du plateau des doctorants 7C de Chevaleret.

Je tiens ici à remercier du fond du coeur ma mère, mon père et mon beau-père pour la confiance qu'ils ont toujours placée en moi. Je voudrais enfin remercier ma compagne Sandrine, à qui je dédie cette thèse, pour son soutien constant, surtout dans les moments les plus durs.

Table des matières

Keywords : elliptic curves, abelian varieties, normalised height, Lehmer problem, slopes inequality
2000 Mathematics Subject Classification : 11G50, 14G40, 14K22
Adresse électronique : ratazzi@math.jussieu.fr

Introduction

Soit G le groupe multiplicatif $\mathbb{G}_m^n$ défini sur $K = \mathbb{Q}$ ou une variété abélienne A/K définie sur un corps de nombres K. Si G est une variété abélienne, on la considère donnée avec un fibré en droites ample et symétrique L. On peut construire sur les points de $G(\overline{\mathbb{Q}})$ une hauteur particulièrement agréable : la hauteur de Néron-Tate $\widehat{h}_L$. Si $P \in G(\overline{\mathbb{Q}})$ et r un entier, cette hauteur vérifie

$$\widehat{h}_L(rP) = \begin{cases} r^2\widehat{h}_L(P) & \text{si } G \text{ est une variété abélienne,} \\ r\widehat{h}_L(P) & \text{si } G = \mathbb{G}_m^n. \end{cases}$$

Dans le cas où $G = \mathbb{G}_m$ il s'agit de la hauteur de Weil (logarithmique absolue) usuelle h. De manière générale cette hauteur est toujours positive et s'annule précisément sur les points de torsion de $G(\overline{\mathbb{Q}})$. On peut facilement voir que le minorant de la hauteur des points qui ne sont pas de torsion doit dépendre du degré D du corps de définition du point dont on minore la hauteur. On va donc avoir une minoration de la forme $\widehat{h}_L(P) \geq \frac{c(G)}{\psi(D)}$ où $D = [K(P) : K]$ et ψ est une fonction croissante. Si l'on ne considère que des points $P \in G(K)$ (autrement dit en considérant $\psi(D)$ comme une constante) et que l'on s'intéresse à la variation de G dans cette minoration, les conjectures de Lang et Silverman nous indiquent que l'on peut prendre $c(G)$ de la forme $c_1(\dim G)\max\{h_{\text{Falt}}(G/K), 1\}$ où h_{Falt} est la hauteur de Faltings de la variété. Le problème de Lehmer quant à lui consiste à fixer G/K (autrement dit à considérer $c(G)$ comme une constante) et à trouver la fonction ψ optimale. C'est à ce dernier problème que l'on s'intéresse dans toute la suite. On peut également s'intéresser à une généralisation naturelle de ce problème qui consiste à minorer non pas la hauteur d'un point, mais la hauteur d'une sous-variété (non de torsion) de G, en fonction cette fois-ci du degré géométrique de la variété considérée. Un autre type d'extension consiste à obtenir une minoration de la hauteur des points en fonction de $[K^{\text{ab}}(P) : K^{\text{ab}}]$, où K^{ab} est la clôture abélienne de K, c'est-à-dire ne dépendant que de la partie non-abélienne du degré $[K(P) : K]$. Enfin on pourrait, cela reste à faire, englober tous ces résultats dans une généralisation globale où l'on minorerait la hauteur des sous-variétés par un invariant du type degré géométrique, généralisant dans le cas des points le degré $[K^{\text{ab}}(P) : K^{\text{ab}}]$.

Ces problèmes de Lehmer ont au moins deux types d'applications : le problème classique peut servir, en conjonction avec une bonne compréhension des points de torsion de $G(\overline{\mathbb{Q}})$, à déterminer si des points $P_1, \ldots, P_m$ de $G(\overline{\mathbb{Q}})$ sont ou non linéairement indépendants. On trouvera une discussion de ce sujet dans l'article [34] de Masser. L'autre application possible

est une utilisation du résultat concernant le problème de Lehmer en dimension supérieure et avec le degré non-abélien (au moins dans le cas des variété abéliennes). Il s'agit des problèmes où l'on cherche à montrer que le cardinal de l'intersection d'une courbe avec l'ensemble des sous-groupes algébriques de codimension donnée de G est fini ou au moins de hauteur bornée. Les preuves des résultats de ce type nécessitent de bonnes minorations de la hauteur sur G. Nous renvoyons à l'article [14] de Bombieri, Masser et Zannier dans le cas où $G = \mathbb{G}_m^n$ et à l'article [45] de Rémond dans le cas où G est une variété abélienne.

L'ensemble de cette thèse concerne le problème de Lehmer et ses différents avatars. Nous nous proposons d'améliorer et d'étendre un certain nombre de résultats que nous allons maintenant rappeler.

Soient x un nombre algébrique et $h(x)$ sa hauteur logarithmique absolue. Le problème classique de Lehmer est le suivant :

Conjecture 1 (Problème de Lehmer) *Il existe une constante $c > 0$ telle que pour tout nombre algébrique qui n'est pas une racine de l'unité, on a*

$$h(x) \geq \frac{c}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

En fait dans son article [32] de 1933, Lehmer ne formule pas une conjecture mais pose juste une question. Il pose même plus exactement la question inverse et il ajoute "whether this is true or not, I do not know".

La conjecture est trivialement vraie si on se restreint au sous-ensemble des nombres algébriques qui ne sont pas des entiers algébriques. Dans ce cas on peut même prendre $c = \log 2$. En 1971 Smyth [52] montre que la conjecture formulée précédemment est vraie pour le sous-ensemble de $\overline{\mathbb{Q}}$ constitué des nombres non-réciproques[1]. C'est à ce moment-là qu'apparaît la version indiquée de la conjecture de Lehmer. En 1979 Dobrowolski [23] obtient, au choix de la constante c près, le meilleur résultat général en direction de la conjecture connu à ce jour. Si x est un nombre algébrique, on note $D = \deg(x) = [\mathbb{Q}(x) : \mathbb{Q}]$.

Théorème 1 (Dobrowolski) *Il existe une constante $c > 0$ telle que pour tout nombre algébrique qui n'est pas une racine de l'unité, on a*

$$h(x) \geq \frac{c}{D} \left(\frac{\log \log 3D}{\log 2D} \right)^3.$$

Dans son article, Dobrowolski montre même que l'on peut prendre $c = \frac{1}{1200}$. Depuis, Voutier [58] a montré que dans l'énoncé précédent, le choix $c = \frac{1}{4}$ convient déja.

[1] les nombres réciproques étant les nombres racines d'un polynôme P vérifiant $P(X) = X^{\deg P} P(\frac{1}{X})$.

La preuve de Dobrowolski est une preuve typique de transcendance. On suppose par l'absurde le résultat faux, ce qui nous donne un x de grand degré D et de petite hauteur. On construit alors, en utilisant un lemme de Siegel, un polynôme P à coefficients entiers qui s'annule avec un grand ordre en x. L'idée nouvelle de Dobrowolski consiste à faire une extrapolation aux places ultramétriques : en utilisant le petit théorème de Fermat, on montre que le polynôme P s'annule modulo p premier en x^p. Utilisant l'hypothèse de petite hauteur sur x et l'inégalité de Liouville (ou la formule du produit) on montre alors que P s'annule en un grand nombre de x^p (tout ceci étant convenablement quantifié en fonction de D). Un lemme de zéros (trivial dans ce cas : il suffit de compter les zéros du polynôme et de comparer à son degré) permet alors de conclure.

Depuis, l'énoncé et la preuve de Dobrowolski ont fait l'objet d'extensions diverses : cas des courbes elliptiques, problème en dimension supérieure et raffinement du problème en utilisant la partie non-abélienne de D. Nous allons maintenant faire un tour d'horizon de ces diverses extensions.

Cas des courbes elliptiques

En 1981, Laurent [31] étend la conjecture de Lehmer aux courbes elliptiques et étend la preuve ainsi que le résultat de Dobrowolski au cas des courbes elliptiques à multiplication complexe. On note $\widehat{h}(\cdot)$ la hauteur de Néron-Tate sur la courbe elliptique $E(\overline{K})$.

Conjecture 2 (Problème de Lehmer elliptique) *Soit E/K une courbe elliptique sur un corps de nombres K. Il existe une constante strictement positive $c(E/K)$ telle que pour tout point $P \in E(\overline{K})\backslash E_{\mathrm{tors}}$, on a*

$$\widehat{h}(P) \geq \frac{c(E/K)}{[K(P):K]}.$$

Théorème 2 (Laurent) *Soit E/K une courbe elliptique à multiplication complexe sur un corps de nombres K. Il existe une constante strictement positive $c(E/K)$ telle que pour tout point $P \in E(\overline{K})\backslash E_{\mathrm{tors}}$ de degré $D = [K(P):K]$, on a*

$$\widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 3D}{\log 2D}\right)^3.$$

Généralisation en dimension supérieure

En 1999-2000, David et Hindry [19] puis Amoroso et David [2] généralisent ces résultats en dimension supérieure : sur les variétés abéliennes pour David et Hindry et sur $\mathbb{G}_m^n$ pour Amoroso et David. Sur $\mathbb{G}_m^n$ on choisit une compactification, par exemple $\mathbb{P}^n$ ou $(\mathbb{P}^1)^n$, et on

se donne un fibré en droites ample L sur cette compactification. Sur une variété abélienne A/K on se donne un fibré en droites ample et symétrique L. Ceci permet de définir un degré $\deg_L$. On renvoie au chapitre 1 pour une définition précise de ce degré. Dans la suite quand on utilisera le degré sur $\mathbb{G}_m^n$, il sera toujours sous-entendu qu'on prend celui-ci dans une compactification donnée et pour un fibré ample fixé, par exemple $\mathcal{O}(1)$ sur $\mathbb{P}^n$. Les auteurs de [19] et [2] utilisent en fait un invariant plus naturel pour le problème de Lehmer en dimension supérieure que le degré : l'indice d'obstruction

$$\delta_L(x) = \min\left\{\deg_L V^{\frac{1}{\operatorname{codim} V}} \ / \ V \text{sous-variété sur } K,\ K\text{-irréductible de } G \text{ et } x \in V(\overline{K})\right\}$$

où G est la variété abélienne A/K ou le tore $\mathbb{G}_m^n$ selon le cas.

Remarque 1 En prenant $V = \overline{\{x\}}$ l'adhérence schématique de x dans G (*i.e.*, en considérant toute l'orbite de x sous l'action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$), on voit que

$$1 \leq \delta_L(x) \leq [K(x) : K]^{\frac{1}{\dim G}}.$$

Conjecture 3 (Problème de Lehmer en dimension supérieure) *Il existe une constante $c(n) > 0$ telle que pour tout point $P \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

$$\widehat{h}_L(P) \geq \frac{c(n)}{\delta_L(P)}.$$

Théorème 3 (Amoroso-David) *Il existe une constante $c(n) > 0$ telle que pour tout point $P \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

$$\widehat{h}_L(P) \geq \frac{c(n)}{\delta_L(P)} \left(\log 2\delta_L(P)\right)^{-\kappa(n)},$$

où $\kappa(n) = (n+1)((n+1)!)^n - n$.

Dans le cas abélien, en notant $\widehat{h}_L(\cdot)$ la hauteur de Néron-Tate associée à un fibré en droites symétrique ample L, on a

Conjecture 4 (Problème de Lehmer abélien) *Soient A/K une variété abélienne de dimension g sur un corps de nombres et L un fibré en droites ample et symétrique sur A. Il existe une constante $c(A/K, L)$ strictement positive telle que pour tout point $P \in A(\overline{K})$ d'ordre infini modulo toute sous-variété abélienne stricte de A, on a*

$$\widehat{h}_L(P) \geq \frac{c(A/K, L)}{\delta_L(P)}. \tag{1}$$

De plus, en terme du degré $D = [K(P) : K]$, on a pour tout point $P \in A(\overline{K})$ qui n'est pas de torsion

$$\widehat{h}_L(P) \geq \frac{c(A/K, L)}{D^{\frac{1}{g_0}}}, \tag{2}$$

où g_0 est la dimension du plus petit sous-groupe algébrique contenant le point P.

Dans la direction de cette conjecture, David et Hindry obtiennent le

Théorème 4 (David-Hindry) *Soient A/K une variété abélienne de dimension g, de type C.M. sur un corps de nombres et L un fibré en droites ample et symétrique. Il existe une constante $c(A/K, L) > 0$ telle que pour tout point $P \in A(\overline{K})$ d'ordre infini modulo toute sous-variété abélienne, on a*

$$\widehat{h}_L(P) \geq \frac{c(A/K, L)}{D^{\frac{1}{g}}} \left(\log 2D\right)^{-\kappa(g)},$$

où $D = [K(P) : K]$ et $\kappa(g) = (2g(g+1)!)^{g+2}$.

En fait ils remarquent que leur preuve donne même le théorème où l'on remplace $D^{\frac{1}{g}}$ par $\delta_L(P)$ et $\log 2D$ par $\log 2\delta_L(P)$, résultat plus proche de la partie (1) de leur conjecture.

Problème de Lehmer pour les sous-variétés

Une généralisation naturelle des énoncés précédents est la suivante : minorer la hauteur des sous-variétés non de torsion de G ($G = A$ ou $G = \mathbb{G}_m^n$). Dans les cas multiplicatif et abélien, David et Philippon ont formulé les conjectures généralisant au cas des sous-variétés les énoncés du type Lehmer. Nous donnons ici des énoncés faisant intervenir le degré plutôt que l'indice d'obstruction. Ces énoncés sont probablement plus intuitifs, par contre ils ne généralisent que la partie (2) des énoncés précédents. On pourrait également formuler des conjectures généralisant la partie des énoncés précédents utilisant l'indice d'obstruction d'une sous-variété.

Conjecture 5 (David-Philippon) *Soit n un entier non nul. Il existe une constante $c(n) > 0$ telle que pour toute sous-variété V stricte de $\mathbb{G}_m^n$, $\mathbb{Q}$-irréductible et telle que $V_{\overline{\mathbb{Q}}}$ n'est pas réunion de sous-variétés de torsion, on a l'inégalité*

$$\frac{\widehat{h}_L(V)}{\deg_L V} \geq c(n)(\deg_L V)^{-\frac{1}{s-\dim V}},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V.

Conjecture 6 (David-Philippon) *Soient A/K une variété abélienne sur un corps de nombres K et L un fibré en droites ample et symétrique. Il existe une constante strictement positive $c(A/K, L)$ telle que pour toute sous-variété V stricte de A sur K, K-irréductible et telle que $V_{\overline{K}}$ n'est pas réunion de sous-variétés de torsion, on a l'inégalité*

$$\frac{\widehat{h}_L(V)}{\deg_L(V)} \geq c(A/K, L) \deg_L(V)^{-\frac{1}{s-\dim V}},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V.

Dans le cas multiplicatif, Amoroso et David montrent (sans toutefois l'écrire explicitement) dans [4] que la conjecture 3 entraîne la conjecture 5 et, en utilisant leur résultat de Lehmer en dimension supérieure, il obtiennent en direction de la conjecture 5 le résultat suivant :

Théorème 5 (Amoroso-David) *Soit n un entier non nul. Il existe une constante strictement positive $c(n)$ telle que pour toute sous-variété V stricte de $\mathbb{G}_m^n$, $\mathbb{Q}$-irréductible et telle que $V_{\overline{\mathbb{Q}}}$ n'est pas réunion de sous-variétés de torsion, on a l'inégalité*

$$\frac{\widehat{h}_L(V)}{\deg_L V} \geq c(n)(\deg_L V)^{-\frac{1}{s-\dim V}} \left(\log 2 \deg_L V\right)^{-\kappa(n)},$$

où $\kappa(n) = (n+1)((n+1)!)^n - n$ et s est la dimension du plus petit sous-groupe algébrique contenant V.

Raffinement en dimension 1

Dans les articles [5] et [6], Amoroso et Dvornicich puis Amoroso et Zannier étendent le problème de Lehmer sur $\mathbb{G}_m$ au cas des extensions abéliennes relatives. Précisément, en notant K^{ab} la clôture abélienne d'un corps de nombres K, ils énoncent la conjecture et démontrent le théorème suivant :

Conjecture 7 (Amoroso-Zannier) *Soit K un corps de nombres. Il existe une constante strictement positive $c(K)$, telle que*

$$\forall x \in \mathbb{G}_m(\overline{K})\backslash\mu_\infty, \quad h(x) \geq \frac{c(K)}{D},$$

où $D = [K^{\mathrm{ab}}(x) : K^{\mathrm{ab}}]$.

Théorème 6 (Amoroso-Zannier) *Soit K un corps de nombres. Il existe une constante $c(K)$ strictement positive, telle que*

$$\forall x \in \mathbb{G}_m(\overline{K})\backslash\mu_\infty, \quad h(x) \geq \frac{c(K)}{D} \left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

où $D = [K^{\mathrm{ab}}(x) : K^{\mathrm{ab}}]$.

La conjecture 7 est bien évidemment une généralisation du problème de Lehmer initial : on travaille avec un corps de nombres K au lieu de travailler avec $\mathbb{Q}$ et surtout on utilise le degré $[K^{\mathrm{ab}}(x) : K^{\mathrm{ab}}]$ qui est la partie non-abélienne du degré usuel $[K(x) : K]$. Le théorème 6 étend le résultat de Amoroso et Dvornicich qui traitait le cas où x appartenait à une extension abélienne de K, *i.e.*, le cas $D = 1$. C'est précisément ce théorème, dans le cas $D = 1$, qui a été étendu aux courbes elliptiques à multiplication complexe ou ayant un j-invariant non-entier par Baker dans [8], puis par Silverman [50] dans le cas des courbes elliptiques sans multiplication complexe. Ainsi pour les courbes elliptiques, on a

Théorème 7 (Baker-Silverman) *Soit E/K une courbe elliptique. Il existe une constante strictement positive $c(E/K)$ telle que*

$$\forall P \in E(K^{\mathrm{ab}})\backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq c(E/K).$$

Ce dernier résultat a été récemment étendu par Baker et Silverman (cf. [9]) au cas des variétés abéliennes.

Théorème 8 (Baker-Silverman) *Soient A/K une variété abélienne sur un corps de nombres K et L un fibré en droites ample et symétrique. Il existe une constante strictement positive $c(A/K, L)$ telle*

$$\forall P \in A(K^{\mathrm{ab}})\backslash A_{\mathrm{tors}}, \quad \widehat{h}_L(P) \geq c(A/K, L).$$

Contenu de la thèse

Le premier chapitre est un chapitre de rappels. Nos résultats originaux sont présentés dans les chapitres 2 à 6 qui sont rédigés sous la forme d'articles logiquement indépendants les uns des autres. Le chapitre 2 correspond à un article à paraître au *Journal of Number Theory* et le chapitre 3 à un article à paraître dans la revue *Acta Arithmetica*.

La **première partie** de la thèse est consacrée au problème de Lehmer sur les sous-variétés des variétés abéliennes.

Dans le **chapitre 1**, nous faisons un certain nombre de rappels concernant les degrés géométrique, arithmétique et la notion de hauteur de points et de variétés. Nous donnons, notamment, une construction complète, par récurrence, de la hauteur sur les variétés en suivant [17]. Nous profitons également de cette partie introductive pour donner les preuves des propriétés simples vérifiées par le degré arithmétique, ces démonstrations n'étant pas toujours très détaillées dans la littérature.

Dans le **chapitre 2**, nous montrons l'analogue, dans le cadre des variétés abéliennes, des résultats de [4]. Précisément, en prouvant un résultat de densité de petits points (cf. le théorème 27 du chapitre 2), nous montrons en corollaire que :

Théorème 9 *Soient A/K une variété abélienne de type C.M. sur K et L un fibré en droites ample et symétrique sur A. Il existe une constante strictement positive $c(A/K, L)$ telle que si V est une sous-variété algébrique stricte de A sur K, K-irréductible et telle que $V_{\overline{K}}$ n'est pas réunion de sous-variétés de torsion, on a l'inégalité*

$$\frac{\widehat{h}_L(V)}{\deg_L(V)} \geq c(A/K, L) \deg_L(V)^{-\frac{1}{s-\dim V}} \left(\log(3 \deg_L(V))\right)^{-\kappa(s)},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V.

Il suit de la preuve de ce théorème que toute avancée en direction de la conjecture 4 entraîne une avancée similaire en direction de la conjecture 6. Autrement dit, une bonne minoration de la hauteur des points (non de torsion) entraîne une bonne minoration de la hauteur de toutes les sous-variétés (non de torsion) de A. En particulier nous prouvons également le résultat suivant :

Théorème 10 *La conjecture 4 de David-Hindry implique la conjecture 6 de David-Philippon.*

La preuve du résultat principal de ce chapitre, à savoir le théorème 27, se fait essentiellement en utilisant des arguments de géométrie sur les variétés abéliennes. Il n'y a pas de transcendance dans ce chapitre, si ce n'est à travers l'application du théorème principal de [19] qui, lui, repose effectivement sur une preuve de transcendance.

Dans le **chapitre 3**, nous améliorons le théorème 9 précédent dans le cas particulier des hypersurfaces de variétés abéliennes de type C.M., étendant ainsi au cadre des variétés abéliennes le résultat analogue sur $\mathbb{G}_m^n$ de Amoroso et David [3]. Dans ce cadre restreint aux hypersurfaces, nous montrons un résultat sensiblement plus fin en direction de la conjecture 6 : on peut prendre pour κ une valeur absolue, indépendante de g. En notant $\delta_{i,j}$ le symbole de Kronecker (valant 1 si $i = j$ et 0 sinon), nous démontrons le résultat suivant :

Théorème 11 *Soient A/K une variété abélienne de type C.M. et L un fibré en droites ample et symétrique sur A. Il existe une constante $c(A/K, L)$ strictement positive telle que si V est une hypersurface irréductible de A sur K telle que $V_{\overline{K}}$ n'est pas réunion de sous-variétés de torsion, on a l'inégalité*

$$\widehat{h}_L(V) \geq c(A/K, L) \frac{(\log\log 3 \deg_L V)^{1+2\delta_{g-s,1}}}{(\log 2 \deg_L V)^{2+\delta_{g-s,1}}},$$

où s est la dimension du stabilisateur de V.

La preuve de ce résultat se fait cette fois-ci en utilisant la machinerie classique de transcendance. Au lieu d'appliquer brutalement le résultat principal de [19], nous reprenons leur démonstration (dont le schéma est calqué sur celui de Dobrowolski) et nous l'adaptons au cadre qui nous intéresse.

En supposant que A/K est une courbe elliptique, L le fibré en droites associé au diviseur $3(0)$ et $V = \overline{\{P\}}$ l'image schématique d'un point d'ordre infini $P \in A(\overline{K})$ défini sur une extension finie de degré $D = [K(P) : K]$, nous retrouvons exactement le théorème 2 de Laurent sur le problème de Lehmer elliptique. Dans le cas d'une "vraie" hypersurface, *i.e.*, quand $\delta_{g-s,1} = 0$, nous obtenons une minoration un peu meilleure.

Dans la **seconde partie** de la thèse nous nous intéressons au problème de Lehmer et à ses différentes variantes en dimension 1.

Dans le **chapitre 4**, nous retrouvons le théorème 1 de Dobrowolski, essentiellement en transcrivant sa preuve dans le formalisme des pentes que J.-B. Bost a introduit dans [15]. Il ne s'agit ici en fait que d'une première étape d'un travail qui reste à faire : l'objectif était ici de voir dans quelle mesure les preuves de transcendance "classiques" concernant le problème de Lehmer peuvent se traduire en utilisant l'inégalité des pentes. Il serait maintenant intéressant d'essayer d'adapter la preuve du théorème 2 de Laurent dans ce langage. L'idée est que l'inégalité des pentes permet de mieux exploiter la géométrie des objets avec lesquels on travaille. Si ceci n'est pas flagrant dans le cas de $\mathbb{G}_m$, cela le serait certainement plus dans le cas d'une courbe elliptique E, où le formalisme des pentes permettrait d'incorporer directement l'inégalité sur la hauteur de Néron-Tate, sans avoir à passer par l'artifice consistant à plonger E dans $E \times E$ et à considérer un "gros" multiple du point considéré en vue de minimiser la différence entre hauteur de Néron-Tate et hauteur de Weil. On pourrait peut-être obtenir ainsi un parallélisme complet pour le problème de Lehmer sur le groupe multiplicatif et sur les courbes elliptiques à multiplication complexe.

Dans le **chapitre 5**, nous nous intéressons, dans le cadre des courbes elliptiques, au raffinement utilisant la partie non-abélienne du degré. Nous obtenons :

Théorème 12 *Soit E/K une courbe elliptique à multiplication complexe. Il existe une constante $c(E/K)$ strictement positive, telle que*

$$\forall P \in E(\overline{K})\backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.

Ce résultat rend naturel de généraliser la conjecture 7 aux courbes elliptiques :

Conjecture 8 *Soit E/K une courbe elliptique. Il existe une constante strictement positive $c(E/K)$, telle que*

$$\forall P \in E(\overline{K})\backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D},$$

où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.

L'exposant 13 apparaissant en exposant des facteurs log et log log dans le théorème 12 peut être amélioré au prix d'une hypothèse supplémentaire.

Théorème 13 *Soit $c_0 > 0$. Il existe une constante strictement positive $c(E/K, c_0)$, telle que : pour toute extension abélienne L/K et pour tout point $P \in E(\overline{K})\backslash E_{\mathrm{tors}}$ vérifiant $D = [L(P) : L]$, si le nombre de nombres premiers qui se ramifient dans L est borné par $c_0 \left(\frac{\log 2D}{\log\log 5D}\right)^2$, alors on a l'inégalité*

$$\widehat{h}(P) \geq \frac{c(E/K, c_0)}{D} \left(\frac{\log\log 5D}{\log 2D}\right)^3.$$

On voit qu'en imposant une contrainte sur l'étendue de la ramification dans l'extension abélienne (théorème 13), nous obtenons une généralisation du théorème 2 de Laurent. Dans le cas général (théorème 12), sans imposer aucune condition, nous obtenons une minoration optimale aux puissances de log près, avec un exposant légèrement dégradé par rapport au cas classique : on a comme puissance de log un exposant 13 au lieu d'un exposant 3 ; toutefois cet exposant 13 est le même que dans le cas multiplicatif dû à Amoroso et Zannier (cf. théorème 6). Ce théorème 12, dans le cas des courbes elliptiques à multiplication complexe, généralise au cas D quelconque un précédent résultat de Baker [8] (cf. théorème 7).

Le théorème 12 est une première étape en direction d'un résultat plus général : une généralisation naturelle de ce chapitre serait l'extension au cas des variétés abéliennes de type C.M. L'idée serait pour cela de reprendre l'article [19] en incorporant les nouvelles idées que l'on trouve dans [6] et dans ce chapitre. Cette extension aurait d'autant plus d'intéret qu'elle permettrait de rendre d'autant plus performant le théorème 1.4 de l'article [45] de Rémond déja mentionné en début d'introduction. Notons que notre théorème 12 permet déjà de simplifier la preuve du theorem 2. de Viada [57]. Avant de donner l'énoncé de ce théorème, on introduit une définition : on dit qu'une courbe sur une variété abélienne A est *transverse* si elle n'est contenue dans aucune translatée de sous-variété abélienne de A différente de A.

Théorème 14 (Viada) *Soient E/K une courbe elliptique à multiplication complexe, n un entier non nul et C/K une courbe transverse dans E^n. Pour $r \geq 0$ on considère les ensembles*

$$S_r(C) := \bigcup_{\mathrm{codim}\, G \geq r} G \cap C(\overline{K})$$

où l'union porte sur les sous-groupes algébriques G de E^n de codimension au moins r. Alors l'ensemble $S_2(C)$ est fini.

La preuve de Viada est calquée sur celle de Bombieri, Masser et Zannier [14] dans le cas de $\mathbb{G}_m^n$. Elle utilise le fait que la hauteur des points de $S_1(C)$ est bornée. Il s'agit du Theorem 1. du même article de Viada qui résulte simplement des propriétés fonctorielles des hauteurs et du théorème du cube pour les variétés abéliennes. Ceci étant acquis on constate, en appliquant le théorème de Northcott, qu'il suffit alors de montrer que le degré des points de $S_2(C)$ est borné. C'est la partie difficile de la preuve. Viada montre ceci en deux étapes : la première consiste à montrer la finitude de l'ensemble $S_3(C)$. La seconde étape consiste à montrer la finitude de $S_2(C)$ en utilisant un subtil argument cohomologique. Nous montrons au chapitre 5 comment éviter cet argument cohomologique en appliquant notre théorème 12. En fait l'utilisation de ce théorème 12 permet de ramener la seconde étape à la première.

Dans le **chapitre 6**, nous faisons deux remarques concernant la conjecture de Lehmer abélienne sur les points : nous montrons que la partie (1) de la conjecture 4 entraîne en fait la partie (2) de cette même conjecture et nous montrons de même que le théorème 4 entraîne le

Corollaire 1 *Soient A/K une variété abélienne de dimension g, de type C.M. sur un corps de nombres et L un fibré en droites ample et symétrique sur A. Il existe une constante $c(A/K, L) > 0$ telle que pour tout point $P \in A(\overline{K})$ d'ordre infini, on a*

$$\widehat{h}_L(P) \geq \frac{c(A/K, L)}{D^{\frac{1}{g_0}}} (\log 2D)^{-\kappa(g_0)},$$

où $D = [K(P) : K]$, g_0 est la dimension du plus petit sous-groupe algébrique contenant P et $\kappa(g_0) = (2g_0(g_0 + 1)!)^{g_0+2}$.

Ce résultat améliore le meilleur résultat précédemment connu pour les variétés abéliennes de type C.M., dû à Masser [33] qui obtient, pour tout point P d'ordre infini de $A(\overline{K})$:

$$\widehat{h}_L(P) \geq \frac{c(A/K, L)}{D^2 \log 2D}.$$

Par ailleurs, nous remarquons également dans ce chapitre que la conjecture 4 entraîne la version multihomogène de cette conjecture telle que formulée dans [19] :

Conjecture 9 (David-Hindry) *Soient A/K une variété abélienne de dimension g sur un corps de nombres et L un fibré en droites symétrique ample sur A. Pour tout entier $n \in \mathbb{N}$ il existe une constante $c(A/K, L, n) > 0$ telle que pour tout n-uplet $(P_1, \ldots, P_n)$ de points d'ordre infini dans $A(\overline{K})$, End(A)-linéairement indépendants, on a :*

$$\prod_{i=1}^{n} \widehat{h}_L(P_i) \geq \frac{c(A/K, L, n)}{D^{\frac{1}{g}}},$$

où $D = [K(P_1, \ldots, P_n) : K]$.

Nous précisons dans cet énoncé l'hypothèse "linéairement indépendants" en $\mathrm{End}(A)$-linéairement indépendants, le même énoncé avec pour seule hypothèse $\mathbb{Z}$-linéairement indépendants étant faux comme nous l'expliquons dans ce dernier chapitre.

Première partie

Problème de Lehmer sur les variétés

Chapitre 1

Degré géométrique, degré arithmétique et hauteur

Dans ce chapitre, on fait des rappels sur les notions de degré géométrique, degré arithmétique, hauteur sur les points et hauteur sur les variétés. Nous aurons besoin de ces notions dans les autres chapitres : la hauteur (tant sur les points que sur les variétés) étant l'objet fondamental sur lequel s'appuie toute cette thèse. Nous rappelons les définitions ainsi que les propriétés usuelles dont nous nous servirons ensuite. Dans le cas du degré arithmétique sur Spec $\mathcal{O}_K$, nous donnons la preuve des quelques propriétés simples que nous rappelons, ces démonstrations n'étant pas toujours très détaillées dans la littérature.

Soit K un corps. Si F/K est une extension de corps et X un Spec K-schéma, alors, la notation X_F dénote le produit fibré $X \times_{\text{Spec } K} \text{Spec } F$ et $X(F)$, appelé l'ensemble des *points F-rationnels de X*, dénote l'ensemble $\text{Mor}_K(\text{Spec } F, X)$. On fera fréquemment l'abus consistant à écrire F au lieu de Spec F quand F est un corps ou même un anneau. On dit que V est une *variété algébrique sur K* si V est un K-schéma de type fini, irréductible et géométriquement réduit. Par sous-variété on entendra toujours sous-variété qui est un sous-schéma fermé. On appelle *courbe* toute variété de dimension 1 et on note $\mathbb{P}^n$ ou $\mathbb{P}^n_K$ l'espace projectif sur K de dimension n.

1.1 Degré géométrique

Dans ce paragraphe on définit le degré géométrique de deux façons : la première dans le cas projectif, en utilisant le polynôme de Hilbert ; la seconde en utilisant la théorie de l'intersection. On commence par définir le degré géométrique dans le cas des variétés projectives. Pour cela, on se ramène au cas des sous-variétés de $\mathbb{P}^n$: soient V une variété projective sur K et L un fibré en droites très ample. Il existe un plongement $\varphi : V \hookrightarrow \mathbb{P}^n$

correspondant à L tel que si $\mathcal{O}(1)$ dénote le fibré standard sur $\mathbb{P}^n$ (dont les sections globales sont les polynômes homogènes en $n+1$ variables de degré 1), alors $L = \varphi^*\mathcal{O}(1)$. Supposons un instant connue la notion de *degré projectif* d'une sous-variété de $\mathbb{P}^n$.

Définition 1 En notant $\deg_K(.)$ le degré projectif, on définit et on note $\deg_L V$, *le degré de* V relativement au fibré en droites très ample L, par

$$\deg_L V = \deg_K(\varphi(V)).$$

Il suffit donc de définir le degré d'une sous-variété de $\mathbb{P}^n$. C'est ce que l'on fait dans ce qui suit.

Soit V une sous-variété de $\mathbb{P}^n$. Elle est déterminée par la donnée d'un idéal saturé $I = I(V)$ de $K[x_0, \ldots, x_n]$. On pose $A = K[x_0, \ldots, x_n]/I(V)$ et on note A_ν la composante homogène de degré ν de A.

Définition 2 Un objet fondamental associé à V est sa *fonction de Hilbert*

$$H(V, \cdot) : \mathbb{N} \to \mathbb{N}.$$

Elle est définie par la formule

$$\forall \nu \in \mathbb{N}, \quad H(V, \nu) = \dim_K A_\nu.$$

Le résultat principal concernant cette fonction est qu'elle est asymptotiquement polynomiale. Autrement dit, on a le

Théorème 15 (Hilbert) *Il existe un unique polynôme,* $P(V, \cdot)$ *de degré* $d = \dim V$, *tel que*

$$\forall \nu \gg 0, \qquad P(V, \nu) = H(V, \nu).$$

On appelle ce polynôme le *polynôme de Hilbert* de V. Son terme dominant est de la forme

$$\frac{m}{d!}\nu^d.$$

Définition 3 Avec les notations précédentes, on définit le *degré projectif* de V comme étant le nombre m. On le note $\deg_K(V)$.

Revenons au cas général d'une variété projective V munie d'un fibré en droites (très) ample L. On peut en fait définir le polynôme de Hilbert de manière complètement explicite et pas uniquement pour des valeurs asymptotiques :

Théorème 16 (Riemann-Roch) *Si* $\chi(V, L^{\otimes\nu}) = \sum(-1)^i \dim_K H^i(V, L^{\otimes\nu})$ *désigne la caractéristique d'Euler-Poincaré de* V, *alors,*

$$\forall \nu \in \mathbb{N}, \qquad P(V, \nu) = \chi(V, L^{\otimes\nu}).$$

Exemple 1 Dans le cas d'une courbe V géométriquement irréductible, lisse sur un corps K algébriquement clos, on rappelle que par définition *le genre* $g(V)$ est la dimension du K-espace vectoriel $\Gamma(V, \Omega^1_{V/K})$. Par dualité de Serre (valable sur une variété projective lisse sur un corps algébriquement clos), on peut également voir le genre comme étant la dimension du K-espace vectoriel $H^1(V, \mathcal{O}_V)$. Le théorème 16 précédent nous donne $P(V, 0) = \chi(V, \mathcal{O}_V)$. Or un théorème classique d'annulation de la cohomologie de Grothendieck nous assure qu'ici,

$$\chi(V, \mathcal{O}_V) = \dim_K \Gamma(V, \mathcal{O}_V) - \dim_K H^1(V, \mathcal{O}_V) = 1 - g(V).$$

En effet, pour une variété X/K propre, lisse et géométriquement connexe, toute fonction régulière est constante. Sur un corps algébriquement clos, on peut donc, non seulement lire le degré, mais aussi lire le genre d'une courbe projective sur son polynôme de Hilbert. De plus, en réappliquant maintenant le même argument avec $\nu = 1$ et en utilisant les notations classiques en géométrie, on obtient le théorème de Riemann-Roch usuel,

$$l(L) - l(K_V - L) = \deg_L V + 1 - g(V).$$

Il se trouve que le degré projectif est un nombre entier. Sur $\mathbb{C}$ on peut montrer qu'il s'agit du cardinal du schéma de dimension zéro $X \cap H$, pour tout plan général H de $\mathbb{P}^n_{\mathbb{C}}$ de dimension $n - d$. Le problème de cette assertion est qu'il faut définir la notion de "général". Ici, dire que le plan est général signifie qu'il est tel qu'une déformation infinitésimale ne change pas le résultat. Autrement dit, quand on "bouge un peu" le plan, le nombre considéré ne change pas. Il s'agit donc bien d'une définition géométrique.

Exemple 2 Sur $\mathbb{C}$ le degré d'un point fermé est 1. De même, étant données une courbe ou une hypersurface dans $\mathbb{P}^n_{\mathbb{C}}$ on peut lire le degré sur un dessin : il suffit de couper la courbe par un hyperplan général et l'hypersurface par une droite générale, puis de compter le cardinal obtenu.

On peut donner une construction rigoureuse de cette approche du degré d'une variété relativement à un diviseur, en utilisant le produit d'intersection. C'est la méthode la plus intrinsèque. En fait, elle ne nécessite pas de supposer la variété projective ; il suffit de la supposer propre. Comment fait-on ? On se donne une variété X sur un corps K, un fibré en droites (faisceau inversible, diviseur de Cartier) L sur X et une sous-variété V de dimension k de X. L'objectif est de définir un entier appelé *degré de* V relativement à L associé à ces données et qui coïncide avec celui précédemment défini dans le cas projectif. En vue de définir ce degré, on construit un produit d'intersection, noté $\cdot$, sur les diviseurs en suivant le livre de Fulton [25] :

1.1.1 Théorie de l'intersection

Dans tout ce paragraphe, K est un corps et X/K une variété propre sur K de dimension n.

Cycles et équivalence rationnelle

Définition 4 Si R est un anneau local de dimension zéro, on définit la *longueur de* R que l'on note $\lg(R)$, comme étant la longueur n d'une chaîne

$$R \supset \mathfrak{m} = I_1 \supset \ldots \supset I_n = \{0\}$$

d'idéaux tels que $I_k/I_{k+1} \simeq R/\mathfrak{m}$ comme R-modules. (Comme R est local de dimension zéro, la longueur est finie et par le théorème de Jordan-Hölder, cette longueur est bien définie, c'est-à-dire, indépendante du choix d'une chaîne ayant ces propriétés.)

Soit V une sous-variété de X de codimension 1. L'anneau local $\mathcal{O}_{V,X}$ est par définition l'anneau local au point générique de V. Il est de dimension 1. Soit $s \in K^*(X)$, on veut définir l'*ordre* d'annulation *de* s selon V, que l'on note $\mathrm{ord}_V(s)$, de sorte que ce soit un homomorphisme, *i.e.*, tel que :

$$\forall s, t \in K^*(X) \quad \mathrm{ord}_V(st) = \mathrm{ord}_V(s) + \mathrm{ord}_V(t).$$

Tout $s \in K^*(X)$ peut s'écrire sous la forme $s = \frac{a}{b}$, avec $a, b \in \mathcal{O}_{V,X}$. On a donc nécessairement, $\mathrm{ord}_V(s) = \mathrm{ord}_V(a) - \mathrm{ord}_V(b)$. Ainsi, il suffit de définir ord_V pour les éléments de $\mathcal{O}_{V,X}$. On pose alors :

$$\forall s \in \mathcal{O}_{V,X} \quad \mathrm{ord}_V(s) = \lg_{\mathcal{O}_{V,X}} \left(\mathcal{O}_{V,X}/(s)\right).$$

Pour $s \in K^*(X)$ fixé, il existe seulement un nombre fini de sous-variétés V de codimension 1 de X telle que $\mathrm{ord}_V(s) \neq 0$.

Sur la variété X on peut maintenant construire un morphisme naturel φ du groupe des diviseurs de Cartier, noté CaDiv X, dans le groupe des $n-1$-cycles $Z_{n-1}(X)$: soit $D = (U_i, f_i)_{i \in I} \in$ CaDiv X et soit V une sous-variété de codimension 1 de X. On pose

$$\mathrm{ord}_V D = \mathrm{ord}_V f_i, \text{ où } i \text{ est tel que } U_i \cap V \neq \emptyset,$$

ceci ayant un sens car, si j est tel que $U_j \cap V \neq \emptyset$, alors $\frac{f_i}{f_j}$ est inversible sur $U_i \cap U_j$, donc $\mathrm{ord}_V f_i = \mathrm{ord}_V f_j$.

Partant d'un diviseur de Cartier D, on définit ainsi un diviseur de Weil

$$[D] = \sum_V \mathrm{ord}_V D \ [V].$$

L'application φ qui à D associe $[D]$ est un morphisme de groupes.

Définition 5 On appelle groupe des k-cycles sur X et on note $Z_k(X)$, le groupe abélien libre engendré par les sous-variétés V de dimension k de X. Un élément de $Z_k(X)$ est appelé un *k-cycle* et si V est une sous-variété k-dimensionnelle de X, on note $[V]$ (ou abusivement V) l'élément correspondant de $Z_k(X)$.

Définition 6 Si $\alpha = \sum_V n_V[V]$ est un cycle, on définit le *support* de α comme étant

$$\text{supp } \alpha = |\alpha| = \bigcup_{n_V \neq 0} V.$$

Si D est un diviseur de Cartier, on appelle *support* de D et on note $|\ D\ |$, le support du diviseur de Weil associé.

Définition 7 Un k-cycle α est *rationnellement équivalent* à 0, $\alpha \sim 0$, s'il existe un nombre fini de sous-variétés W_i de dimension $k+1$ de X et des $s_i \in K^*(W_i)$ tels que $\alpha = \sum \text{div}(s_i)$. Comme $\text{div}(s^{-1}) = -\text{div}(s)$, les cycles rationnellement équivalents à zéro forment un sous-groupe $\text{Rat}_k(X)$ de $Z_k(X)$. Le groupe des classes de k-cycles modulo équivalence rationnelle sur X est le groupe noté :

$$A_k(X) = Z_k(X)/\text{Rat}_k(X).$$

On définit alors

$$Z_*(X) = \bigoplus_{k=0}^{\dim(X)} Z_k(X) \text{ et de même, } A_*(X) = \bigoplus_{k=0}^{\dim(X)} A_k(X).$$

Produit d'intersection sur les diviseurs : soit V une sous-variété de X sur K de dimension k. On note D le diviseur de Cartier associé au faisceau inversible L et on définit $D \cdot V$, noté également $D \cdot [V]$, dans $\text{A}_{k-1}(|\ D\ | \cap V)$ comme suit :

Notons $j : V \hookrightarrow X$ l'inclusion naturelle. Deux cas se présentent :

- Si $V \subsetneq |\ D\ |$, alors D se restreint en un diviseur de Cartier, j^*D sur V et on pose
$$D \cdot [V] = [j^*D].$$

- Si $V \subseteq |\ D\ |$, on prend l'image réciproque faisceautique de D, *i.e.*, $j^*\mathcal{O}_X(D)$. On obtient ainsi un faisceau inversible sur V. À ce faisceau correspond un diviseur de Cartier, C tel que $\mathcal{O}_V(C) = j^*\mathcal{O}_X(D)$. On note $[C]$ sa classe de diviseur de Weil dans $\text{A}_{k-1}(V)$ et on pose
$$D \cdot [V] = [C].$$

Par linéarité, on en déduit un produit d'intersection entre les diviseurs de Cartier et les cycles de dimension quelconque de X.

1.1.2 Degré d'un cycle

On note toujours X/K une variété propre de dimension n.

Définition 8 Soit $\alpha = \sum n_P[P]$ un 0-cycle sur X. En identifiant $\mathbb{Z}$ et $A_0(\text{Spec } K)$, on définit le *degré du* 0*-cycle* α comme étant :

$$\deg \alpha = \sum n_P[K(P) : K] = \pi_*(\alpha),$$

où π est le morphisme structural de X vers Spec K. On peut maintenant définir le *degré relativement à L* d'une sous-variété V de X : en appliquant k fois l'opération "prendre le produit d'intersection avec D", on obtient un cycle de dimension zéro, $\sum n_P[P]$. On pose alors

$$\deg_L V = \pi_* \left(L^k \cdot [V]\right) = \sum n_P [K(P) : K],$$

où π est le morphisme structural de X vers Spec K. On peut montrer que dans le cas projectif, on retombe sur le degré projectif défini précédemment.

Exemple 3 Si $x \in X(\overline{K})$ est un point $\overline{K}$-rationnel de X, en notant $V := \overline{\{x\}}$ la variété définie en prenant l'image schématique de $x \in X_{\overline{K}}$ dans X, on a :

$$\deg_L(V) = [K(x) : K].$$

1.2 Degré arithmétique sur Spec $\mathcal{O}_K$

Dans cette section, on donne la définition du degré arithmétique sur Spec $\mathcal{O}_K$ le spectre de l'anneau des entiers d'un corps de nombres K et on donne une application de cette notion : l'inégalité des pentes. Cette dernière, introduite pour la première fois par J.-B.Bost dans son article [15], a connu récemment quelques belles applications en géométrie diophantienne (voir par exemple [15], [16] et [26]). En utilisant ce langage et surtout l'inégalité des pentes, on donne au chapitre 4 une démonstration du théorème de Dobrowolski [23] concernant le problème de Lehmer sur $\mathbb{G}_m$.

1.2.1 Degré arithmétique : définition

Désormais K est un corps de nombres. On note $S = \text{Spec } \mathcal{O}_K$ le spectre de l'anneau des entiers de K. Alors que dans le cas des corps de fonctions, S représente l'ensemble de toutes les places de K, dans le cas des corps de nombres, $S = \text{Spec } \mathcal{O}_K$ ne représente (en oubliant le point générique) que les places finies. Pour pouvoir étendre l'analogie entre corps de nombres et corps de fonctions, il faut aussi prendre en compte les places à l'infini : c'est l'idée de la théorie initiée par Arakelov [7].

Dans la suite, on note S^0 l'ensemble des points fermés de S (*i.e.*, les places finies de $\mathcal{O}_K$), S_∞ l'ensemble des places archimédiennes et $M_K = S_{\text{Ar}} := S^0 \amalg S_\infty$ l'ensemble de toutes les places de K. Pour $v \in S^0$ au dessus d'un nombre premier p, on normalise la valeur absolue v-adique par $\mid p \mid_v = p^{-1}$ et on pose $|| \cdot ||_v = | \cdot |_v^{d_v}$ où d_v est le degré local $[K_v : \mathbb{Q}_p]$. De même si v est une place archimédienne, on prend pour valeur absolue la valeur absolue usuelle et on pose $d_v = 1$ si $K_v = \mathbb{R}$ et $d_v = 2$ si $K_v = \mathbb{C}$.

Définition 9 Un *fibré vectoriel métrisé* de rang r sur $S = \text{Spec } \mathcal{O}_K$ est un $\mathcal{O}_K$-module E projectif (*i.e.*, sans torsion puisque $\mathcal{O}_K$ est de Dedekind) de rang r, muni d'une collection $\{|| \cdot ||_v\}_{v \in S_\infty}$, telle que $|| \cdot ||_v$ est une norme hermitienne sur le K_v-espace vectoriel $E_{K_v} =$

$E \otimes_{\mathcal{O}_K} K_v$, vérifiant

$$|| \, x \, ||_\sigma = || \, \overline{x} \, ||_{\overline{\sigma}}, \quad \text{pour tout plongement } \sigma : K \hookrightarrow \mathbb{C}.$$

On note un tel fibré métrisé $\overline{E} = (E, || \cdot ||_v)$.

Exemples de métriques

Dans ce paragraphe, les variétés X et Y sont des variétés différentielles analytiques complexes. On appliquera ensuite ceci au cas où, partant d'une variété algébrique lisse sur un corps de nombres K, on associe à un plongement $\sigma : K \hookrightarrow \mathbb{C}$ la $\mathbb{C}$-variété algébrique lisse $X_\sigma = X \times_\sigma \mathbb{C}$, puis l'ensemble de ses points complexes $X_\sigma(\mathbb{C})$ qui est naturellement muni d'une structure de variété analytique complexe. Si L est un fibré vectoriel sur une variété analytique X, on dit qu'il *hermitien* s'il est muni d'une métrique hermitienne C^∞ stable par conjugaison complexe.

La métrique image réciproque : soient $f : X \to Y$ un morphisme de variétés analytiques et $\overline{L}$ un fibré en droites sur Y muni d'une métrique hermitienne. On munit le fibré en droites f^*L d'une structure hermitienne en posant, pour tout $x \in X$,

$$|| \, f^* s \, ||_x := || \, s \circ f \, ||_{f(x)} \, .$$

La métrique produit tensoriel : soient $\overline{E}$ et $\overline{F}$ deux fibrés hermitiens sur la variété X. On munit $E \otimes F$ d'une structure hermitienne en posant,

$$\langle e_i \otimes f_i, e_j \otimes f_j \rangle_x := \langle e_i, e_j \rangle_x \cdot \langle f_i, f_j \rangle_x \, .$$

La métrique somme directe : soient $\overline{E}$ et $\overline{F}$ deux fibrés hermitiens sur la variété X. On munit $E \oplus F$ d'une structure hermitienne en posant,

$$\langle e_i \oplus f_i, e_j \oplus f_j \rangle_x := \langle e_i, e_j \rangle_x + \langle f_i, f_j \rangle_x \, .$$

La métrique produit exterieur : soient $\overline{E}$ un fibré hermitien de rang r sur la variété X et $k \leq r$. On munit $\bigwedge_{l=1}^k E$ d'une structure hermitienne en posant,

$$|| \bigwedge_{l=1}^{k} e_l \, ||_x^2 := |\det \left(\langle e_i, e_j \rangle_x \right)| \, ,$$

où $\langle \cdot, \cdot \rangle$ est le produit hermitien définissant la métrique sur $\overline{E}$.

La métrique duale : soit $\overline{E}$ un fibré hermitien sur X. On muni le fibré dual $E^\vee = \mathrm{Hom}(E, \mathbb{C})$ d'une structure hermitienne en posant,

$$|| \, f \, ||_x := \sup_{s \in E} \frac{|| \, f(s) \, ||_x}{|| \, s \, ||_x},$$

où on a muni $\mathbb{C}$ de sa métrique naturelle $|| \, 1 \, ||_x = 1$.

Degré arithmétique

Le *degré d'Arakelov* (ou *degré arithmétique*) d'un fibré en droites métrisé sur Spec $\mathcal{O}_K$ $\overline{L} = (L, ||\cdot||_v)$ est défini en prenant un élément non nul $s \in L$ et en posant

$$\widehat{\deg}_n\ \left(\overline{L}\right) = \frac{1}{[K:\mathbb{Q}]}\left(\log \#\left(L/s\mathcal{O}_K\right) - \sum_{\sigma:K\hookrightarrow\mathbb{C}} \log ||\ s\ ||_\sigma\right),$$

le n en indice signifiant que l'on a normalisé par $[K:\mathbb{Q}]$.

Proposition 1 *Le degré d'Arakelov d'un fibré en droites ne dépend pas du choix de la section s.*

Démonstration : Soient s et t deux sections globales non nulles du fibré en droites L. Il existe un $k \in K^*$ tel que $t = ks$, donc

$$\begin{aligned} -\sum_{v\in S_{\mathrm{Ar}}} \log ||\ t\ ||_v &= -\sum_{v\in S_{\mathrm{Ar}}} \log ||\ ks\ ||_v \\ &= -\sum_{v\in S_{\mathrm{Ar}}} \log ||\ s\ ||_v - \sum_{v\in S_{\mathrm{Ar}}} \log ||\ k\ ||_v \\ &= -\sum_{v\in S_{\mathrm{Ar}}} \log ||\ s\ ||_v \ \text{ par la formule du produit.} \end{aligned}$$

Il reste pour conclure à voir que

$$\log \#\left(L/s\mathcal{O}_K\right) = -\sum_{v\in S^0} \log ||\ s\ ||_v\ .$$

Or on sait par [18] que, si L est un $\mathcal{O}_K$-module projectif de rang 1,

$$\left(L/s\mathcal{O}_K\right) = \prod_{\mathfrak{p}} \left(L/s\mathcal{O}_K\right)_{\mathfrak{p}} = \prod_{\mathfrak{p}} \left(L_{\mathfrak{p}}/s\mathcal{O}_{K_{\mathfrak{p}}}\right).$$

De plus, $L_{\mathfrak{p}}$ est isomorphe isométriquement à $\mathcal{O}_{K_{\mathfrak{p}}}$. On a donc

$$\left(L/s\mathcal{O}_K\right) \simeq \prod_{\mathfrak{p}} \left(\mathcal{O}_{K_{\mathfrak{p}}}/s\mathcal{O}_{K_{\mathfrak{p}}}\right) \simeq \prod_{\mathfrak{p}} \mathcal{O}_K/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(s)}.$$

Ainsi, en passant aux cardinaux,

$$\#\left(L/s\mathcal{O}_K\right) = \prod_{\mathfrak{p}\in S^0} e^{d_{\mathfrak{p}}\,\mathrm{ord}_{\mathfrak{p}}(s)} = \prod_{\mathfrak{p}\in S^0} ||\ s\ ||_{\mathfrak{p}}^{-1}\ .$$

Ceci permet de conclure. □

Remarque 2 Notons au passage que si $s \in L$ est non nulle, on a montré la formule

$$\widehat{\deg}_n\ \left(\overline{L}\right) = \frac{-1}{[K:\mathbb{Q}]} \sum_{v \in S_{\mathrm{Ar}}} \log ||\ s\ ||_v\ .$$

Définition 10 On définit le *degré arithmétique d'un fibré vectoriel F métrisé de rang fini d* en posant :

$$\widehat{\deg}_n\ (\overline{F}) = \widehat{\deg}_n\ \left(\overline{\bigwedge_{k=1}^{d} F} \right).$$

1.2.2 Degré arithmétique : propriétés

Dans tout ce pararaphe, on travaille avec des fibrés vectoriels sur Spec $\mathcal{O}_K$.

Propriétés classiques

Proposition 2 *Soit $\overline{\mathcal{O}_K}$ le fibré trivial muni de sa métrique triviale $||\ 1\ ||_v = 1$. On a $\widehat{\deg}_n\ \overline{\mathcal{O}_K} = 0$.*

Démonstration : Par la remarque 1, si s est une section non nulle de $\mathcal{O}_K$,

$$\widehat{\deg}_n\ \overline{\mathcal{O}_K} = \frac{-1}{[K:\mathbb{Q}]} \sum_{v \in S_{\mathrm{Ar}}} \log ||\ s\ ||_v\ .$$

En appliquant ceci avec $s = 1$ on constate que le membre de droite est nul. □

Proposition 3 *Soient $\overline{E}$ et $\overline{F}$ deux fibrés vectoriels hermitiens de rang respectif m et n et $\overline{L}$ un fibré en droites hermitien de rang 1. On a*

1. $\widehat{\deg}_n\ (\overline{E \otimes F}) = m\widehat{\deg}_n\ \overline{E} + n\widehat{\deg}_n\ \overline{F}$.
2. $\widehat{\deg}_n\ (\overline{E \oplus F}) = \widehat{\deg}_n\ \overline{E} + \widehat{\deg}_n\ \overline{F}$.
3. $\widehat{\deg}_n\ \overline{L^\vee} = -\widehat{\deg}_n\ \overline{L}$.

Démonstration : On commence par montrer 1. dans le cas où $m = n = 1$. Soient $s \in E$, $t \in F$ deux sections telles que $s \otimes t \neq 0$. Pour tout $v \in S_{\mathrm{Ar}}$, on a $||\ s \otimes t\ ||_v = ||\ s\ ||_v ||\ t\ ||_v$. En effet, si $v \in S_\infty$ c'est la définition et si $v \in S^0$, $E_v \otimes F_v$ est isomorphe à $\mathcal{O}_{K_v}$ par l'isomorphisme qui envoie $s \otimes t$ sur $j_v^E(s) j_v^F(t)$. Ainsi

$$||\ s \otimes t\ ||_v = ||\ j_v^E(s) j_v^F(t)\ ||_v = ||\ j_v^E(s)\ ||_v ||\ j_v^F(t)\ ||_v = ||\ s\ ||_v ||\ t\ ||_v\ .$$

En appliquant la remarque p. 31, on conclut dans ce cas. Dans le cas général, on utilise l'isomorphisme isométrique

$$\overline{\bigwedge_{l=1}^{nm} E \otimes F} \simeq \left(\overline{\bigwedge_{l=1}^{n} E} \right)^{\otimes m} \otimes \left(\overline{\bigwedge_{l=1}^{m} F} \right)^{\otimes n}.$$

Le premier cas permet alors de conclure.
2. On applique le 1. en utilisant l'isomorphisme isométrique

$$\bigwedge_{l=1}^{n+m} \overline{E \oplus F} \simeq \bigoplus_{l=1}^{n+m} \left(\bigwedge_{k=1}^{l} \overline{E} \otimes \bigwedge_{k=1}^{n+m-l} \overline{F} \right) \simeq \bigwedge_{l=1}^{n} \overline{E} \otimes \bigwedge_{l=1}^{m} \overline{F}.$$

3. Par définition du faisceau inverse (ou fibré dual) on a $L \otimes L^{\vee} \simeq \mathcal{O}_K$. En munissant $\mathcal{O}_K$ de sa métrique triviale et $L^{\vee}$ de la métrique duale, cet isomorphisme est isométrique. Ainsi, on a $\widehat{\deg}_n\ \left(\overline{L \otimes L^{\vee}}\right) = 0$ par la proposition 2. En appliquant le point 1. on conclut. □

Inégalité des pentes

Définition 11 Soit $\overline{E}$ un $\mathcal{O}_K$-fibré vectoriel, on définit *la pente de* $\overline{E}$ par

$$\widehat{\mu}(\overline{E}) = \frac{\widehat{\deg}_n\ \overline{E}}{\mathrm{rg}E}.$$

Définition 12 Avec les mêmes notations, on définit *la pente maximale de* E par

$$\widehat{\mu}_{\max}(\overline{E}) = \max \widehat{\mu}(\overline{F}),\ \text{où}$$

le max porte sur les sous-$\mathcal{O}_K$-fibrés de E de rang supérieur à 1 et munis des métriques déduites de celle de $\overline{E}$ par restriction.

Définition 13 Si φ est un morphisme entre deux $\mathcal{O}_K$-fibrés hermitiens $\overline{E}$ et $\overline{F}$, on note $h(\varphi)$ et on appelle *hauteur de* φ le nombre

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S_{\mathrm{Ar}}} \log ||\ \varphi\ ||_v,\ \text{où,}$$

$||\ \varphi\ ||_v$ est la norme d'opérateur de φ_{K_p} et $||\ \varphi\ ||_\sigma$ la norme de l'opérateur $\varphi_{\mathbb{C},\sigma}$.

Lemme 1 *Soit $\varphi : E \to F$ un morphisme entre $\mathcal{O}_K$-fibrés hermitiens de rang r. On a,*

$$\forall v \in S_{\mathrm{Ar}},\quad ||\ \bigwedge_{l=1}^{r} \varphi\ ||_v \leq ||\ \varphi\ ||_v^r\ .$$

Démonstration : Soit $v \in S_\infty$. En choisissant des bases orthonormées pour les espaces hermitiens E_{K_v} et F_{K_v}, on identifie φ à une matrice de $M_r(\mathbb{C})$. Par définition de la puissance extérieure, $||\ \bigwedge_{l=1}^{r} \varphi\ ||_v = ||\ \det\ \varphi\ ||_v$. Or le déterminant est le produit des valeurs propres, alors que $||\ \varphi\ ||_v$ est la norme de la plus grande valeur propre. D'où l'inégalité. Dans le cas où $v \in S_0$, cela résulte de l'inégalité ultramétrique. □

Avec les notations précédentes, on a le théorème suivant, dû à J.-B. Bost,

Théorème 17 (Inégalités des pentes 1) *Si le morphisme $\varphi_K : E_K \to F_K$ est injectif, alors,*

$$\widehat{\deg}_n\ \overline{E} \leq \mathrm{rg}(E)\big(\widehat{\mu}_{\max}(\overline{F}) + h(\varphi)\big).$$

Démonstration : Le morphisme φ_K étant injectif on a un isomorphisme

$$\varphi : E_K \to \varphi(E_K).$$

On note F' un sous-$\mathcal{O}_K$-module de F tel que $F'_K = \varphi_K(E_K)$. L'application

$$\bigwedge_{l=1}^{r} \varphi_K : \bigwedge_{l=1}^{r} E_K \to \bigwedge_{l=1}^{r} F'_K$$

est bijective donc non nulle. En particulier elle définit un élément non-nul du K-espace vectoriel de dimension 1 associé au fibré en droites hermitien $\overline{L} := \big(\bigwedge_{l=1}^{r} \overline{E}\big)^{\vee} \otimes \bigwedge_{l=1}^{r} \overline{F'}$. En utilisant la proposition 3, on obtient

$$\begin{aligned}
\widehat{\deg}_n\ \overline{E} - \widehat{\deg}_n\ \overline{F'} &= -\widehat{\deg}_n\ \overline{L} \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S_{\mathrm{Ar}}} \log || \bigwedge_{l=1}^{r} \varphi ||_v \\
&\leq \frac{r}{[K:\mathbb{Q}]} \sum_{v \in S_{\mathrm{Ar}}} \log || \varphi ||_v \qquad \text{par le lemme 1} \\
&= r h(\varphi).
\end{aligned}$$

Par ailleurs, la définition de $\widehat{\mu}_{\max}$ implique que $\widehat{\deg}_n\ \overline{F'} \leq r\widehat{\mu}_{\max}(\overline{F})$. □

En fait, dans la pratique c'est plutôt une version filtrée de cette inégalité qui est utile. On va donc filtrer : soit F_K un K-espace vectoriel de dimension finie muni d'une filtration

$$\{0\} = F_K^{N+1} \subset F_K^N \subset \ldots \subset F_K^0 = F_K$$

par des K-espaces vectoriels. On suppose de plus que les sous-quotients successifs

$$G_K^l = F_K^l / F_K^{l+1}$$

sont les K-espaces vectoriels sous-jacents à certains fibrés vectoriels hermitiens $\overline{G}^l$ sur $\mathrm{Spec}\ \mathcal{O}_K$. Soient par ailleurs $\overline{E}$ un fibré vectoriel hermitien et $\varphi_K : E_K \to F_K$ une application K-linéaire injective. On pose pour tout $l \in [\![0, N+1]\!]$

$$E_K^l = \varphi_K^{-1}(F_K^l), \text{ et } E^l = E \cap E_K^l.$$

Ainsi les sous-$\mathcal{O}_K$-modules E^l de E forment une filtration

$$\{0\} = E^{N+1} \subset E^N \subset \ldots \subset E^0 = E.$$

De plus, munie des métriques de restriction sur $\overline{E}$, cette filtration est une filtration de $\mathcal{O}_K$-modules hermitiens. Enfin, pour tout $l \in [\![0, N]\!]$ on considère les applications

$$\varphi_K^l : E_K^l \to G_K^l \quad \text{et} \quad \widetilde{\varphi}_K^l : E_K^l / E_K^{l+1} \to G_K^l$$

définies par composition de φ_K et de la projection sur G_K^l. On peut maintenant énoncer la version filtrée du théorème précédent.

Théorème 18 (Inégalités des pentes 2) *Avec les notations précédentes, on a,*

$$\widehat{\deg}_n\, \overline{E} \leq \sum_{l=0}^{N} \operatorname{rg}\left(E^l/E^{l+1}\right)\left(\widehat{\mu}_{\max}(\overline{G}^l) + h(\varphi^l)\right).$$

Démonstration : Il suffit d'appliquer la preuve précédente à chaque cran de la filtration et de sommer le tout ensuite. C'est l'inégalité (**4.14**) de la *Proposition* **4.6.** de [16]. □

On donne également une variante que nous utiliserons au chapitre 4.

Théorème 19 *Avec les notations précédentes, on a*

$$\begin{aligned}\widehat{\deg}_n\, \overline{E} \;\leq\; & \textstyle\sum_{l=0}^{N} \operatorname{rg}\left(E^l/E^{l+1}\right)\left(\widehat{\mu}_{\max}(\overline{G^l}) + \sum_{p \text{ premiers}} \log \|\, \varphi^l \,\|_p\right) \\ & + \textstyle\sum_{l=0}^{N} \log \|\, \bigwedge^{max} \widetilde{\varphi}^l \,\|_{\mathbb{C}}\,.\end{aligned}$$

Démonstration : On reprend la preuve précédente et on ne remplace pas les termes $\| \bigwedge^r \varphi^l \|$ par $\| \varphi^l \|^r$ aux places archimédiennes. □

1.3 Hauteur sur les points

1.3.1 Hauteur sur $\mathbb{P}^n(\overline{\mathbb{Q}})$

Soient K un corps de nombres de degré d et M_K l'ensemble des valeurs absolues (deux à deux non équivalentes) sur K, normalisées comme précédemment par $|p|_v = p^{-1}$ pour toute place finie v au dessus du nombre premier p. On note $d_v = [K_v : \mathbb{Q}_p]$ le degré local et on définit la *hauteur (logarithmique absolue)* sur $\mathbb{P}^n(\overline{\mathbb{Q}})$ par

$$h(x_0 : \ldots : x_n) = \frac{1}{d} \sum_{v \in M_K} d_v \log \max_{0 \leq i \leq n} |x_i|_v.$$

On voit sur la définition que la hauteur d'un point est toujours positive ou nulle. Dans cette définition, la renormalisation par $\frac{1}{d}$ sert juste à faire en sorte que le réel $h(x)$ soit indépendant du choix du corps K contenant x. De plus par la formule du produit, la hauteur est aussi indépendante du choix d'un système de coordonnées projectives.

Proposition 4 *Soient $r \in \mathbb{Z}$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et $x \in \mathbb{P}^n(\overline{\mathbb{Q}})$. On a*

$$h(x^r) =\mid r \mid h(x), \quad \text{et,} \quad h(\sigma(x)) = h(x).$$

Cette hauteur vérifie les théorèmes de Northcott et de Kronecker :

Théorème 20 (Northcott) *Soient A et B deux réels. L'ensemble*

$$\left\{ x \in \mathbb{P}^n(\overline{\mathbb{Q}}) \ / \ [\mathbb{Q}(x) : \mathbb{Q}] \leq A, \ \ h(x) \leq B \ \right\}$$

est fini.

Théorème 21 (Kronecker) *Soient $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ non nul et i tel que $x_i \neq 0$. On a l'équivalence*

$$h(x) = 0 \iff \forall j \in [\![1, n]\!] \ \ \frac{x_j}{x_i} \in \mu_\infty \cup \{0\}.$$

1.3.2 Hauteur de Néron-Tate sur les variétés abéliennes

Définition 14 Soient X/K une variété projective et L un fibré très ample sur X. En notant φ_L le plongement de X dans un espace projectif $\mathbb{P}^n$ associé à L (c'est-à-dire tel que $L = \varphi_L^* \mathcal{O}(1)$), on définit la *hauteur* $h_L \ : \ X(\overline{K}) \to \mathbb{R}^+$ par $h_L(P) := h(\varphi_L(P))$, où $h(x_0 : \ldots : x_n)$ est la hauteur logarithmique absolue sur $\mathbb{P}^n(\overline{K})$ définie précédemment.

Dans le cas où $X = A$ est une variété abélienne et où L est de plus symétrique, cette hauteur vérifie un certain nombre de propriétés agréables. Nous indiquons les plus essentielles, qui nous serviront dans la suite. On renvoie par exemple au livre [30] Part B pour tout ce qui concerne les hauteurs.

Proposition 5 *Sur une variété abélienne A/K munie d'un fibré en droites L très ample et symétrique, la hauteur h_L vérifie :*

1. $\forall P \in A(\overline{K}) \qquad h_L([m]P) = m^2 h_L(P) + O(1).$
2. $\forall P, Q \in A(\overline{K}) \qquad h_L(P+Q) + h_L(P-Q) = 2h_L(P) + 2h_L(Q) + O(1).$
3. $\forall h > 0 \ \ \forall d > 0$ l'ensemble $\{P \in A(\overline{K}) / \ h_L(P) \leq h, \ \ \deg(P) \leq d\}$ est fini.

Dans les affirmations précédentes, la constante $O(1)$ dépend de A, L et m, mais pas des points P et Q.

Toujours dans le cas des variétés abéliennes, on peut à partir de cette hauteur en construire une plus jolie : la *hauteur de Néron-Tate*, notée $\widehat{h}_L$. La définition est la suivante :

$$\widehat{h}_L(P) = \lim_{n \to +\infty} \frac{h_L([2^n]P)}{4^n}.$$

Les propriétés classiques de cette hauteur sont résumées dans le théorème suivant.

Théorème 22 (Néron-Tate) *Soient A/K une variété abélienne et L un fibré ample et symétrique sur A. La hauteur canonique est une forme quadratique positive semi-définie sur $A(\overline{K})$, telle que*

1. $\forall P \in A(\overline{K}) \quad \widehat{h}_L(P) = h_L(P) + O(1)$

2. $\widehat{h}_L(P) = 0 \iff P \in A_{\text{tors}}$.

1.4 Hauteur sur les variétés

Il y a essentiellement deux approches de la notion de hauteur d'une variété, toutes deux consistant en une généralisation de la notion de hauteur d'un point. On a d'une part l'approche de Philippon (cf. [38], [39], [40]), consistant comme ce que l'on a fait au début du premier paragraphe, à se ramener au cas d'une sous-variété d'un $\mathbb{P}^n$, puis dans ce cas, à donner une définition élémentaire. D'autre part, il y a l'approche de Bost-Gillet-Soulé [17] fondée sur les travaux de Gillet-Soulé [27] [28], consistant à travailler en parfaite analogie avec le degré en construisant un produit d'intersection arithmétique, puis en voyant la hauteur comme un degré arithmétique (ou degré d'Arakelov). Un théorème de Soulé (th.3 p.366 de [53]) indique que ces deux notions de hauteurs coïncident, à condition de prendre les bonnes conventions pour les places à l'infini dans la définition de Philippon, *i.e.*, en prenant la définition de hauteur qu'il donne dans [40] paragraphe 2.

1.4.1 Définition à la Bost-Gillet-Soulé

Contrairement au cas géométrique où la construction du produit d'intersection sur les diviseurs n'est pas dure, dans le cas arithmétique c'est difficile. On ne va donc pas définir le produit d'intersection arithmétique (même sur les diviseurs). Par contre, on peut donner une définition auto-contenue, suivant [17] proposition 3.2.1., de la hauteur en utilisant une construction par récurrence. C'est ce que l'on fait dans ce qui suit.

Le corps K est toujours un corps de nombres, d'anneau d'entiers $\mathcal{O}_K$. On note $S = \operatorname{Spec} \mathcal{O}_K$ le schéma affine associé. Si X/S est un S-schéma de fibre générique une K-variété, on notera $X(\mathbb{C})$ la variété analytique complexe réunion disjointes des variétés $X_\sigma(\mathbb{C})$ où $X_\sigma(\mathbb{C})$ est la variété (analytique complexe) des points complexes de la variété (algébrique complexe) X_σ déduite de X par extension des scalaires de $\mathcal{O}_K$ à K, puis de K à $\mathbb{C}$ selon le morphisme σ, les σ décrivant l'ensemble des plongements de K dans $\mathbb{C}$.

Définition 15 On dit que X est une *variété arithmétique* sur S si c'est un S-schéma plat quasi-projectif, tel que sa fibre générique X_K soit une K-variété lisse.

Exemple 4 Un schéma abélien, le modèle de Néron d'une variété abélienne, le modèle de Weierstrass d'une courbe elliptique, son modèle minimal sont des exemples de variétés arithmétiques.

Définition 16 On dit que $\overline{L} = (L, h)$ est un *fibré en droites hermitien* si L est un fibré en droites sur X et h une métrique hermitienne C^∞ stable par conjugaison complexe sur le fibré en droites holomorphe $L_{\mathbb{C}}$ canoniquement associé à L sur $X(\mathbb{C})$.

On vérifie immédiatement que ceci généralise la notion de fibré en droites hermitien sur Spec $\mathcal{O}_K$ introduite au paragraphe 1.2.

Définition 17 Soient X une variété arithmétique sur S, $\overline{L}$ un fibré en droites hermitien sur X et Y un sous-schéma fermé, propre sur S. On va définir par récurrence sur la dimension de Y, un nombre réel $h_{\overline{L}}(Y)$ appelé *hauteur de Y relativement à $\overline{L}$* :

- si Y est vertical, *i.e.*, s'il est contenu dans une fibre spéciale de X au dessus d'un idéal premier $\mathfrak{p}$, alors on pose
$$h_{\overline{L}}(Y) = \frac{1}{[K:\mathbb{Q}]} \deg_{L_{\mathbb{F}_\mathfrak{p}}}(Y) \log\left(N_{\mathbb{Q}}^K \mathfrak{p}\right),$$
où $\deg_{L_{\mathbb{F}_\mathfrak{p}}}$ dénote le degré géométrique usuel au dessus de $\mathbb{F}_\mathfrak{p}$ défini au début de ce chapitre.
- si s est une section rationnelle de L dans Y de diviseur $\mathrm{div}(s) = \sum n_\alpha Z_\alpha$, on pose
$$h_{\overline{L}}(Y) = \sum_\alpha n_\alpha h_{\overline{L}}(Z_\alpha) - \frac{1}{[K:\mathbb{Q}]} \int_{Y(\mathbb{C})_{\mathrm{lisse}}} \log \mid\mid s \mid\mid c_1(\overline{L_{\mathbb{C}}})^{\dim Y(\mathbb{C})}.$$
Il reste à définir $c_1(\overline{L})$ quand L est un fibré en droites hermitien holomorphe sur une variété analytique complexe X. On note ∂ et $\overline{\partial}$ les opérateurs différentiels usuels (∂ envoie les (p,q)-formes différentielles sur les $(p+1,q)$-formes et $\overline{\partial}$ envoie les (p,q)-formes sur les $(p,q+1)$-formes). Soit maintenant s une section rationnelle de L dans X, on définit $c_1(\overline{L})$ par
$$c_1(\overline{L}) = \frac{1}{2i\pi} \partial\overline{\partial} \log \mid\mid s \mid\mid^2 .$$

Proposition 6 *Dans le cas où $Y = X = S$, on a $h_{\overline{L}}(S) = \widehat{\deg}_n \overline{L}$, où $\widehat{\deg}_n$ est le degré arithmétique normalisé.*

Démonstration : On applique la définition par récurrence de $h_{\overline{L}}(S)$: soit s une section rationnelle de L dans S, *i.e.*, un élément non nul du $\mathcal{O}_K$-module (des section globales, que l'on note encore L) associé au fibré en droites L. On a $\mathrm{div}(s) = \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(s)[\mathrm{Spec}\,\mathbb{F}_\mathfrak{p}]$. Par ailleurs, $S(\mathbb{C})$ est de dimension zéro : c'est l'ensemble des plongements $\sigma : K \hookrightarrow \mathbb{C}$. Ainsi, on a
$$\int_{Y(\mathbb{C})_{\mathrm{lisse}}} \log \mid\mid s \mid\mid c_1(\overline{L_{\mathbb{C}}})^{\dim Y(\mathbb{C})} = \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log \mid\mid s \mid\mid_\sigma .$$
Enfin, la variété Spec $\mathbb{F}_\mathfrak{p}$ est visiblement un $\mathbb{F}_\mathfrak{p}$-schéma de degré 1 (relativement à L), donc, la définition par récurrence nous donne
$$h_{\overline{L}}(S) = \frac{1}{[K:\mathbb{Q}]} \left(\sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(s) \log p^{d_\mathfrak{p}} - \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log \mid\mid s \mid\mid_\sigma \right),$$

où p est le nombre premier au-dessous de $\mathfrak{p}$ et où $d_\mathfrak{p}$ est le degré de l'extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$. Sous cette forme, on reconnait le degré normalisé de L. □

Dans ce qui suit, on suppose (pour ne pas avoir à écrire partout l'hypothèse Y/S propre) que X/S est projective.

Définition 18 Soient L un fibré en droites hermitien sur la variété arithmétique X et V/K une sous-variété de la fibre générique X_K de X. On définit la *hauteur de V relativement à L*, comme étant la hauteur de l'image schématique[1] $\mathcal{V}$ de V dans X.

Il nous reste maintenant à définir la hauteur d'une variété projective, sans supposer connu aucun modèle : on suppose donc donnée V une K-variété projective sur un corps de nombres. Par définition il existe un fibré en droites très ample L sur V définissant un plongement $\varphi : V \hookrightarrow \mathbb{P}^n_K$ dans un espace projectif. L'espace projectif $\mathbb{P}^n_K$ a un modèle naturel sur S, $\mathbb{P}^n_S$, qui est une variété arithmétique naturellement munie d'un fibré en droites hermitien, le fibré $\mathcal{O}(1)$ muni de la métrique de Fubini-Study définie comme suit : pour toute section $s \in H^0\left(\mathbb{P}^n_\mathbb{C}, \mathcal{O}(1)\right)$ (assimilable à l'espace des polynômes homogènes de degré 1 en $X_0, \ldots, X_n$), on a

$$|| \, s \, || \, (x_0 : \ldots : x_n) = \frac{1}{2} \frac{\mid s(x_0 : \ldots : x_n) \mid}{\sqrt{x_0^2 + \cdots + x_n^2}}.$$

Ceci nous permet de définir la hauteur de V :

Définition 19 Avec les notations précédentes, on appelle *hauteur de V* relativement à L et on note $h_L(V)$ le réel

$$h_L(V) = h_{\overline{\mathcal{O}(1)}}\left(\overline{\varphi(V)}\right),$$

où $\overline{\varphi(V)}$ est l'image schématique dans $\mathbb{P}^n_S$ de $\varphi(V)$.

Remarque 3 Si V est une sous-variété de $\mathbb{P}^n_{\overline{K}}$, alors V admet un modèle Y_F défini sur un corps de nombres F. On peut donc étendre la notion de hauteur aux sous-variétés de $\mathbb{P}^n_{\overline{K}}$. La normalisation par le degré d'un corps de définition, assure comme dans le cas des points que cette définition a bien un sens : si Y'/F' est un autre modèle défini sur un autre corps de nombres, on a $h_L(Y_F) = h_L(Y'_{F'})$.

Exemple 5 Si $x \in \mathbb{P}^n(\overline{\mathbb{Q}})$, en notant $V = \overline{\{x\}}$ l'image schématique de x dans $\mathbb{P}^n$ et en posant $L = \mathcal{O}(1)$, on a

$$\frac{h_L(V)}{\deg_L V} = h_2(x),$$

où h_2 la hauteur sur les points de $\mathbb{P}^n(\overline{\mathbb{Q}})$ définie en utilisant la norme $\mathbf{L}^2$ aux places archimédiennes plutôt que la norme $\mathbf{L}^\infty$ comme au paragraphe 1.3.1.

[1] le plus petit sous-schéma fermé de X contenant $p(V)$. Son espace topologique sous-jacent coïncide avec l'adhérence topologique de $p(V)$.

1.4.2 Hauteur de Faltings d'une variété abélienne

On explique ici ce qu'on appelle dans la littérature la *hauteur de Faltings (stable)* d'une variété abélienne A/K sur un corps de nombres K. Le problème consiste à associer un réel $h_{\mathrm{Falt}}(A)$ qui est défini de manière intrinsèque à partir de A. Notamment on ne veut pas que cette définition dépende d'un quelconque plongement de A dans un espace projectif, mais on veut par contre que cette hauteur vérifie les propriétés usuelles d'une "bonne" hauteur, à savoir on voudrait que

- Pour tout $g \in \mathbb{N}$, il existe $C(g) \in \mathbb{R}$ tel que pour toute variété abélienne de dimension g, définie sur $\overline{\mathbb{Q}}$ on ait
$$h_{\mathrm{Falt}}(A) \geq C(g).$$
- À isomorphisme près, il n'y a qu'un nombre fini de variétés abéliennes de dimension g, de hauteur de Faltings bornée et définies sur un corps de nombres de degré borné.

Un tel objet existe et s'appelle la hauteur de Faltings (stable) de A. Il a été introduit pour la première fois par Faltings [24] dans sa preuve de la conjecture de Mordell sur la finitude du nombre de points rationnels d'une courbe de genre $g \geq 2$.

Construction : soit A une variété abélienne de dimension $g \geq 1$ sur $\overline{\mathbb{Q}}$. Il existe un corps de nombres K sur lequel A est définie et a réduction semi-stable. Soient alors $\pi : \mathcal{A} \to S$ son modèle de Néron, $\varepsilon : S \to \mathcal{A}$ sa section neutre et $\Omega^g_{\mathcal{A}/S}$ le faisceau localement libre de rang 1 des g-formes différentielles. On pose $\omega_{\mathcal{A}/S} = \varepsilon^* \Omega^g_{\mathcal{A}/S}$. C'est un fibré en droites et comme $\mathcal{A}/S$ est un schéma en groupes lisse, on a l'isomorphisme $\omega_{\mathcal{A}/S} \simeq \pi_* \Omega^g_{\mathcal{A}/S}$. S'agissant d'un fibré de rang 1 sur $\operatorname{Spec} \mathcal{O}_K$, on peut l'identifier au module de ses sections globales. Or l'isomorphisme précédent (et la définition de l'image directe π_*) nous indique que ce module n'est autre que $H^0\left(\mathcal{A}, \Omega^g_{\mathcal{A}/S}\right)$. En notant pour tout plongement $\sigma : K \hookrightarrow \mathbb{C}$, $\omega_{\mathcal{A}/S} \otimes_\sigma \mathbb{C}$ le fibré en droites holomorphe associé, on le munit d'une métrique hermitienne par :

$$\forall \alpha \in \omega_{\mathcal{A}/S} \otimes_\sigma \mathbb{C}, \quad || \alpha ||^2_\sigma = \frac{i^{g^2}}{(2\pi)^g} \int_{A_\sigma(\mathbb{C})} \alpha \wedge \overline{\alpha}.$$

On a ainsi fabriqué un fibré en droites hermitien $\overline{\omega}_{\mathcal{A}/S}$ sur S, ne dépendant que de A/S. On pose maintenant

$$h_{\mathrm{Falt}}(A) = \widehat{\deg}_n\left(\overline{\omega}_{\mathcal{A}/S}\right) = h_{\overline{\omega}_{A/S}}(S),$$

la dernière hauteur étant la hauteur de Bost-Gillet-Soulé. Du fait de la normalisation, ceci est indépendant du choix de K (tel que A/K est semi-stable) et on peut montrer que cette hauteur vérifie bien les propriétés voulues. Ceci illustre la souplesse de la notion de hauteur sur les variétés : la hauteur de Faltings n'est rien d'autre que la hauteur de $\operatorname{Spec} \mathcal{O}_K$ pour un fibré en droites hermitien astucieux.

1.4.3 Hauteur de Néron-Tate

Partant d'une variété abélienne sur un corps de nombres K et d'un fibré en droites ample symétrique L, on peut fabriquer une hauteur sur les sous-variétés de A/K et même par la remarque 2 fabriquer une hauteur sur les sous-variétés de $A_{\overline{K}}/\overline{K}$. De même que pour les points, on peut en dimension supérieure, fabriquer à partir de ces données une hauteur plus belle : la hauteur normalisée, ou hauteur canonique (encore appelée hauteur de Néron-Tate). Dans le cas où la variété abélienne A a partout bonne réduction, Moret-Bailly [37] a montré comment faire en utilisant les méthodes précédentes. Par contre le cas général d'une variété abélienne à réduction quelconque ne peut se traiter de la même façon : dans ce cas, on ne peut pas construire la hauteur canonique comme une hauteur à la Bost-Gillet-Soulé. Dans ses travaux sur la conjecture de Bogomolov [60], Zhang a montré comment fabriquer cette hauteur en utilisant un procédé de limite dans l'esprit de celui utilisé par Tate pour fabriquer la hauteur canonique des points. On peut ainsi voir cette hauteur canonique comme une limite de hauteurs arakeloviennes.

La métrique du cube sur une variété abélienne : Soient A/K une variété abélienne de modèle de Néron $\mathcal{A}/\mathcal{O}_K$ et $\mathcal{L}$ un fibré en droites symétrique sur $\mathcal{A}$. Pour tout ensemble $I \subset \{1,2,3\}$ non vide, on note $p_I : \mathcal{A}^3 \to \mathcal{A}$ le morphisme défini sur les points géométriques par

$$p_I(x_1, x_2, x_3) = \sum_{i \in I} x_i.$$

On définit alors le fibré en droites $\mathcal{D}_3(\mathcal{L})$ sur $\mathcal{A}^3$ par

$$\mathcal{D}_3(\mathcal{L}) := \bigotimes_{\substack{I \subset \{1,2,3\} \\ I \neq \emptyset}} p_I^* \mathcal{L}^{\otimes (-1)^{\#I}}.$$

Par le théorème du cube, ce fibré est trivial. On choisit une trivialisation et on munit $\mathcal{D}_3(\mathcal{L})$ de la structure hermitienne induite par cette trivialisation. Si $\mathcal{L}$ est muni d'une structure hermitienne induisant une telle métrique triviale sur $\mathcal{D}_3(\mathcal{L})$, *i.e.*, induisant un isomorphisme isométrique avec le fibré en droites trivial $\overline{\mathcal{O}_{\mathcal{A}^3}}$, on dit que $\mathcal{L}$ est muni d'une *métrique cubiste*.

Cas de bonne réduction : On suppose que $\mathcal{A}/\mathcal{O}_K$ est un schéma abélien. On fixe un isomorphisme φ entre $\mathcal{O}_{\mathcal{A}^3}$ et $\mathcal{D}_3(\mathcal{L})$. On munit pour tout plongement σ le fibré en droites L_σ de la métrique cubiste (qui existe et est unique par un théorème de Moret-Bailly [37]) $|| \cdot ||_\sigma$ associée à φ_σ. Notons qu'un autre choix d'isomorphisme φ aurait multiplié les métriques $|| \cdot ||_\sigma$ par $\mid l \mid_\sigma$ où l est une unité de $\mathcal{O}_K$. Ainsi par la formule du produit, la hauteur associée à $\mathcal{L}$ ne dépend pas du choix de φ. On peut enfin voir que la classe de $\overline{\mathcal{L}}$ ne dépend que de la classe de $L \in \mathrm{Pic}(A)$. On appelle la hauteur ainsi construite, la *hauteur canonique* relativement au fibré en droites L et on la note $\widehat{h}_L(\cdot)$.
Par symétrie de $\mathcal{L}$ on peut trouver un isomorphisme $\psi : [-1]^*\mathcal{L} \to \mathcal{L}$ qui est une isométrie pour tout σ. Ainsi, en utilisant la propriété cubiste, on vérifie facilement que la hauteur

normalisée est quadratique : pour tout cycle $\mathcal{V} \in Z_p(\mathcal{A})$, on a

$$\widehat{h}_L([n]_*\mathcal{V}) = n^{2p}\widehat{h}_L(\mathcal{V}).$$

Cas général : On se donne une variété abélienne A/K, une sous-variété V de A et un fibré en droites symétrique ample L sur A. On se donne alors un modèle $\mathcal{A}/S$ propre et plat, l'image schématique $\mathcal{V}$ de V dans $\mathcal{A}$, un faisceau inversible ample $\mathcal{L}$ sur $\mathcal{A}$ étendant L et pour chaque place σ, une métrique hermitienne (à courbure positive) sur L_σ. On a alors le théorème suivant :

Théorème 23 (Zhang [60]) *la suite* $\frac{1}{4^n}h_{\mathcal{L}}\left([2^n]_*\mathcal{V}\right)$ *converge uniformément vers une limite finie appelée hauteur normalisée de* V *et notée* $\widehat{h}_L(V)$*. Cette limite ne dépend pas des choix de* $\mathcal{A}$*,* $\mathcal{L}$ *ni des métriques choisies. Elle coïncide avec la hauteur de Néron-Tate usuelle sur les points de* $A(K)$*.*

Exemple 6 Si $x \in A(\overline{K})$ et $V = \overline{\{x\}}$ est l'image schématique de x dans A, on a

$$\frac{\widehat{h}_L(V)}{\deg_L V} = \widehat{h}_L(x),$$

où $\widehat{h}_L(x)$ est la hauteur de Néron-Tate usuelle sur les points $\overline{K}$-rationnels de A.

1.4.4 Définition à la Philippon

Soit V/K une variété projective sur un corps de nombres K. On se donne un plongement $\varphi : V \hookrightarrow \mathbb{P}^n$ dans un espace projectif, associé à un fibré en droites ample et symétrique L. On va définir une hauteur sur les sous-variétés de $\mathbb{P}^n$ et on en déduira une hauteur pour V en posant $h_L(V) := h(\varphi(V))$.
L'idée de Philippon est la suivante : si X est une hypersurface de $\mathbb{P}^n$ de degré d, alors X est définie par une équation homogène

$$F_X(\underline{x}) = \sum_{i_0+\ldots+i_n=d} a_{\underline{i}}\underline{x}^{\underline{i}} = 0.$$

De plus, cette équation F_X est déterminée de manière unique, à multiplication par une constante non-nulle près, par X. On peut alors poser $h_\infty(X) := h(F_X) = h(\underline{a})$ où la dernière hauteur est la hauteur projective usuelle du point $\underline{a}$. Ceci étant on peut étendre cette construction d'une hypersurface au cas général d'une sous-variété quelconque de $\mathbb{P}^n$ en utilisant les formes de Cayley-Chow : si X est une sous-variété de degré d et de dimension r de $\mathbb{P}^n$ on peut lui associer une forme multihomogène F_X de multidegré $(d, \cdots, d)$ qui est déterminée par

$$F_X(a_{00}, \ldots, a_{n0}, a_{01}, \ldots, a_{nr}) = 0$$

si et seulement si l'intersection de X avec les $r+1$ hyperplans $\sum_{k=0}^{n} a_{ki}X_k = 0$ pour $0 \leq i \leq r$ est non-vide. La forme F_X s'appelle *la forme de Chow* (ou *forme éliminante*) de X. On pose alors $h_\infty(X) := h(F_X)$.

Cette hauteur, si elle est naturelle et comparable à la hauteur de Bost-Gillet-Soulé, ne coïncide toutefois pas exactement avec cette dernière. Pour cela, Philippon donne dans son article [40] paragraphe 2, la modification adéquate pour définir une hauteur h coïncidant avec celle définie de manière arakelovienne : on conserve la construction précédente, mais on modifie aux places à l'infini la définition de la hauteur projective standard : au lieu de prendre la norme infinie, on prend la norme $\mathbf{L}^2$ et on rajoute de plus le terme constant $\frac{1}{2}(r+1)\deg_L(X)\sum_{j=1}^{n}\frac{1}{j}$.

À partir de là, Philippon définit une hauteur canonique sur les variétés abéliennes. On se donne donc A/K une variété abélienne et L un fibré en droites ample et symétrique (la construction de Philippon se fait en fait sur le fibré projectivement normal $L^{\otimes 4}$ mais on peut oublier ce détail). On veut définir une hauteur canonique associée à ces données. Pour cela l'idée est d'utiliser le procédé limite à la Tate existant pour fabriquer la hauteur canonique des points. On note G_X le stabilisateur de X dans A et on pose

$$\widehat{h}_L(X) = \lim_{n\to\infty} \frac{|\ \ker[n] \cap G_X\ |}{n^{2(\dim X+1)}} h_L([n]X).$$

Là encore, on peut montrer que cette définition a un sens (*i.e.*, la limite existe) et coïncide bien avec celle donnée de façon arakelovienne.

1.5 Résultats et conjecture sur la hauteur canonique

Soient K un corps de nombres, A/K une variété abélienne de dimension g et L un fibré en droites très ample symétrique définissant un plongement de A dans un espace projectif $\mathbb{P}^n$.

1.5.1 Résultats de base

Ces résultats sont montrés dans les propositions et lemmes aboutissant à la proposition 9. de [38].

Proposition 7 *Avec les notations précédentes, on a :*

1. *Il existe une constante $c(A,L)$ telle que pour toute sous-$\overline{K}$-variété X de $A_{\overline{K}}$ on a*

$$|\ \widehat{h}_L(X) - h_L(X)\ | \leq c(A,L)\deg_L(X).$$

2. $\widehat{h}_{L^{\otimes m}}(X) = m^{\dim X+1}\widehat{h}_L(X)$.
3. *Si $\xi \in A\left(\overline{K}\right)_{\text{tors}}$, alors on a, $\widehat{h}_L(X+\xi) = \widehat{h}_L(X)$.*

4. Si $\alpha \in \mathrm{End}(A)$ est tel que $\alpha^* L \sim L^{\otimes q(\alpha)}$, alors

$$\widehat{h}_L(\alpha(X)) = \frac{q(\alpha)^{\dim X+1}}{\mid \ker\, \alpha \cap G_X \mid} \widehat{h}_L(X), \quad et, \ \ \widehat{h}_L(\alpha^{-1}(X)) = q(\alpha)^{\mathrm{codim} X-1} \widehat{h}_L(X).$$

Démonstration : Le point 2. est un résultat vrai pour la hauteur h_L, donc on conclut en passant à la limite. Le point 3. découle facilement de la définition : tout d'abord on a $G_X = G_{(X+\xi)}$ et $\dim X = \dim(X+\xi)$. Ainsi, en notant k l'ordre de ξ, on a, en prenant la sous-suite (kn) de (n),

$$\begin{aligned} \widehat{h}_L(X+\xi) &= \lim_{n\to\infty} \frac{\mid \ker[n] \cap G_X \mid}{n^{2(\dim X+1)}} h_L([n](X+\xi)) \\ &= \lim_{n\to\infty} \frac{\mid \ker[kn] \cap G_X \mid}{(kn)^{2(\dim X+1)}} h_L([kn]X) = \widehat{h}_L(X). \end{aligned}$$

Les points 1. et 4. nécessitent une véritable preuve. le point 1. est démontré dans [38] et le point 4. dans [38] pour $\alpha = [n]$ et dans [19] proposition 2.3. dans le cas général. □

1.5.2 Résultats principaux et conjecture

Soient K un corps de nombres, A/K une variété abélienne et L un fibré en droites symétrique ample sur A. Comme le cas de dimension 0, on peut se demander comment caractériser les sous-variétés de A de hauteur normalisée nulle. On sait depuis les travaux de Zhang [61] et indépendamment David-Philippon [20], caractériser ces variétés :

Théorème 24 (Zhang) *Soit X une sous-variété irréductible de $A_{\overline{K}}$. On a l'équivalence*

$$\widehat{h}_L(X) = 0 \iff \exists \xi \in A(\overline{K})_{\mathrm{tors}},\ \exists B \text{ sous-variété abélienne de } A_{\overline{K}} \text{ tels que } X = B + \xi.$$

Définition 20 Une variété telle que dans le théorème précédent est dite *sous-variété de torsion* de $A_{\overline{K}}$. Si X est une sous-variété irréductible de A/K telle que $X_{\overline{K}}$ est une réunion de sous-variété de torsion, on dit que X est une *sous-variété de torsion* de A.

Par ailleurs, si X est une sous-variété de A, on notera

$$X(\varepsilon) = \left\{ x \in X(\overline{K}) \ / \ \widehat{h}_L(x) \leq \varepsilon \right\}.$$

Le théorème 24 est en fait directement lié à une conjecture de Bogomolov. On peut montrer que les énoncés correspondants aux théorèmes 24 et 25 sont équivalents.

Théorème 25 (Conjecture de Bogomolov) *Soit X une sous-variété irréductible de $A_{\overline{K}}$ qui n'est pas de torsion. Il existe une constante $\varepsilon > 0$ telle que l'ensemble $X(\varepsilon)$ ne soit pas Zariski-dense dans X.*

En fait, la conjecture originelle de Bogomolov se limite au cas où X est une courbe. Sous cette forme, elle a été démontrée par Ullmo [56]. La généralisation en dimension supérieure a alors immédiatement été démontrée par Zhang [61] en adaptant les idées d'Ullmo. La preuve de ce résultat s'appuie de manière cruciale sur un précédent travail de Szpiro-Ullmo-Zhang [54]. Une référence concernant ceci est l'exposé d'Abbes [1] au séminaire Bourbaki. On tire trivialement de ce théorème le résultat suivant, né conjecture de Manin-Mumford et démontré en premier par Raynaud [44] :

Corollaire 2 (Conjecture de Manin-Mumford) *Soit C une courbe irréductible de $A_{\overline{K}}$ qui n'est pas de torsion. Alors, l'ensemble $C \cap A_{\mathrm{tors}}\left(\overline{K}\right)$ des points de $C(\overline{K})$ de torsion dans $A_{\overline{K}}$ est fini.*

Un résultat crucial dans la preuve de la conjecture de Bogomolov est le théorème 26 suivant, dit des minimas successifs, dû à Zhang [60] dans une version bien plus précise.

Définition 21 Soient X une sous-variété de A sur K et θ un nombre réel positif. On pose $X(\theta, L) = \left\{ x \in X(\overline{K}) \ / \ \widehat{h}_L(x) \leq \theta \right\}$. On définit alors le *minimum essentiel* de X et on note $\hat{\mu}_L^{\mathrm{ess}}(X)$ le réel

$$\hat{\mu}_L^{\mathrm{ess}}(X) = \inf \left\{ \theta > 0 \ / \ \overline{X(\theta, L)} = X \ \right\}$$

où $\overline{X(\theta, L)}$ est l'adhérence de Zariski de $X(\theta, L)$ dans A.

Théorème 26 (Zhang) *Si X est une sous-variété de A/K, alors,*

$$\frac{\widehat{h}_L(X)}{(\dim X + 1)\deg_L X} \leq \hat{\mu}_L^{ess}(X) \leq \frac{\widehat{h}_L(X)}{\deg_L X}.$$

Au vu du théorème 24, qui est l'analogue pour les variétés abéliennes et en dimension supérieure du théorème 21 de Kronecker, on peut se demander ce qu'il en est des variétés qui ne sont pas des variétés de torsion : existe-t-il un énoncé, même conjectural, donnant une minoration de la hauteur de telles variétés et généralisant en dimension supérieure le problème de Lehmer abélien ? Comme annoncé dans l'introduction, une telle conjecture existe effectivement :

Conjecture 10 (David-Philippon) *Soient A/K une variété abélienne munie d'un fibré en droites ample et symétrique L. Si X est une sous-variété stricte de A sur K, K-irréductible et qui n'est pas de torsion, alors on a l'inégalité*

$$\frac{\widehat{h}_L(X)}{\deg_L(X)} \geq c(A, L) \deg_L(X)^{-\frac{1}{s - \dim X}},$$

où s est la dimension du plus petit sous-groupe algébrique contenant X.

Les chapitres 2 et 3 de cette thèse sont consacrés à l'obtention de résultats en direction de cette conjecture dans le cas des variétés abéliennes de type C.M.

Chapitre 2

Densité de points et minoration de hauteur

Il s'agit, à quelque modifications de notations près, de l'article [42] paru au *Journal of number theory*.

2.1 Introduction

On sait depuis les travaux de Philippon [38] [39] [40], puis Bost, Gillet et Soulé [17] dans le cadre de l'intersection arithmétique, comment définir la hauteur des variétés projectives ; l'idée étant de considérer un point comme une variété de dimension zéro et de généraliser ceci en dimension supérieure. De même que dans le cas des points, on sait pour les variétés abéliennes munies d'un fibré en droites ample et symétrique définir une hauteur particulierement agréable : la hauteur canonique $\widehat{h}_L$, ou hauteur normalisée. En dimension zéro, il existe un théorème caractérisant les points de hauteur normalisée nulle ; c'est un résultat de Kronecker dans le cas de $\mathbb{G}_m$. Philippon [40] (dans le cas d'un produit de courbes elliptiques) puis Zhang [60] et David-Philippon [20] dans le cas général ont montré comment généraliser ce résultat pour caractériser les sous-variétés de hauteur normalisée nulle : ce sont les translatées d'un sous-groupe algébrique par un point de torsion. On dit qu'une telle sous-variété est une sous-variété de torsion. La réponse à cette question résoud une conjecture de Bogomolov qui, dans sa formulation initiale a été démontrée en premier par Ullmo [56]. Ceci étant, on peut se demander comment minorer la hauteur normalisée d'une sous-variété de hauteur non-nulle d'une variété abélienne. Dans leur article [20], David et Philippon ont formulé un problème général (le problème 1.7) contenant cette question. On peut notamment faire ressortir de la discussion suivant la formulation de leur problème l'énoncé suivant :

Conjecture 11 (David-Philippon) *Soit A une variété abélienne définie sur un corps de nombres k, munie d'un fibré ample et symétrique L. Soit V une sous-variété stricte de*

A sur k, k-irréductible et telle que $V_{\overline{k}}$ n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité

$$\frac{\widehat{h}_L(V)}{\deg_L(V)} \geq c(A,L)\deg_L(V)^{-\frac{1}{s-\dim V}},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V, et où $c(A,L)$ est une constante ne dépendant que de A et de L.

Dans ce qui suit, on reprend le résultat principal (ainsi que le schéma de démonstration) de Amoroso-David [4] concernant le groupe multiplicatif $\mathbb{G}_m^n$, pour obtenir un résultat analogue dans le cadre des variétés abéliennes. En utilisant les résultats de David-Hindry [19] concernant le problème de Lehmer abélien, on obtient en corollaire un résultat en direction de la conjecture 11. Ce dernier ne concerne que les variétés abéliennes de type C.M., par contre il est essentiellement optimal (à un facteur log près) en le degré de V.

Remerciements Je tiens à remercier M. Hindry pour sa patiente relecture, et je le remercie également, ainsi que S. David, pour m'avoir encouragé à écrire cet article. Par ailleurs je souhaite aussi remercier chaleureusement É. Gaudron et G. Rémond pour m'avoir indiqué une erreur dans la preuve du lemme 4 dans une version préliminaire de cet article.

2.1.1 Degré et hauteur

Soit k un corps de nombres. On dira que V est une *variété algébrique* sur k si V est un k-schéma de type fini géométriquement réduit. On dira que G est un *groupe algébrique* sur k si c'est une variété en groupes sur k. On dira que A est une *variété abélienne* définie sur k si c'est un groupe algébrique connexe propre et lisse sur k. Par sous-variété on entendra toujours sous-variété fermée.

Soient $\mathcal{O}_k$ l'anneau des entiers de k, n un entier, et X une variété projective munie d'un plongement $\varphi_L : X \hookrightarrow \mathbb{P}_k^n$ défini par un fibré L très ample sur X. Si $\mathcal{O}(1)$ dénote le fibré standard sur $\mathbb{P}^n_{\mathcal{O}_k}$, on a $\varphi_L^*\mathcal{O}(1)_k \simeq L$. On note $\overline{\mathcal{O}(1)}$ le fibré standard muni de la métrique de Fubini-Study. Si V est une sous-variété de X, on note $\mathcal{V}_L$ l'adhérence schématique de $\varphi_L(V)$ dans $\mathbb{P}^n_{\mathcal{O}_k}$.

Définition 22 On définit le *degré de la variété V* relativement à L, et on note $\deg_L V$ l'entier $\deg_k\left(c_1(\mathcal{O}(1)_k)^{\dim V}\cdot\varphi_L(V)\right)$ où $\deg_k$ est le degré projectif usuel sur $\mathbb{P}_k^n$.

Définition 23 On appelle *hauteur de la variété V* associée à L, et on note $h_L(V)$ la hauteur de $\mathcal{V}_L$, au sens de Bost-Gillet-Soulé [17] p. 945 définition 3.1.1., associée au fibré hermitien $\overline{\mathcal{O}(1)}$. Notons que l'on ne normalise pas cette hauteur par le degré $\deg_L(V)$.

Remarque 4 Par le théorème 3 p. 366 de [53], $h_L(V)$ coincide avec la hauteur $h(f_{V,L})$ de Philippon, telle que définie au paragraphe 2. de [40], où $f_{V,L}$ est une forme éliminante de l'idéal de définition de $\varphi_L(V)$ dans $k[X_0,\ldots,X_n]$. (Le terme d'erreur de [53] disparait du

fait du changement de normalisation pour la hauteur de Philippon entre les articles [38] et [40]).

Définition 24 Dans le cas où $X = A$ est une variété abélienne, et où L est en plus symétrique, Philippon [40] (dans le cas où L définit un plongement projectivement normal) puis Zhang [60], avec des méthodes arakeloviennes, ont montré en utilisant un procédé de limite à la Néron-Tate, comment définir une *hauteur canonique*, notée $\widehat{h}_L(.)$, sur l'ensemble des sous-variétés de A. Cette hauteur vérifie notamment : si V est une sous-variété de A, de stabilisateur G_V, et si n est un entier, alors,

$$\widehat{h}_L\left([n](V)\right) = \frac{n^{2(\dim V+1)}}{\mid \ker\, [n] \cap G_V \mid} \widehat{h}_L(V).$$

Définition 25 Soient A/k une variété abélienne et V une variété sur k géométriquement irréductible. On dit qu'une sous variété V de A/k est une *sous-variété de torsion* de A si $V_{\overline{k}} = a + B$ avec $a \in A_{\text{tors}}$ et B une sous-variété abélienne de $A_{\overline{k}}$. On dit que c'est une *sous-variété de torsion stricte* de A si $V_{\overline{k}}$ est une sous-variété de torsion $a + B$ avec B une sous-variété abélienne stricte de $A_{\overline{k}}$.

D'après les résultats de Philippon [40], David-Philippon [20] et Zhang [60], on a, si V est une sous-variété de $A_{\overline{k}}/\overline{k}$ géométriquement irréductible,

$$\widehat{h}_L(V) = 0 \text{ si et seulement si } V \text{ est une sous-variété de torsion.}$$

Définition 26 Soient V une sous-variété de A sur k, et θ un nombre réel positif. On pose $V(\theta, L) = \left\{ x \in V(\overline{k}) \ / \ \widehat{h}_L(x) \leq \theta \right\}$. On définit alors le *minimum essentiel* de V, et on note $\mu_L^{\text{ess}}(V)$ le réel

$$\mu_L^{\text{ess}}(V) = \inf \left\{ \theta > 0 \ / \ \overline{V(\theta, L)} = V \ \right\},$$

où $\overline{V(\theta, L)}$ est l'adhérence de Zariski de $V(\theta, L)$ dans A.

2.1.2 Résultats

Soient k un corps de nombres, A/k une variété abélienne de dimension g, et L un fibré en droites très ample sur A. On démontre le théorème suivant :

Théorème 27 *Soient K/k une extension finie, et V une sous-variété algébrique de A_K sur K, K-irréductible telle que $V_{\overline{k}}$ n'est contenue dans aucune réunion de sous-variétés de torsion strictes de $A_{\overline{k}}$. Alors, pour tout réel $\varepsilon > 0$, l'ensemble des points $x \in V(\overline{K})$ d'ordre infini modulo toute sous-variété abélienne stricte de A_K, et dont la hauteur de Néron-Tate relativement à L vérifie*

$$\widehat{h}_L(x) \leq \frac{\widehat{h}_L(V)}{\deg_L V} + \varepsilon$$

est Zariski dense dans V.

On peut donner deux corollaires à ce théorème. Pour cela, on a besoin d'une définition.

Définition 27 Soient A une variété abélienne définie sur un corps de nombres k, L un fibré en droites ample symétrique, et $x \in A(\overline{k})$. Suivant [19] définition 1.2., on appelle *indice d'obstruction de* x, et on note $\delta_L(x)$ la quantité

$$\delta_L(x) = \min\left\{\deg_L X^{\frac{1}{\operatorname{codim} X}} \quad / \quad x \in X(\overline{k})\right\},$$

où le minimum est pris sur l'ensemble des sous-variétés strictes, X, de A sur k, k-irréductibles.

On peut voir le point $x \in A(\overline{k})$ comme une sous-variété de A, définie sur k, k-irréductible, de dimension 0 et de degré $[k(x) : k]$. Avec cette interprétation, la définition précédente admet la généralisation suivante : si V est une sous-variété stricte de A sur k, k-irréductible, on appelle *indice d'obstruction de* V, et on note $\delta_L(V)$ la quantité

$$\delta_L(V) = \min\left\{\deg_L X^{\frac{1}{\operatorname{codim} X}} \quad / \quad V \subset X\right\},$$

où le minimum est pris sur l'ensemble des sous-variétés strictes, X, de A sur k, k-irréductibles.

Remarque 5 On a par définition, $1 \leq \delta_L(V) \leq \deg_L(V)^{\frac{1}{\operatorname{codim} V}}$. Dans le cas où V est de dimension 0, on retrouve ainsi le lemme 1.3. de [19].

En utilisant le résultat de [19] concernant le problème de Lehmer pour les variétés abéliennes de type C.M., on peut alors montrer le résultat suivant :

Corollaire 3 *Supposons de plus que A est de type C.M. Soit V une sous-variété algébrique stricte de A sur k, k-irréductible et telle que $V_{\overline{k}}$ n'est contenue dans aucune réunion de sous-variétés de torsion strictes de $A_{\overline{k}}$. Alors, l'ensemble*

$$\left\{x \in V(\overline{k}) \quad / \quad \widehat{h}_L(x) \leq \frac{c(A,L)}{\delta_L(V)}\left(\frac{\log\log(3\delta_L(V))}{\log(2\delta_L(V))}\right)^{\kappa(g)}\right\},$$

n'est pas Zariski dense dans V. Ici $c(A, L)$ est une constante ne dépendant que de A et de L, et $\kappa(g)$ est une constante effectivement calculable ne dépendant que de g (par exemple $\kappa(g) = (2g(g+1)!)^{g+2}$ convient).

Remarque 6 Ce corollaire est une conséquence formelle du théorème 27 et du théorème principal de [19]. En particulier, toute amélioration dans la direction de la conjecture de Lehmer abélienne, améliore d'autant le corollaire. Le meilleur résultat possible correspondrait au cas où A/k est une variété abélienne quelconque, et où l'on peut prendre $\kappa(g) = 0$, i.e., à la conjecture de Lehmer abélienne telle que énoncée dans [19].

Dans ce qui suit, si A est une variété abélienne, on suppose donné avec A une isogénie avec un produit de variétés abéliennes simples $\prod A_i^{n_i}$. On suppose de plus que la variété produit est munie du fibré associé au plongement

$$A = \prod_{i=1}^{n} A_i^{r_i} \hookrightarrow \prod_{i=1}^{n} \mathbb{P}_{n_i}^{r_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^N,$$

les A_i étant plongées dans $\mathbb{P}_{n_i}$ par des fibrés L_i amples et symétriques. Si L est un fibré en droites symétrique ample sur A, on notera par $c(A, L)$ une constante ne faisant intervenir que ces données.

Corollaire 4 *Si A est de type C.M., L un fibré en droites ample et symétrique de A, et si V est une sous-variété algébrique stricte de A sur k, k-irréductible et telle que $V_{\overline{k}}$ n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité*

$$\frac{\widehat{h}_L(V)}{\deg_L(V)} \geq \mu_L^{\text{ess}}(V) \geq c(A, L) \deg_L(V)^{-\frac{1}{s-\dim V}} \left(\log(2 \deg_L(V))\right)^{-\kappa(s)},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V.

Remarque 7 Soit $P \in A(\overline{k})$. En notant V la sous-variété de A sur k obtenue à partir de P en rajoutant tous ses conjugués (plus exactement en prenant l'image schématique de P dans A), on constate que le résultat obtenu est bien une généralisation d'un énoncé du type Lehmer : il s'agit d'un énoncé de nature arithmétique faisant intervenir le degré d'un corps de définition de V.

Remarque 8 En fait, il suit des preuves des corollaires 3 et 4 le résultat suivant :

soient A/k une variété abélienne de dimension g, L un fibré en droites symétrique ample sur A. On appelle Lehmer$(A/k, L, \gamma)$ la propriété suivante : il existe des constantes $c(A, L)$ ne dépendant que de A et de L, et $\gamma(g)$ ne dépendant que de g, telles que pour tout point $x \in A(\overline{k})$ qui est d'ordre infini modulo toute sous-variété abélienne stricte de A, on a

$$\widehat{h}_L(x) \geq c(A, L)\delta(x)^{-\gamma(g)}.$$

On note ensuite Minorant$(A/k, L, V, \gamma)$ l'énoncé : il existe des constantes strictement positives $c'(A, L)$ ne dépendant que de A et de L, et $\gamma(g)$ ne dépendant que de g, telles que si V est une sous-variété algébrique stricte de A sur k, k-irréductible et telle que $V_{\overline{k}}$ n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité

$$\frac{\widehat{h}_L(V)}{\deg_L(V)} \geq c'(A, L) \deg_L(V)^{-\frac{\gamma(g)}{s-\dim V}},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V.

Avec ces notations, on a

$$\text{Lehmer}(A/k, L, \gamma) \Rightarrow \text{ Minorant}(A/k, L, V, \gamma).$$

De plus, et avec les notations de la remarque précédente 8, on trouve dans [19] la conjecture suivante concernant le problème de Lehmer abélien :

Conjecture 12 (David-Hindry) *L'assertion* $\text{Lehmer}(A/k, L, 1)$ *est vraie pour toute variété abélienne* A/k.

En utilisant la remarque, on en déduit qu'une bonne minoration de la hauteur sur les points entraîne une bonne minoration de la hauteur sur toutes les sous-variétés. Plus précisément, on a :

Corollaire 5 *La conjecture 12 implique la conjecture 11.*

La suite est consacrée à une démonstration du théorème 27 et de ces corollaires.

2.2 La proposition clé

Proposition 8 (Amoroso-David) *Soient n un entier et X une sous-variété de $\mathbb{P}^n$ sur k, k-irréductible. Pour tout $\varepsilon > 0$, il existe $\delta_0 = \delta_0(\varepsilon, X) > 0$ vérifiant les propriétés suivantes :*

soient δ un entier supérieur à δ_0, et Y une sous-variété de $\mathbb{P}^n$ sur k ne contenant pas X. Si

$$\log \deg_k(Y) \leq \frac{\delta\varepsilon}{4\dim X},$$

alors il existe $x \in (X \setminus Y)(\overline{k})$ tel que

$$h_{\mathcal{O}(1)}(x) \leq \frac{h_{\mathcal{O}(1)}(X)}{\deg_k(X)} + \varepsilon \quad \text{et} \quad [k(x) : k] \leq (\deg_k(X))\delta^{\dim X}.$$

Démonstration : C'est la proposition 2.1. de [4] : cette dernière est simplement énoncée avec Y une hypersurface, mais la preuve dans le cas général reste mot pour mot la même. □

En utilisant un procédé de limite, on en déduit :

Corollaire 6 *Soit V une sous-variété de A sur k, k-irréductible. Pour tout $\varepsilon_1 > 0$, il existe $\delta_1 = \delta_1(\varepsilon_1, V, A, L) > 0$ vérifiant les propriétés suivantes :*

soient δ un entier supérieur à δ_1, et W une sous-variété de A sur k ne contenant pas V. Si

$$\log \deg_L W \leq \frac{\delta}{4\dim V},$$

alors il existe $x \in (V \setminus W)(\overline{k})$ tel que

$$\widehat{h}_L(x) \leq \frac{\widehat{h}_L(V)}{\deg_L V} + \varepsilon_1 \quad \text{et} \quad [k(x) : k] \leq c_0(\varepsilon_1, A, L)(\deg_L V)\delta^{\dim V},$$

où $c_0(\varepsilon_1, A, L)$ est une constante strictement positive ne dépendant que de ε_1, A et L.

Démonstration : Quitte à remplacer L par $L^{\otimes 4}$, on suppose que le plongement $\varphi : A \hookrightarrow \mathbb{P}^n$ associé au fibré en droites très ample symétrique L, est projectivement normal. Soit p un nombre premier et N un entier strictement positif. On considère le plongement projectif $\psi = \psi_{p,L}$ de A, composé des plongements suivants

$$\begin{array}{ccccccc} A & \hookrightarrow & A^N & \hookrightarrow & (\mathbb{P}^n)^N & \underset{\text{Segre}}{\hookrightarrow} & \mathbb{P}^{(n+1)^N-1} \\ x & \mapsto & (x, [p]x, \ldots, [p^{N-1}]x) & & & & \end{array}$$

Il s'agit du *plongement enroulé* défini dans [40] paragraphe 3. En notant h_ψ la hauteur associée à ce plongement, la proposition 7. de [40] nous dit que

$$\deg_\psi(V) = \left(\frac{p^{2N}-1}{p^2-1}\right)^{\dim V} \deg_L(V), \quad \text{et} \quad \widehat{h}_\psi(V) = \left(\frac{p^{2N}-1}{p^2-1}\right)^{\dim V} \widehat{h}_L(V).$$

Ainsi, en appliquant la proposition 9. de [40], on en déduit qu'il existe un réel $c_p > 0$ indépendant de N, tel que

$$\left| \left(\frac{p^{2N}-1}{p^2-1}\right) \frac{\widehat{h}_L(V)}{\deg_L(V)} - \frac{h_{\mathcal{O}(1)}(\psi(V))}{\deg_k(\psi(V))} \right| \leq 8c_pN. \tag{2.1}$$

Soit maintenant $\varepsilon_1 > 0$. On fixe $p = 3$ par exemple, et on choisit $N = N(\varepsilon_1, A, L)$ le plus petit entier tel que

$$\frac{16c_pN + 1}{\left(\frac{p^{2N-1}}{p^2-1}\right)} \leq \varepsilon_1.$$

On va appliquer la proposition précédente 8 avec $\varepsilon = 1$, $X = \varphi(V)$ et $Y = \varphi(W)$. On choisit $\delta \geq \delta_1(\varepsilon_1, V, A, L) = \max\{8(\dim V)^2 N \log p,\ \delta_0(1, X)\}$, et on suppose que

$$\log \deg_L(W) \leq \frac{\delta}{4\dim X}.$$

Avec ces choix, on a

$$\begin{aligned}\log \deg_k Y &= \dim V \log\left(\frac{p^{2N}-1}{p^2-1}\right) + \log \deg_L W \\ &\leq 2N \dim V \log p + \log \deg_L W \\ &\leq 2N \dim V \log p + \frac{\delta}{4\dim V} \leq \frac{\delta}{2\dim V} \quad \text{par choix de } \delta_1.\end{aligned}$$

La proposition 8 nous dit qu'il existe $y \in (\varphi(V) \setminus \varphi(W))(\overline{k})$ tel que :

$$h_{\mathcal{O}(1)}(y) \leq \frac{h_{\mathcal{O}(1)}(X)}{\deg_k(X)} + 1 \leq 8c_p N + \frac{p^{2N}-1}{p^2-1}\frac{\widehat{h}_L(V)}{\deg_L(V)} + 1,$$

et tel que

$$[k(y):k] \leq \deg_k(X)\delta^{\dim V} \leq \left(\frac{p^{2N}-1}{p^2-1}\right)^{\dim V} \deg_L(V)\delta^{\dim V}.$$

Par définition, il existe $x \in V \setminus W$ tel que

$$y = \varphi(x), \text{ et tel que } \mid h_{\mathcal{O}(1)}(y) - \frac{p^{2N}-1}{p^2-1}\widehat{h}_L(x) \mid \leq 8c_p N.$$

On en déduit

$$\widehat{h}_L(x) \leq \frac{\widehat{h}_L(V)}{\deg_L V} + \frac{16c_p N + 1}{\left(\frac{p^{2N}-1}{p^2-1}\right)}, \text{ et } [k(x):k] \leq \left(\frac{p^{2N}-1}{p^2-1}\right)^{2\dim V} \delta^{\dim V} \deg_L V.$$

Le choix de N permet de conclure. □

2.3 Un lemme de majoration

Dans ce qui suit, A/k est une variété abélienne définie sur un corps de nombres k, et L est un fibré en droites symétrique très ample sur A. On suppose k plongé dans $\mathbb{C}$. On commence par rappeler un résultat classique concernant le corps de définition d'une sous-variété abélienne de $A_{\overline{k}}$.

Lemme 2 *Il existe une extension F/k finie, ne dépendant que de A, et notamment de degré majoré par une constante ne dépendant que de A, telle que toute sous-variété abélienne B de $A_{\overline{k}}$ soit définie sur F, i.e., il existe une sous-variété abélienne B_0 de A_F telle que $B_0 \times_F \overline{k} \simeq B$.*

Démonstration : Le groupe $\mathrm{End}_{\overline{k}}(A_{\overline{k}})$ est un $\mathbb{Z}$-module de type fini. Il existe donc une extension finie F/k ne dépendant que de A telle que $\mathrm{End}_{\overline{k}}(A_{\overline{k}}) = \mathrm{End}_F(A_F)$. Soit maintenant B une sous-variété abélienne de $A_{\overline{k}}$. Par le théorème d'irréductibilité de Poincaré, il

existe une sous-variété abélienne C de $A_{\overline{k}}$ et une isogénie $\varphi : A_{\overline{k}} \to B \times C$. En notant pr_1 la projection de $B \times C$ sur B, et i l'inclusion de B dans $A_{\overline{k}}$, on a : $f = i \circ pr_1 \circ \varphi \in \mathrm{End}_F(A_F)$. Or $B = f_{\overline{k}}(A_{\overline{k}}) = f_{\overline{k}}(A_F \times_F \overline{k}) \simeq f(A_F) \times_F \overline{k}$, donc en prenant $B_0 = f(A_F)$, on voit que B est définie sur F. □

Remarque 9 En fait on peut prendre F/k de degré inférieur à $3^{16\dim A^4}$ (cf. [36] lemma 2.2.).

Au vu de ce lemme, on supposera dans toute la suite que toutes les sous-variétés abéliennes de $A_{\overline{k}}/\overline{k}$ sont définies sur k.

Lemme 3 *Soient d un entier, et $x \in A$ un point rationnel sur une extension de degré inférieur à d. Si x est un point de torsion modulo une sous-variété abélienne stricte B de A, alors on peut écrire $x = y + \xi$ avec $y \in B$ et $\xi \in A(F)_{\mathrm{tors}}$ où F est une extension de degré inférieur à $c_1(A)d$, $c_1(A)$ étant une constante ne dépendant que de A.*

Démonstration : On note $\pi : A \to A/B = C$. On sait (cf. [11]) que l'on peut construire une sous-variété abélienne C' de A telle que $A = B + C'$, et telle que $\mathrm{Card}\,(B \cap C') \leq c_1(A)$ pour une constante $c_1(A)$ ne dépendant que de A. Notons $\pi' = \pi_{|C'}$ l'isogénie de C' vers C, et posons $K = k(x)$. On peut écrire $x = b + c'$ avec $b \in B$ et $c' \in C'$. On a $\pi(x) = \pi'(c') \in C(K)_{\mathrm{tors}}$. L'application π' étant une isogénie, le point c' est de torsion, et il est rationnel sur une extension de K de degré majoré par $c_1(A)$. □

Lemme 4 *Soient d un entier, et $x \in A$ un point rationnel sur une extension de degré inférieur à d. Si x est de torsion modulo une sous-variété abélienne stricte B de A, alors, il existe une sous-variété abélienne B_x stricte de A et un point de torsion ξ défini sur une extension de degré au plus $c_1(A)d$ de k, tels que $x \in (B_x + \xi)$, et tels que*

$$\deg_L B_x \leq c_2(A, L) d^{c_3(A)} \max\{1, \hat{h}_L(x)\}^{c_4(A)}, \quad \text{où}$$

c_2 ne dépend que de A de L, et où c_3, c_4 sont des constantes ne dépendant que de A.

Démonstration : On note G_x le plus petit sous-groupe algébrique contenant x, et on note $B_x = G_x^0$ sa composante neutre. Par hypothèse sur x, la sous-variété abélienne B_x est strictement incluse dans A, et x est de torsion modulo B_x. Ainsi, le lemme 3 entraîne que $x \in (B_x + \xi)$ avec ξ point de torsion défini sur une extension de degré au plus $c_1(A)d$ de k. Il reste à voir que le degré de B_x est majoré comme on veut. On va pour cela utiliser l'article [10] de Bertrand. En suivant les notations de cet article, on note $\mathcal{H}(A)$ l'ensemble des classes d'isomorphismes de sous-variétés abéliennes de A. La proposition 1.(ii) de [10] nous assure que cet ensemble est fini. De plus, si K/k est une extension de degré d telle que le point x est K-rationnel, en utilisant le theorem p. 154 de [35], on note que le cardinal de $A(K)_{\mathrm{tors}}$ est majoré par $c_8'(A)d^{7\dim A}$. Il en va donc de même du cardinal de $Y(K)_{\mathrm{tors}}$ pour toute sous-variété abélienne Y de A. Par le lemme 2, pour toute

sous-variété abélienne Y de A, le cardinal du sous-groupe de torsion de $(A/Y)(K)$ divise une quantité majorée par $c'_9(A)d^{c'_{10}(A)}$. Avec les notations de [10] poroposition 1. (i), on peut donc prendre $\nu(A/K) \leq c'_9(A)d^{c'_{10}(A)}$. En appliquant maintenant le Corollary p.239 et la remark 2. (i) p.231 de [10], et avec ses notations, on obtient la majoration

$$\deg_L B_x \leq c(A,K)^{-1} c''_9(A,L) d^{c'_{11}(A)} \max\{1, \hat{h}_L(x)\}^g.$$

Il nous suffit maintenant de montrer que $c(A,K) \geq c''_{11}(A,L)d^{-c''_{10}(A)}$. L'ensemble $\mathcal{H}(A,K) = \mathcal{H}(A,k)$ de classes de K-isomorphismes de sous-variétés abéliennes de A est fini (et ne dépend que de A et k par le lemme 2) :

$$\mathcal{H}(A,k) = \left\{B_1, \ldots, B_{n(A)}\right\}.$$

On note b_i le degré de la polarisation sur B_i déduite de (A,L). On pose $c'_{12}(A,L) = \min b_i > 0$. La remarque suivant le corollary p.239 de [10] nous indique alors (en mettant dans une même constante $c_2(A,L)$ la dépendance en $h_{\mathrm{Falt}}(A)$ et en $c'_{12}(A,L)$) que

$$c(A,K) \geq c''_{11}(A,L)d^{-c''_{10}(A)}.$$

□

Remarque 10 La preuve de ce lemme nous permet même de spécifier B_x : on peut prendre pour B_x la composante neutre du plus petit sous-groupe algébrique contenant le point x.

Remarque 11 Dans son article [45], Rémond obtient une version plus fine de ce lemme 4.

Soit D un entier. On définit une sous-variété de A sur k, notée $Y(D,d)$, par :

$$Y(D,d) = \bigcup_B \left(\bigcup_\xi (B + \xi) \right),$$

où B décrit l'ensemble $\mathcal{E}_L(D)$ des sous-variétés abéliennes strictes de A de degré (relativement à L) inférieur à D, et ξ décrit l'ensemble des points de torsion de A définis sur une extension de degré au plus $c_1(A)d$ de k.

Lemme 5 *Il existe une constante $c_5(A,L)$ telle que*

$$\mathrm{Card}\ \mathcal{E}_L(D) \leq c_5(A,L) D^{(2\dim A)^2}.$$

Démonstration : Le fibré L est très ample, donc il définit une forme de Riemann H_L sur $t_{A(\mathbb{C})}$, telle que la forme symplectique $E_L = \mathrm{Im} H_L$, est à valeurs entières sur le réseau des périodes $\Omega_{A(\mathbb{C})}$. En utilisant essentiellement le théorème de Riemann-Roch pour les variétés abéliennes, la proposition 3 p.269 de [12] nous indique que, si B est une sous-variété abélienne de A, alors

$$\deg_L B = (\dim B)! \mathrm{Vol}_{E_L} \Omega_{B(\mathbb{C})},$$

où le volume est relatif à la norme $||\cdot||$ induite par la forme bilinéaire symétrique définie positive e_L donnée par $e_L(x,y) = E_L(ix,y)$. En notant $c_6'(A,L)$ le volume de la boule unitée de $\mathbb{R}^{2\dim A}$ pour cette norme, le théorème des minimas successifs de Minkowski nous permet d'en déduire qu'il existe une base de $\Omega_{B(\mathbb{C})}$ formée d'éléments (notés $\{\omega_1,\ldots,\omega_{2\dim B}\}$) appartenant à $\Omega_{A(\mathbb{C})}$, tels que

$$\prod_{i=1}^{2\dim B} ||\,\omega_i\,|| \leq c_6'(A,L)\deg_L B.$$

On pose $c_{\min}(A,L) = \min\left\{1, ||\,\lambda_i\,|| \ / \ \lambda_i \in \Omega_{A(\mathbb{C})} - \{0\}\right\}$, et on note $\omega_{\max}$ le ω_i de plus grande norme. On a

$$||\,\omega_{\max}\,||\,c_{\min}(A,L)^{2g-1} \leq \prod_{i=1}^{2\dim B} ||\,\omega_i\,|| \leq c_6'(A,L)D.$$

Ainsi, on tire $||\,\omega_{\max}\,|| \leq c_7'(A,L)D$, ce qui entraîne

$$\text{Card}\ \mathcal{E}_L(D) \leq c_5(A,L)D^{(2\dim A)^2}.$$

□

Lemme 6 *Le degré relativement à L de $Y(D,d)$ est majoré par une expression de la forme $c_6(A,L)D^{c_7(A)}d^{c_8(A)}$.*

Démonstration : On sait par le theorem p. 154 de [35] que tout point de torsion de $A(\overline{k})$ défini sur une extension de degré inférieur à $c_1(A)d$ est d'ordre majoré par $c_8'(A)d^{7\dim(A)}$. On en déduit donc que l'ensemble des points de torsion définis sur une extension de degré inférieur à $c_1(A)d$ est de cardinal majoré par

$$c_9'(A)d^{(7\dim(A))(2\dim(A)+1)}. \tag{2.2}$$

Par ailleurs, on sait majorer le cardinal de $\mathcal{E}_L(D)$ par le lemme précédent, donc l'additivité du degré nous donne

$$\deg_L Y(D,d) \leq D\cdot\left(c_5(A,L)D^{(2\dim A)^2}\right)\cdot\left(c_9'(A)d^{(7\dim(A))(2\dim(A)+1)}\right). \tag{2.3}$$

L'inégalité (2.3) est bien de la forme voulue. □

2.4 Preuve du théorème 27

Quitte à remplacer V par la réunion des $\sigma(V)$ avec $\sigma \in \text{Gal}(\overline{k}/k)$, précisément, quitte à prendre l'image schématique de $V \subset A_K$ dans A, on peut supposer que V est définie sur k

et k-irréductible. Soit $\varepsilon > 0$ un réel. On suppose par l'absurde qu'il existe une hypersurface Z de A sur k, ne contenant pas V mais contenant tous les points de V d'ordre infini modulo toute sous-variété abélienne stricte de A, et tels que la hauteur vérifie $\widehat{h}_L(x) \leq \frac{\widehat{h}_L(V)}{\deg_L V} + \varepsilon$. Soit alors, δ un entier non nul. On considère la sous-variété Y_δ de A sur k de codimension supérieure à 1, définie par

$$Y_\delta = Y(D, d),$$

où $Y(D,d)$ est définie comme au paragraphe précédent, et où

$$D = c_2(A,L)\left(\frac{\widehat{h}_L(V)}{\deg_L(V)} + \varepsilon\right)^{c_4(A)} \left(c_0(\varepsilon)\deg_L(V)\delta^{\dim V}\right)^{c_3(A)},$$

et,

$$d = c_0(\varepsilon)\deg_L(V)\delta^{\dim V}.$$

Par hypothèse, V n'est contenue dans aucune réunion de sous-variétés de torsion strictes de A, donc $V \nsubseteq Y_\delta$. Il existe $\delta_1(\varepsilon, V, A, L)$ tel que pour tout $\delta \geq \delta_1(\varepsilon, V, A, L)$, on a l'inégalité

$$\log \deg_L(Y_\delta \cup Z) \leq \frac{\delta}{4\dim V}.$$

En effet, par le lemme 6, on sait que

$$\deg_L Y_\delta \leq c_6(A,L) D^{c_7(A)} d^{c_8(A)}.$$

En remplaçant D et d par leurs valeurs, et par additivité du degré, on en déduit l'inégalité pour tout $\delta \geq \delta_1(\varepsilon, V, A, L)$ assez grand. On se fixe désormais un tel δ, et on applique le corollaire 6 à $Y_\delta \cup Z$. On obtient ainsi un $x \in V \setminus (Y_\delta \cup Z)$ tel que

$$\widehat{h}_L(x) \leq \frac{\widehat{h}_L(V)}{\deg_L V} + \varepsilon \quad \text{et} \quad [k(x):k] \leq c_0(\varepsilon)(\deg_L V)\delta^{\dim V}.$$

Si x est un point de torsion modulo une sous-variété abélienne stricte de A, alors, le lemme 4 et le choix de D dans Y_δ entraîne que $x \in Y_\delta$. Ceci est impossible, donc par définition de Z, x appartient à Z. Mais ceci est également impossible. Ceci conclut par l'absurde. □

2.5 Preuve du corollaire 3

On commence par rappeler le théorème de Zhang sur les minimas successifs (cf. [59] theorem 5.2, et [60] theorem 1.10). Plus exactement, on en donne une version affaiblie qui nous suffira, ne faisant intervenir que le minimum essentiel.

Théorème 28 (Zhang) *Si V est une sous-variété de A sur K, alors*

$$\frac{\widehat{h}_L(V)}{(\dim V + 1)\deg_L V} \leq \mu_L^{\mathrm{ess}}(V) \leq \frac{\widehat{h}_L(V)}{\deg_L V}.$$

On peut maintenant passer à la preuve du corollaire 3 : soit $\varepsilon > 0$, le théorème 27 nous indique que l'ensemble des $x \in V(\overline{k})$ d'ordre infini modulo toute sous-variété abélienne stricte de A et qui sont de hauteur $\widehat{h}_L(x) \leq \frac{\widehat{h}_L(V)}{\deg_L V} + \varepsilon$ est Zariski dense dans V. En utilisant le théorème 28 de Zhang, on en déduit que les points $x \in V(\overline{k})$ d'ordre infini modulo toute sous-variété abélienne, et de hauteur $\widehat{h}_L(x) \leq (\dim V + 1)\mu_L^{\mathrm{ess}}(V) + \varepsilon$ est Zariski dense dans V. En particulier cet ensemble est non-vide. On choisit un élément x dedans. En appliquant le théorème 1.5. de [19] ainsi que la remarque qui suit ce théorème, on en déduit

$$\widehat{h}_L(x) \geq \frac{c(A,L)}{\delta_L(x)} \left(\frac{\log\log(3\delta_L(x))}{\log(2\delta_L(x))} \right)^{\kappa(g)},$$

où $c(A,L)$ est une constante ne dépendant que de A et de L, et $\kappa(g)$ est une constante effectivement calculable ne dépendant que de g (par exemple $\kappa(g) = (2g(g+1)!)^{g+2}$ convient). Or $\delta_L(x) \leq \delta_L(V)$ car une sous-variété de A contenant V contient x. On en déduit

$$\widehat{h}_L(x) \geq \frac{c(A,L)}{\delta_L(V)} \left(\frac{\log\log(3\delta_L(V))}{\log(2\delta_L(V))} \right)^{\kappa(g)}.$$

Notamment on en conclut

$$(\dim V + 1)\, \mu_L^{\mathrm{ess}}(V) + \varepsilon \geq \frac{c(A,L)}{\delta_L(V)} \left(\frac{\log\log(3\delta_L(V))}{\log(2\delta_L(V))} \right)^{\kappa(g)}.$$

Ceci termine la preuve en faisant tendre ε vers 0. □

2.6 Preuve du corollaire 4

On commence par prouver le corollaire dans un cas particulier, auquel on se ramènera ensuite.

Corollaire 7 *Si $A = \prod_{i=1}^n A_i^{r_i}$, où les A_i sont simples, est de type C.M., et si V est une sous-variété algébrique stricte de A sur k, k-irréductible et qui n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité*

$$\frac{\widehat{h}_M(V)}{\deg_M(V)} \geq \mu_M^{\mathrm{ess}}(V) \geq c(A,M) \deg_M(V)^{-\frac{1}{s-\dim V}} \left(\log(2\deg_M(V))\right)^{-\kappa(s)},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V, et où M est le fibré en droites ample associé au plongement

$$A = \prod_{i=1}^n A_i^{r_i} \hookrightarrow \prod_{i=1}^n \mathbb{P}_{n_i}^{r_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^N,$$

les A_i étant plongées dans $\mathbb{P}_{n_i}$ par des fibrés L_i très amples et symétriques.

Démonstration : On note G le plus petit sous-groupe algébrique contenant V. On note G^0 la composante connexe de l'identité de G. C'est une sous-variété abélienne de A, et elle est donc isogène à $B = \prod_{i=1}^n A_i^{s_i}$ où $0 \leq s_i \leq r_i$. On note alors $\pi : A \to B$ une projection naturelle obtenue par oubli de certaines coordonnées, de sorte que $\pi_{|G}$ est une isogénie. Montrons maintenant que l'on est dans les conditions d'application du corollaire 3 en prenant comme variété abélienne B, et comme sous-variété algébrique $\pi(V)$.

Si $\pi(V)$ est inclus dans une réunion de sous-variétés de torsion $\bigcup (C_i + \xi_j)$ où $\dim C_i < \dim B$, en notant H le plus petit sous-groupe algébrique contenant $\pi(V)$, on a toujours $\dim H < \dim B$. Ainsi $G_1 = G \cap \pi^{-1}(H)$ est un sous-groupe algébrique strict de G (car $\pi_{|G}$ est une isogénie), contenant V. Ceci est absurde.

Si $\pi(V) = B$, alors V est de torsion. Ceci est absurde.

Finalement, $\pi(V)$ est une k-sous-variété stricte de B, irréductible, et n'est pas incluse dans une réunion de sous-variétés de torsion strictes. On peut donc appliquer le corollaire 3. Par ailleurs, la hauteur et le degré sont définis relativement aux plongements

$$A = \prod_{i=1}^n A_i^{r_i} \hookrightarrow \prod_{i=1}^n \mathbb{P}_{n_i}^{r_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^{N_A}, \text{ et } B = \prod_{i=1}^n A_i^{s_i} \hookrightarrow \prod_{i=1}^n \mathbb{P}_{n_i}^{s_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^{N_B}.$$

De plus l'application $\overline{\pi} : \prod_{i=1}^n \mathbb{P}_{n_i}^{r_i} \to \prod_{i=1}^n \mathbb{P}_{n_i}^{s_i}$ est la projection linéaire définie par oubli de coordonnées. Dans ce cas et pour ces plongements on a,

$$\mu_{M_B}^{\text{ess}}(\pi(V)) \leq \mu_M^{\text{ess}}(V), \quad \text{et,} \quad \deg_{M_B} \pi(V) \leq \deg_M(V).$$

Ceci nous donne

$$\begin{aligned}
\mu_M^{\text{ess}}(V) &\geq \mu_{M_B}^{\text{ess}}(\pi(V)), \quad \text{d'où par le corollaire 3 et la remarque 5,} \\
&\geq c(B, M_B) \left(\deg_{M_B} \pi(V)\right)^{-\frac{1}{s-\dim V}} \left(\log 2 \deg_{M_B} \pi(V)\right)^{-\kappa(s)} \\
&\geq c(B, M_B) \left(\deg_M V\right)^{-\frac{1}{s-\dim V}} \left(\log 2 \deg_M(V)\right)^{-\kappa(s)}. \\
&\geq c'(A, M) \left(\deg_M V\right)^{-\frac{1}{s-\dim V}} \left(\log 2 \deg_M(V)\right)^{-\kappa(s)},
\end{aligned}$$

où on a pris pour $c'(A, M)$ le minimum des $c(B, M_B)$ quand s_i varie dans $[\![0, r_i]\!]$. On conclut en appliquant le théorème 28 de Zhang. □

On donne maintenant la preuve du corollaire 4 : la variété abélienne A est donnée avec une isogénie ρ vers $B = \prod_{i=1}^n A_i^{r_i}$. Soit V la sous-variété de A comme dans les hypothèses. On vérifie que $W = \rho(V)$ est une sous-variété de B vérifiant les mêmes hypothèses. Il résulte facilement de la preuve de la proposition 14. de [40] qu'il existe $c'(A, L)$ tel que

$$\widehat{h}_L(V) \geq c'(A, L) \widehat{h}_M(W).$$

Ainsi, en appliquant le résultat précédent, on en déduit presque l'inégalité voulue : il faut encore remplacer le degré $\deg_M(W)$ par $\deg_L(V)$. Or

$$\deg_M(W) = (\deg \rho) \deg_{\rho^* M}(V).$$

D'autre part $\rho^* M$ et L sont amples, donc on a des inégalités

$$c_2(A, L) \deg_{\rho^* M}(V) \geq \deg_L V \geq c_3(A, L) \deg_{\rho^* M}(V).$$

En injectant ceci dans l'inégalité donnée par le corollaire 7 précédent, on peut conclure.

Chapitre 3

Problème de Lehmer pour les hypersurfaces de variétés abéliennes de type C.M.

Il s'agit, à quelques modifications de notations près, de l'article [43] paru dans la revue *Acta Arithmetica*.

3.1 Introduction

On sait depuis les travaux de Philippon [38] [39] [40], puis Bost, Gillet, Soulé [17] dans le cadre de l'intersection arithmétique, comment définir la hauteur des variétés projectives ; l'idée étant de considérer un point comme une variété de dimension zéro et de généraliser ceci en dimension supérieure. De même que dans le cas des points, on sait pour les variétés abéliennes munies d'un fibré en droites ample et symétrique définir une hauteur particulièrement agréable : la hauteur canonique $\widehat{h}_L$, ou hauteur normalisée. En dimension zéro, il existe un théorème caractérisant les points de hauteur normalisée nulle ; c'est un résultat de Kronecker dans le cas de $\mathbb{G}_m$. Philippon [40] (dans le cas d'un produit de courbes elliptiques) puis Zhang [61] et David-Philippon [20] dans le cas général ont montré comment généraliser ce résultat pour caractériser les sous-variétés de hauteur normalisée nulle : ce sont les translatées d'une sous-variété abélienne par un point de torsion. On dit qu'une telle sous-variété est une sous-variété de torsion. La réponse à cette question résoud une conjecture de Bogomolov qui, dans sa formulation initiale a été démontrée en premier par Ullmo [56]. Ceci étant, on peut se demander comment minorer la hauteur normalisée d'une sous-variété de hauteur non-nulle d'une variété abélienne. Dans leur article [20], David et Philippon ont formulé un problème général (le problème 1.7) contenant cette question. En terme du degré défini ci-dessous, on peut notamment faire ressortir de la discussion suivant la formulation de leur problème l'énoncé suivant :

Conjecture 13 (David-Philippon) *Soit A une variété abélienne définie sur un corps de nombres k, munie d'un fibré ample et symétrique $\mathcal{L}$. Soit V une sous-variété stricte de*

A sur k, k-irréductible et telle que $V_{\overline{k}}$ n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité

$$\frac{\widehat{h}_{\mathcal{L}}(V)}{\deg_{\mathcal{L}}(V)} \geq c(A/k,\mathcal{L})\deg_{\mathcal{L}}(V)^{-\frac{1}{s-\dim V}},$$

où s est la dimension du plus petit sous-groupe algébrique contenant V, et où $c(A/k,\mathcal{L})$ est une constante ne dépendant que de A/k et de $\mathcal{L}$.

3.1.1 Degré et hauteur

Soient k un corps de nombres supposé plongé dans $\mathbb{C}$, et $\mathcal{O}_k$ son anneau d'entiers. On dira que V est une *variété algébrique* sur k si V est un k-schéma de type fini géométriquement réduit. On dira que G est un *groupe algébrique* sur k si c'est une variété en groupes sur k. On dira que A est une *variété abélienne* définie sur k si c'est un groupe algébrique connexe propre et lisse sur k. Par sous-variété on entendra toujours sous-variété fermée.

Définition 28 On dit qu'une variété abélienne simple A/k sur un corps de nombres est *de type C.M.* si son anneau d'endomorphismes tensorisé par $\mathbb{Q}$ contient (après éventuellement extension du corps de base) un corps commutatif F de dimension $2\dim A$ sur $\mathbb{Q}$. Une variété abélienne A/k est dite *de type C.M.* si son anneau d'endomorphismes tensorisé par $\mathbb{Q}$ contient un produit de corps de nombres $K_1\times\cdots\times K_r$ tels que $\sum[K_i:\mathbb{Q}]=2\dim A$.

Soit X une variété projective munie d'un plongement $\varphi_{\mathcal{L}}: X\hookrightarrow\mathbb{P}^n_k$ défini par un fibré $\mathcal{L}$ très ample sur X. Si $\mathcal{O}(1)$ dénote le fibré standard sur $\mathbb{P}^n_{\mathcal{O}_k}$, on a $\varphi_{\mathcal{L}}^*\mathcal{O}(1)_k\simeq\mathcal{L}$. On note $\overline{\mathcal{O}(1)}$ le fibré standard muni de la métrique de Fubini-Study. Si V est une sous-variété de X, on note $\mathcal{V}_{\mathcal{L}}$ l'adhérence schématique de $\varphi_{\mathcal{L}}(V)$ dans $\mathbb{P}^n_{\mathcal{O}_k}$.

Définition 29 Si $\mathcal{L}$ est un fibré ample sur une variété abélienne A, et V une sous-variété de A, on définit le *degré de la variété V* relativement à $\mathcal{L}$, et on note $\deg_{\mathcal{L}}V$ l'entier $\deg\left(c_1(\mathcal{L})^{\dim V}\cdot V\right)$ où deg est le degré projectif usuel d'un 0-cycle.

Définition 30 On appelle *hauteur de la variété V* associée à $\mathcal{L}$, et on note $h_{\mathcal{L}}(V)$ le réel $h_{\overline{\mathcal{O}(1)}}(\mathcal{V}_{\mathcal{L}})$ où $h_{\overline{\mathcal{O}(1)}}(.)$ est la hauteur, au sens de Bost-Gillet-Soulé [17], associée au fibré hermitien $\overline{\mathcal{O}(1)}$.

Remarque 12 Par le théorème 3 p. 366 de [53], $h_{\mathcal{L}}(V)$ coincide avec la hauteur $h(f_{V,\mathcal{L}})$ de Philippon, telle que définie au paragraphe 2. de [40], où $f_{V,\mathcal{L}}$ est une forme éliminante de l'idéal de définition de $\varphi_{\mathcal{L}}(V)$ dans $k[X_0,\ldots,X_n]$. (Le terme d'erreur de [53] disparait du fait du changement de normalisation pour la hauteur de Philippon entre les articles [38] et [40]).

Définition 31 Dans le cas où $X=A$ est une variété abélienne, et où $\mathcal{L}$ est de plus symétrique, Philippon [40], puis Zhang [60] avec des méthodes arakeloviennes, ont montré en utilisant un procédé de limite à la Néron-Tate, comment définir une *hauteur canonique*, notée $\widehat{h}_{\mathcal{L}}(.)$, sur l'ensemble des sous-variétés de A. Cette hauteur vérifie notamment : si V

est une sous-variété de A, de stabilisateur G_V, et si n est un entier, alors,

$$\widehat{h}_{\mathcal{L}}\left([n](V)\right) = \frac{n^{2(\dim V+1)}}{|\ \ker\ [n] \cap G_V\ |}\widehat{h}_{\mathcal{L}}(V).$$

Définition 32 Soit A/k une variété abélienne. On dit qu'une sous-variété V de A/k est une *sous-variété de torsion* de A si $V_{\overline{k}} = a + B$ avec $a \in A_{\text{tors}}$ et B une sous-variété abélienne de $A_{\overline{k}}$.

D'après les résultats de Philippon [40], David-Philippon [20] et Zhang [60], on a, si V est une sous-variété de $A_{\overline{k}}/\overline{k}$, géométriquement irréductible

$$\widehat{h}_{\mathcal{L}}(V) = 0 \text{ si et seulement si } V \text{ est une sous-variété de torsion.}$$

Définition 33 Soient V une sous-variété de A sur k, et θ un nombre réel positif. On pose $V(\theta, \mathcal{L}) = \left\{ x \in V(\overline{k})\ /\ \widehat{h}_{\mathcal{L}}(x) \leq \theta \right\}$. On définit alors le *minimum essentiel* de V, et on note $\hat{\mu}^{\text{ess}}_{\mathcal{L}}(V)$ le réel

$$\hat{\mu}^{\text{ess}}_{\mathcal{L}}(V) = \inf\left\{ \theta > 0\ /\ \overline{V(\theta, \mathcal{L})} = V\ \right\},$$

où $\overline{V(\theta, \mathcal{L})}$ est l'adhérence de Zariski de $V(\theta, \mathcal{L})$ dans A.

3.1.2 Résultats

Dans la direction de la conjecture 13, on a le résultat suivant (cf. corollaire 2 de [42]) :

Théorème 29 *Soient A une variété abélienne de type C.M., $\mathcal{L}$ un fibré en droites ample et symétrique de A et V une sous-variété algébrique stricte de A sur k, k-irréductible et telle que $V_{\overline{k}}$ n'est pas réunion de sous-variétés de torsion. On a l'inégalité*

$$\frac{\widehat{h}_{\mathcal{L}}(V)}{\deg_{\mathcal{L}}(V)} \geq \hat{\mu}^{\text{ess}}_{\mathcal{L}}(V) \geq c(A/k, \mathcal{L}) \deg_{\mathcal{L}}(V)^{-\frac{1}{n-\dim V}} \left(\log(2\deg_{\mathcal{L}}(V))\right)^{-\kappa(n)},$$

où n est la dimension du plus petit sous-groupe algébrique contenant V, et où $\kappa(n)$ est une constante effectivement calculable ne dépendant que de n (par exemple la fonction $\kappa(n) = (2n(n+1)!)^{n+2}$ convient).

On se restreint dans cet article au cas particulier des hypersurfaces V d'une variété abélienne de type C.M. Dans ce cas et sous les hypothèses du théorème précédent, on a nécessairement $n = g$. En effet, par définition n appartient à $\{g-1, g\}$. De plus, si n était égal à $g-1$, alors V serait une réunion de sous-variétés de torsion, ce qui contredit l'hypothèse faite sur V. Ainsi, dans le cas des hypersurfaces, la conjecture est la suivante :

Conjecture 14 *Sous les hypothèses précédentes, et en supposant de plus que V est hypersurface de A, on a l'inégalité*

$$\widehat{h}_{\mathcal{L}}(V) \geq c(A/k, \mathcal{L}),$$

où $c(A/k, \mathcal{L})$ est une constante ne dépendant que de A/k et de $\mathcal{L}$.

De même, le théorème 29 se spécialise en

Théorème 30 *Sous les hypothèses précédentes, et en supposant que V est une hypersurface de A, on a l'inégalité*

$$\widehat{h}_{\mathcal{L}}(V) \geq \deg_{\mathcal{L}}(V)\hat{\mu}^{\mathrm{ess}}_{\mathcal{L}}(V) \geq c(A/k, \mathcal{L}) \left(\log(2\deg_{\mathcal{L}}(V))\right)^{-\kappa(g)},$$

où g est la dimension de A, et où $\kappa(g)$ est une constante effectivement calculable ne dépendant que de g (par exemple $\kappa(g) = (2g(g+1)!)^{g+2}$ convient).

Dans ce cadre restreint aux hypersurfaces, on montre un résultat sensiblement plus fin en direction de la conjecture 14 : on peut prendre pour κ une valeur absolue, indépendante de g. En notant $\delta_{i,j}$ le symbole de Kronecker (valant 1 si $i = j$ et 0 sinon), on démontre ici le résultat suivant :

Théorème 31 *Si A est une variété abélienne de type C.M., $\mathcal{L}$ un fibré en droites ample et symétrique de A et si V est une hypersurface irréductible de A sur k telle que $V_{\overline{k}}$ n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité*

$$\widehat{h}_{\mathcal{L}}(V) \geq \deg_{\mathcal{L}}(V)\hat{\mu}^{\mathrm{ess}}_{\mathcal{L}}(V) \geq c(A/k, \mathcal{L}) \frac{(\log\log 3\deg_{\mathcal{L}} V)^{1+2\delta_{g-s,1}}}{(\log 2\deg_{\mathcal{L}} V)^{2+\delta_{g-s,1}}},$$

où s est la dimension du stabilisateur de V.

Notons que $\delta_{g-s,1} = 0$ sauf si A/k est le produit $E \times B$ d'une courbe elliptique E/k et d'une variété abélienne B/k, et si V est de la forme $\overline{\{P\}} \times B$, où P est un point $\overline{k}$-rationnel de E qui n'est pas de torsion. Dans ce cas, en supposant que A/k est une courbe elliptique, $\mathcal{L}$ le fibré associé au diviseur $3(0)$, et où $V = \overline{\{P\}}$ est l'ensemble des conjugués d'un point non de torsion $P \in A(K)$ dans une extension finie $D = [K : k]$, on retrouve exactement le résultat de Laurent [31] sur le problème de Lehmer elliptique, à savoir

$$\widehat{h}(P) \geq \frac{c(A)}{D} \left(\frac{\log\log 3D}{\log 2D}\right)^3.$$

Dans le cas d'une "vraie" hypersurface, (i.e., quand $\delta_{g-s,1} = 0$), on obtient une minoration un peu meilleure.

La démonstration suit fondamentalement les idées (et reprend une grande partie des preuves) de l'article de David-Hindry [19] concernant le problème de Lehmer pour les

points d'une variété abélienne. Il s'agit en fait d'une extension d'un travail de Amoroso-David [3] concernant le cas des tores, au cas des variétés abéliennes de type C.M. On fait un raisonnement par l'absurde, et on se fixe une hypersurface V contredisant la conclusion du théorème. La preuve consiste essentiellement en une preuve de transcendance classique. On commence tout d'abord par construire une fonction auxiliaire, nulle avec un grand ordre sur V. Pour cela on met en oeuvre une astuce dûe à Amoroso-David (qu'ils introduisent dans [3]) permettant de se ramener à un système d'équations fini et de hauteur controlée. Ceci nous permet d'appliquer un lemme de Siegel pour construire la fonction auxiliaire F. La deuxième partie de la preuve, l'extrapolation, consiste à montrer que F continue à s'annuler avec un ordre relativement grand sur les transformées $\alpha_v(V)$ de V par certaines isogénies α_v où v décrit un ensemble de places finies convenables du corps de définition k (les α_v sont des relevées sur A/k des morphismes de Frobenius en caractéristique finie p_v. C'est pour assurer l'existence de ces isogénies que l'on se restreint au cas C.M.). Il s'agit d'une extrapolation aux places v-adiques. L'idée pour montrer ceci est d'appliquer une généralisation du petit théorème de Fermat : c'est la méthode employée pour la première fois par Dobrowolski [23] dans le cas du problème de Lehmer sur $\mathbb{G}_m$. Cette idée a ensuite été reprise par Laurent [31] dans le cas des courbes elliptiques à multiplication complexes puis étendue au cas des variétés abéliennes de type C.M. par David-Hindry [19]. C'est cette dernière généralisation que nous allons reprendre. Ceci étant fait, il suffit pour conclure d'appliquer le théorème de Bézout géométrique pour aboutir à une contradiction (pour peu que les différents paramètres intervenant dans l'étape de transcendance aient étés convenablement choisis). Pour cette dernière étape, on a besoin d'avoir une bonne minoration du degré de l'union des $\alpha_v(V)$. Ceci se fait en suivant les calculs de [19].

Remerciements : Je tiens à remercier Sinnou David pour m'avoir suggérer l'écriture de cet article, et je tiens également à remercier Marc Hindry pour les nombreuses discussions que nous avons eu sur le sujet.

3.2 Frobenius, isogénies admissibles et dérivations

3.2.1 Morphismes de Frobenius

On commence par introduire quelques notations :

Si k est un corps de nombres, on note $\mathcal{O}_k$ son anneau d'entiers, v une place finie de k, et k_v le corps résiduel associé à v.

Si A/k est une variété abélienne, on note $\mathcal{A}/\mathcal{O}_k$ son modèle de Néron, et A_v/k_v la fibre spéciale correspondant à la place finie v. Rappelons la propriété universelle du modèle de Néron : si $\mathcal{X}/\mathcal{O}_k$ est lisse, de fibre générique X/k, tout k-morphisme $X \to A$ se relève de manière unique en un $\mathcal{O}_k$-morphisme $\mathcal{X} \to \mathcal{A}$.

Sur la variété A_v/k_v, on dispose d'un endomorphisme particulier : le morphisme de Frobenius Frob_v, correspondant en coordonnées projectives à l'élévation à la puissance $q = \mathrm{N}(v)$,

où $\mathrm{N}(v)$ est la norme $K/\mathbb{Q}$ de v.

La propriété universelle du produit fibré $A_v = \mathcal{A} \times_{\mathcal{O}_k} k_v$ permet d'associer naturellement à tout $\mathcal{O}_k$-endomorphisme de $\mathcal{A}$ un k_v-endomorphisme de A_v. En utilisant la propriété universelle du modèle de Néron, on en déduit une flèche naturelle

$$\Psi : \mathrm{End}_k(A) \to \mathrm{End}_{k_v}(A_v).$$

Cette flèche n'est en général pas surjective, mais on peut par contre montrer qu'elle est injective aux places de bonne réduction. Dans le cas C.M., un théorème de Shimura-Taniyama permet d'affirmer que le morphisme Frob_v se relève en presque toutes places :

Proposition 9 (Shimura-Taniyama) *Soit A/k une variété abélienne de type C.M. Notons $\prod_{i=1}^r K_i$ le produit de corps de nombres inclus dans $\mathrm{End}_k(A) \otimes \mathbb{Q}$ et tel que $\sum_{i=1}^r [K_i : \mathbb{Q}] = 2\dim A$. On suppose que le corps de nombres k contient tous les K_i, et que $\prod_{i=1}^r \mathcal{O}_{K_i}$ est inclus dans $\mathrm{End}_k(A)$. Alors, pour presque toutes places, l'endomorphisme Frob_v se relève en un k-endomorphisme α_v de A. On appelera morphisme de Frobenius sur A un tel endomorphisme.*

Démonstration C'est le Theorem 1 paragraphe III.13 de [49]. □

Ce sont ces morphismes de Frobenius sur A/k qui vont nous permettre d'écrire l'étape d'extrapolation.

Remarque 13 En fait on pourrait spécifier les places qu'il faut exclure dans la proposition, mais nous n'en aurons pas besoin. Par ailleurs, pour pouvoir appliquer le théorème, il faut vérifier deux conditions : la première est toujours satisfaite quitte à faire une extension de degré borné de k. La seconde n'est pas toujours satisfaite, mais on peut toujours trouver une variété abélienne isogène qui la vérifie.

Quitte à faire une extension de degré borné de k, et quitte à prendre une variété abélienne isogène à la variété de départ, on supposera désormais toujours que les hypothèses de la proposition 9 sont satisfaites.

3.2.2 Isogénies admissibles

On rappelle la notion d'isogénie admissible telle qu'introduite dans [19].

Définition 34 Soient A une variété abélienne et $\mathcal{L}$ un fibré ample sur A. Une isogénie α de A est dite *admissible* par rapport à $\mathcal{L}$ si

1. α est dans le centre de $\mathrm{End}(A)$.
2. il existe un entier $\mathrm{q}(\alpha)$ appelé *poids* de α tel que $\alpha^\star \mathcal{L} \simeq \mathcal{L}^{\otimes \mathrm{q}(\alpha)}$.

Remarque 14 En fait la condition (1) ne sert qu'a simplifier l'énoncé du lemme 9. C'est la condition (2) qui importe vraiment. Les seules isogénies qui nous intéresseront sont les relevées α_v des morphismes de Frobenius qui sont admissibles (cf. la Proposition 10).

Lemme 7 *Soient A une variété abélienne de dimension g munie d'un fibré en droites très ample $\mathcal{L}$, et α une isogénie admissible relativement à $\mathcal{L}$, de poids $q = \mathrm{q}(\alpha)$. Dans le plongement projectif de A, associé à $\mathcal{L}$, $A \hookrightarrow \mathbb{P}_n$, on a :*

1. $\mathrm{card}\,(\ker(\alpha)) = q^g$,
2. *pour toute sous-variété V de A de stabilisateur G_V, on a*

$$\deg_{\mathcal{L}}(\alpha(V)) = \frac{q^{\dim(V)}}{|G_V \cap \ker(\alpha)|} \deg_{\mathcal{L}}(V)$$

Démonstration Le point (1) est facile : par définition, $\alpha^\star\mathcal{L} \simeq \mathcal{L}^{\otimes q}$. On a donc,

$$q^g \deg_{\mathcal{L}}(A) = \deg_{\mathcal{L}^{\otimes q}}(A) = \deg_{\alpha^\star\mathcal{L}}(A) = |\ker(\alpha)| \deg_{\mathcal{L}}(A).$$

L'amplitude de $\mathcal{L}$ nous assure que le dernier degré est strictement positif. On simplifie pour conclure. Pour le point (2), il s'agit du point (ii) du lemme 6. de [29]. □

Lemme 8 *Soient G un sous-groupe algébrique de la variété abélienne A/k, $\mathcal{L}$ un fibré très ample sur A, et α une isogénie admissible relativement à $\mathcal{L}$ de poids $\mathrm{q}(\alpha)$ de A. On a*

$$\mathrm{q}(\alpha)^{\dim G} \leq \mathrm{card}\,(\ker(\alpha) \cap G) \leq \left[G : G^0\right] \mathrm{q}(\alpha)^{\dim G}.$$

Démonstration On note que

$$\left[G : G^0\right] \mathrm{card}\left(\ker(\alpha) \cap G^0\right) \geq \mathrm{card}\,(\ker(\alpha) \cap G) \geq \mathrm{card}\left(\ker(\alpha) \cap G^0\right).$$

La restriction de α à la sous-variété abélienne G^0 est encore une isogénie admissible de poids $\mathrm{q}(\alpha)$ pour $(G^0, \mathcal{L}_{|G^0})$ (cf. Lemme 2.4. point (ii) de [19]). Par le point (1) du lemme 7 précédent, on en déduit que le cardinal du noyau de cette isogénie $\alpha_{|G^0}$ est $\mathrm{q}(\alpha)^{\dim G^0}$. □

Soit V une sous-k-variété stricte de A, k-irréductible. Le lemme suivant (dont l'origine remonte à Dobrowolski [23]) montre que les images par une isogénie admissible des composantes géométriquement irréductibles de $V_{\overline{k}}$ sont essentiellement distinctes. On commence pour cela par donner une définition :

Définition 35 Soient A une variété abélienne et $\mathcal{L}$ un fibré en droites ample sur A. Deux isogénies admissibles de A par rapport à $\mathcal{L}$ sont dites *premières entre elles* si leurs poids sont premiers entre eux.

Lemme 9 *Soient A une variété abélienne sur k de dimension $g \geq 1$, $\mathcal{L}$ un fibré en droites très ample sur A, V une sous-k-variété stricte de A, irréductible sur k. Si $V_{\overline{k}}$ n'est pas une réunion de sous-variétés de torsion de $A_{\overline{k}}$, on a :*

1. *Pour tout couple (α, β) d'isogénies admissibles pour $\mathcal{L}$, de poids distincts, pour tout $\sigma \in \mathrm{Gal}(\overline{k}/k)$, et pour toute composante géométriquement irréductible W de $V_{\overline{k}}$, les sous-variétés $\alpha(W)$ et $\beta(\sigma(W))$ sont distinctes.*

2. *Soit $\mathcal{P}$ un ensemble d'isogénies admissibles pour $\mathcal{L}$, deux à deux premières entre elles. Notons $V_1, \ldots, V_M$ les composantes géométriquement irréductibles de $V_{\overline{k}}$, et notons $\mathcal{Q}$ le sous-ensemble de $\mathcal{P}$ défini par*

$$\mathcal{Q} = \{\alpha \in \mathcal{P} \ / \ \exists i, j, \ 1 \leq i < j \leq M, \quad \alpha(V_i) = \alpha(V_j)\}.$$

Le cardinal de $\mathcal{Q}$ est majoré par $\frac{\log M}{\log 2}$.

Démonstration Dans ce contexte il s'agit de la proposition 2.7. de [19] □

On conclut ce paragraphe en "rappelant" que les morphismes de Frobenius sur A/k sont des isogénies admissibles :

Définition 36 Soient A une variété abélienne et $\mathcal{L}$ un fibré en droites ample sur A. Suivant Mumford , on dit que $\mathcal{L}$ est *totalement symétrique* si $\mathcal{L}$ est le carré d'un fibré symétrique.

Le théorème de Lefschetz (cf. par exemple le Theorem A.5.3.6 de [30]) nous indique que si $\mathcal{L}$ est un fibré ample, alors $\mathcal{L}^{\otimes 3}$ est très ample.

Proposition 10 *Soient A/k une variété abélienne de type C.M. vérifiant les hypothèses de la proposition 9, et $\mathcal{L}$ un fibré très ample et totalement symétrique sur A. Soit α_v un morphisme de Frobenius sur A pour la place finie v. Alors, α_v est une isogénie admissible pour $\mathcal{L}$ de poids* $\mathrm{q}(\alpha)$.

Démonstration C'est la proposition 3.3. de [19]. □

3.3 Données

3.3.1 Situation

Définition 37 On dit qu'une sous-variété X de $\mathbb{P}_n$ est *projectivement normale* si son anneau de coordonnées $S(X)$ est un anneau normal (i.e., intégralement clos).

On peut montrer (cf. par exemple Birkenhake-Lange [13] p. 190-193) que $X \subset \mathbb{P}_n$ est projectivement normale si et seulement si elle est normale, et pour tout $d \geq 0$ la flèche naturelle

$$H^0(\mathbb{P}_n, \mathcal{O}_{\mathbb{P}_n}(d)) \to H^0(X, \mathcal{O}_X(d))$$

est surjective.

Concernant les variétés abéliennes plongées de manière projectivement normale, on a le résultat suivant que l'on trouve dans [13] theorem 3.1 p. 190.

Proposition 11 *Soient A/k une variété abélienne, et $\mathcal{L}$ un fibré ample sur A. Pour tout $n \geq 3$, le fibré $\mathcal{L}^{\otimes n}$ définit un plongement projectivement normal de A dans un espace projectif $\mathbb{P}_n$.*

Soient A/k une variété abélienne sur un corps de nombres, munie d'un fibré symétrique ample $\mathcal{L}$. Quitte à travailler avec $\mathcal{L}^{\otimes 4}$ plutôt qu'avec $\mathcal{L}$, on peut supposer que $\mathcal{L}$ est très ample, totalement symétrique et définit un plongement projectivement normal de A dans un projectif $\mathbb{P}_n$. On note $\mathcal{M} = \mathcal{L}\boxtimes\mathcal{L}$ le fibré sur $A\times A$ associé à $\mathcal{L}$. Soit V une k-hypersurface irréductible de A. On note I_V l'idéal de définition de V dans $\mathbb{P}_n$. Si N est un entier, on a

$$\begin{array}{ccccccccc} V & \subset & A & \overset{i}{\hookrightarrow} & A\times A & \hookrightarrow & \mathbb{P}_n\times\mathbb{P}_n & \underset{\text{Segre}}{\hookrightarrow} & \mathbb{P}_{(n+1)^2-1} \\ & & x & \mapsto & (x,[N]x) & & & & \end{array}$$

Soient L et T deux entiers. On note $\{s_0,\dots,s_l\}$ une base de $H^0(A\times A,\mathcal{M})$. On peut, par projective normalité, choisir une base $\{Q_1,\dots,Q_m\}$ du k-vectoriel $H^0\left(A\times A,\mathcal{M}^{\otimes L}\right)$ telle que tous les Q_i sont homogènes de degré L en les s_j. De plus, on peut aussi voir les s_i comme des $(1,1)$-formes homogènes de $k[\mathbf{X},\mathbf{Y}]$ où $\mathbf{X}=(X_0,\dots,X_n)$, et $\mathbf{Y}=(Y_0,\dots,Y_n)$. Enfin on note T_B l'espace tangent à l'origine de la sous-variété abélienne $B=i(A)$ de $A\times A$ définie par $y=[N]x$.

3.3.2 Choix des paramètres

Soit C_0 un réel positif, on note s la dimension du stabilisateur de V, et $\delta_{i,j}$ le symbole de Kronecker (valant 1 si $i=j$ et 0 sinon). On pose

$$N_1 = \left[C_0^{g+2}\left(\log 2\deg_{\mathcal{L}} V\right)^{1+\delta_{g-s,1}}\left(\log\log 3\deg_{\mathcal{L}} V\right)^{1-2\delta_{g-s,1}}\right],$$

$$m = \left[\frac{\log\left(C_0^{\frac{g+1}{2}}\left(\deg_{\mathcal{L}} V\right)^{\frac{1}{2}}\left(\log 2\deg_{\mathcal{L}} V\right)^{\frac{1}{2}}\left(\log\log 3\deg_{\mathcal{L}} V\right)^{-1}\right)}{\log 2}\right],\ N=2^{m+1}$$

$$T = \left[C_0^{g+1}\deg_{\mathcal{L}} V\log 2\deg_{\mathcal{L}} V\left(\log\log 3\deg_{\mathcal{L}} V\right)^{-3}\right],$$

$$L = \left[C_0^{g+\frac{1}{2}}\deg_{\mathcal{L}} V\log 2\deg_{\mathcal{L}} V\left(\log\log 3\deg_{\mathcal{L}} V\right)^{-2}\right],$$

et,

$$T_1 = \left[C_0^{g}\deg_{\mathcal{L}} V\left(\log\log 3\deg_{\mathcal{L}} V\right)^{-2}\right].$$

Ces paramètres sont choisis de sorte que :

1. le nombre N est une puissance de 2 et vérifie l'encadrement

$$\frac{N}{2} \le C_0^{\frac{g+1}{2}}\left(\deg_{\mathcal{L}} V\right)^{\frac{1}{2}}\left(\log 2\deg_{\mathcal{L}} V\right)^{\frac{1}{2}}\left(\log\log 3\deg_{\mathcal{L}} V\right)^{-1} < N.$$

2. $N^2 > L+1$, afin qu'une forme F bihomogène de bi-degré (L,L) qui est non-identiquement nulle sur $A\times A$, ne soit pas identiquement nulle sur la sous-variété abélienne B.

3. le minimum essentiel des variétés intervenant est borné, autrement dit,

$$N^2 N_1 \hat{\mu}^{\text{ess}}(V) \leq c,$$

4. $T > L$, où T va être l'ordre d'annulation dans le lemme de Siegel, et L le degré du polynôme construit.
5. $T > T_1$, puisqu'on ne peut pas, par extrapolation espérer un ordre d'annulation meilleur que celui dont on est parti (T_1 étant l'ordre d'annulation sur les sous-variétés sur lesquelles on extrapole).

On fixe un premier p_0 (ne dépendant que de A) tel que pour tout premier $p \geq p_0$ et pour toute place v divisant p, le morphisme de Frobenius α_v sur A existe. On fixe alors pour chaque premier $p \geq p_0$ une place v au dessus de p. On note $\mathcal{P}_k$ l'ensemble des places ainsi obtenues.

Dans toute la suite, les inégalités que l'on écrira seront vraies pour tout $\deg_{\mathcal{L}} V$ et C_0 assez grands (i.e., plus grands qu'une constante ne dépendant que du couple $(A, \mathcal{L})$).

3.4 Lemme de Siegel

But : fabriquer un polynôme, $F = \sum_{i=1}^{m} b_i Q_i$, à coefficients entiers relatifs, en les fonctions abéliennes de $A \times A$, tel que F est de "petite" hauteur, et tel que F s'annule à un ordre supérieur à T sur $i(V)$, le long de T_B.

En notant Θ l'application thêta définie sur $T_{A(\mathbb{C})}$ par la composition

$$T_{A(\mathbb{C})} \xrightarrow{\exp_{A(\mathbb{C})}} A(\mathbb{C}) \xrightarrow{\varphi_{\mathcal{L}}} \mathbb{P}_n$$

associée à $\mathcal{L}$, ceci correspond à trouver une solution de petite hauteur au système d'inconnues les b_i

$$\frac{\partial^{\kappa} F\left(\Theta(\mathbf{u}+\mathbf{z}), \Theta(N(\mathbf{u}+\mathbf{z}))\right)}{\partial \mathbf{z}^{\kappa}}\Big|_{\mathbf{z}=0} = 0, \tag{3.1}$$

pour tout $\mid \kappa \mid \leq T$ et $\mathbf{u} \in T_{A(\mathbb{C})}$ tels que $\Theta(\mathbf{u}) \in V(\overline{k})$.

Lemme 10 *Soit $\theta > \hat{\mu}^{\text{ess}}_{\mathcal{L}}(V)$. Il existe un entier d_0 tel que si F est une solution du système*

$$\frac{\partial^{\kappa} F\left(\Theta(\boldsymbol{u}+\boldsymbol{z}), \Theta(N(\boldsymbol{u}+\boldsymbol{z}))\right)}{\partial \boldsymbol{z}^{\kappa}}\Big|_{\boldsymbol{z}=0} = 0, \tag{3.2}$$

pour tout $\mid \kappa \mid \leq T$ et $\boldsymbol{u} \in T_{A(\mathbb{C})}$ tels que $\Theta(\boldsymbol{u})$ appartient à l'ensemble fini

$$S_{d_0}(\theta) = \left\{ x \in V(\overline{k}) \ / \ \widehat{h}_{\mathcal{L}}(x) \leq \theta, \quad [k(x) : k] \leq d_0 \right\},$$

alors, F est une solution du système (3.1).

Démonstration Soit $d \geq 0$ un entier. On peut noter que l'ensemble $S_d(\theta)$ est stable sous l'action de $\mathrm{Gal}(\overline{k}/k)$ car V est une k-variété. Par ailleurs, on a clairement $S_d(\theta) \subset S_{d+1}(\theta)$ pour tout $d \geq 0$. Notons $k[\mathbf{X}]_L$ le k-espace vectoriel des polynômes homogènes de degré L, et $\mathcal{A}_d(\theta)$ le sous-k-espace vectoriel associé à $S_d(\theta)$. La suite $(\mathcal{A}_d(\theta))_{d\in\mathbb{N}}$ est une suite décroissante d'espaces vectoriels de dimension finie, elle est donc stationnaire. Notons d_0 l'indice à partir duquel cette suite est stationnaire. Par ailleurs, tous ces espaces contiennent le k-vectoriel ${I_V^{(T)}}_{|L}$ où $I^{(T)}$ est la puissance symbolique T-ième de I. Par définition de d_0, si P est un polynôme homogène de degré L nul sur S_{d_0}, il appartient à $\mathcal{A}_{d_0}(\theta)$, et donc il s'annule sur $\bigcup_{d\geq 0} S_d(\theta)$. De plus, par définition du minimum essentiel, $\bigcup_{d\geq 0} S_d(\theta)$ est Zariski-dense dans V, donc le polynôme P s'annule sur V. Ainsi, dans le système (3.1), on peut se restreindre aux $\mathbf{u} \in T_{A(\mathbb{C})}$ tels que $\Theta(\mathbf{u})$ appartient à $S_{d_0}(\theta)$. Par un théorème classique de Northcott, cet ensemble est fini. □

On appelle système (3.2) le nouveau système ainsi obtenu. On passe maintenant à une estimation du rang.

Lemme 11 *Il existe une constante c_1 telle que le rang du système (3.1) est majoré par*

$$c_1 T (LN^2)^{g-1} \deg_{\mathcal{L}} V.$$

Démonstration Il s'agit du lemme (ou plutôt de la preuve du lemme) 5.1 de [19]. En effet, dans ce lemme, les auteurs de [19] cherchent à obtenir une majoration du rang du sytème

$$\frac{\partial^\kappa F\left(\Theta(\mathbf{u}+\mathbf{z}), \Theta(N(\mathbf{u}+\mathbf{z}))\right)}{\partial \mathbf{z}^\kappa}\Big|_{\mathbf{z}=0} = 0, \tag{3.3}$$

où $\mathbf{u}$ est le logarithme d'un point Q fixé. L'idée est d'appliquer "l'astuce de Philippon-Waldschmidt" (voir [41] paragraphe 6, lemme 6.7). Pour majorer le rang de ce système, ils se donnent une variété V de dimension d contenant le point Q, et il majorent le système

$$\frac{\partial^\kappa F\left(\Theta(\mathbf{u}+\mathbf{z}), \Theta(N(\mathbf{u}+\mathbf{z}))\right)}{\partial \mathbf{z}^\kappa}\Big|_{\mathbf{z}=0} = 0, \tag{3.4}$$

pour tout $\mid \kappa \mid \leq T$ et $\mathbf{u} \in T_{A(\mathbb{C})}$ tels que $\Theta(\mathbf{u}) \in V(\overline{k})$. Il obtiennent comme majorant du rang de ce système le nombre $c_1 T^{g-d} (LN^2)^d \deg_{\mathcal{L}} V$. (on remplace dans leurs notations T_0 par T). En appliquant ceci à l'hypersurface V considérée, on obtient donc le résultat cherché. □

On peut maintenant énoncer le lemme de Siegel qui nous intéresse. Si $F = \sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ est un polynôme coefficients dans $\overline{k}$, on définit classiquement sa hauteur $h(F)$ comme étant la hauteur logarithmique absolue du point projectif défini par 1 et tous les coefficients a_i de F.

L'objectif de l'article consiste à montrer que, $\deg_{\mathcal{L}}(V)\hat{\mu}^{\mathrm{ess}}_{\mathcal{L}}(V) > \frac{c(A/k,\mathcal{L})}{\log 2 \deg_{\mathcal{L}}(V)^\alpha}$. On peut donc toujours supposer que $\hat{\mu}^{\mathrm{ess}}_{\mathcal{L}}(V)$ est strictement inférieur à 1.

Proposition 12 *Il existe une solution $F = \sum_{i=1}^{m} b_i Q_i$, $b_i \in \mathbb{Z}$ du système (3.1) de degré L et de hauteur*

$$h(F) \leq c_2 C_0^{\frac{1}{2}(g+1)} \deg_{\mathcal{L}}(V) \log 2 \deg_{\mathcal{L}}(V) (\log\log 3 \deg_{\mathcal{L}} V)^{-2}.$$

Démonstration Soit $1 > \theta > \hat{\mu}_{\mathcal{L}}^{\text{ess}}(V)$. Par le lemme 10 il suffit, pour trouver une solution du système (3.1), de trouver une solution du système (2). Ceci remarqué, on est ramené à une preuve classique. On suit pour cela la preuve du lemme 5.4. de [19].

On commence par évaluer la hauteur de système (2). Le système (18) ainsi que l'inégalité qui suit p. 42 de [19] nous indique que la hauteur de chaque coefficient du système est majorée par

$$c_4' L N^2 \theta + T \left(\log(T+L) + \log N\right). \tag{3.5}$$

Par ailleurs, le nombre d'inconnues I est $\dim H^0\left(A \times A, \mathcal{M}^{\otimes L}\right)$. Le théorème de Riemann-Roch pour les variétés abéliennes nous assure que I vérifie l'encadrement

$$c_5 L^{2g} \leq I \leq c_6 L^{2g}. \tag{3.6}$$

Notons M la matrice du système (2). Elle est définie sur k, donc si $\mathfrak{B}$ dénote le noyau de M, il est muni d'une k-structure. Si $\mathfrak{b}$ est la dimension de $\mathfrak{B}$, on a $\mathfrak{b} = I - \text{rg}(M)$. Le lemme de Siegel classique (cf. par exemple Schmidt [48] Lemma IVB, p.10) nous indique alors qu'il existe une solution non-triviale comme recherchée, de hauteur

$$h(F) \leq c_7 \frac{h(\mathfrak{B})}{\mathfrak{b}}, \tag{3.7}$$

où $h(\mathfrak{B})$ représente la hauteur du point $\mathfrak{B}$ défini dans la grassmannienne correspondante. De plus, le Lemma IV p.10 de [48] nous indique que $h(\mathfrak{B}) = h\left(\mathfrak{B}^{\perp}\right)$. L'espace $\mathfrak{B}^{\perp}$ étant l'espace vectoriel engendré par les colonnes de M, sa hauteur est par définition majorée par celle d'un mineur maximal $\Delta_{\max}$ de M. Cette dernière hauteur est majorée par

$$\begin{aligned} h(\Delta_{\max}) &\leq c_8 \text{rg}(M) \left(\log(\text{rg}M) + c_4' L N^2 \theta + T\left(\log(T+L) + \log N\right)\right) \\ &\leq c_9 T (L N^2)^{g-1} \deg_{\mathcal{L}} V \left(\log(2 \deg_{\mathcal{L}} V) + 2T \log T\right), \end{aligned}$$

la première inégalité découlant de (3.5), et la seconde du lemme 11 en utilisant également le fait que $T > L$ et $T > N$. En remplacant T et N par leur valeur, on obtient

$$h(\Delta_{\max}) \leq c_{10} L^{g-1} C_0^{(g+1)^2} (\deg_{\mathcal{L}} V \log 2 \deg_{\mathcal{L}} V)^{g+2} (\log\log 3 \deg_{\mathcal{L}} V)^{-2(g+2)}. \tag{3.8}$$

De plus, par l'inégalité (3.6), et par le choix de L, on a

$$\mathfrak{b} \geq c_{11} L^{g-1} \left(L^{g+1} - c_1 T (N^2)^{g-1} \deg_{\mathcal{L}} V\right) \geq c_{12} L^{(g+1)} L^{(g-1)}.$$

En remplaçant L^{g+1} par sa valeur, on obtient la minoration

$$\mathfrak{b} \geq c_{13} C_0^{(g+1)(g+\frac{1}{2})} L^{g-1} (\deg_{\mathcal{L}} V \log 2 \deg_{\mathcal{L}} V)^{g+1} (\log\log 3 \deg_{\mathcal{L}} V)^{-2(g+1)}. \tag{3.9}$$

On reprend maintenant l'inégalité (3.7) en remplaçant les paramètres par leurs valeurs. On obtient ainsi l'inégalité

$$h(F) \leq c_2 C_0^{\frac{1}{2}(g+1)} \deg_{\mathcal{L}}(V) \log 2 \deg_{\mathcal{L}}(V) (\log\log 3 \deg_{\mathcal{L}} V)^{-2}.\square$$

Remarque 15 La fonction auxiliaire F ainsi construite est une forme bihomogène de bidegré (L, L) non identiquement nulle sur $A \times A$. Elle n'est donc pas identiquement nulle sur B car $N^2 > L + 1$.

3.5 Extrapolation

On veut montrer dans ce paragraphe que F s'annule sur $i(\alpha_v(V))$, pour $v \in \mathcal{P}_k$ appartenant à un ensemble convenable. Pour cela, on utilise un argument remontant à Dobrowolski [23] dans son célèbre article sur la conjecture de Lehmer sur les points pour $\mathbb{G}_m$. Cet argument a été réécrit et adapté dans le cadre des variétés abéliennes de type C.M. dans l'article [19] suivant des idées de Laurent [31]. Ce que l'on fait ici repose sur le paragraphe 6 de [19].

Proposition 13 *La fonction auxiliaire F est nulle sur $i(\alpha_v(V))$ à un ordre supérieur à T_1 le long de T_B pour toute place $v \in \mathcal{P}_k$ de norme comprise entre $\frac{1}{2}N_1$ et N_1.*

Démonstration Soit $1 > \theta > \hat{\mu}_{\mathcal{L}}^{\text{ess}}(V)$. Il s'agit de reprendre la proposition 6.5. de [19]. On conserve donc leurs notations. Soient v une place comme dans l'énoncé, R un point de $V(\overline{k})$ défini sur une extension k' de k de hauteur normalisée inférieure à θ, et w une place de k' au dessus de v. Notons $\mathbf{R} = (R_0, \ldots, R_n)$ un système de coordonnées projectives de R dans $\mathcal{O}_w$, telles que $|| \mathbf{R} ||_w = 1$. Soit ∂^κ un opérateur différentiel d'ordre $| \kappa | \leq T_1$ le long de $T_{B(\mathbb{C})}$. L'application du petit théorème de Fermat dans le cadre des variétés abéliennes nous donne

$$\left|\partial^\kappa F\left(\mathbf{F}_{\alpha_v}(\mathbf{R}), \mathbf{F}^{(N)} \circ \mathbf{F}_{\alpha_v}(\mathbf{R})\right)\right|_w \leq |\pi_v|_w^{T-|\kappa|}, \tag{3.10}$$

où $\mathbf{F}_{\alpha_v}$ et $\mathbf{F}^{(N)}$ sont des formes homogènes de $\mathcal{O}_k[\mathbf{X}]$ de degré respectifs $\mathrm{N}(v)$ et 4^{m+1}, représentant respectivement l'endomorphisme de Frobenius sur A associé à v, et la multiplication par $N = 2^{m+1}$. Il s'agit de l'inégalité (20) p.47 de [19].
On veut maintenant sommer sur toutes les places w au-dessus de v. Malheureusement, le choix du système de coordonnées projectives pour R dépend de w. On est donc obliger d'alourdir les notations pour pallier ce probème. Soient S, S_N, S_{α_v}, S_{N,α_v} des coordonnées projectives non nulles de R, $\mathbf{F}^{(N)}(\mathbf{R})$, $\mathbf{F}_{\alpha_v}(\mathbf{R})$, $\mathbf{F}^{(N)} \circ \mathbf{F}_{\alpha_v}(\mathbf{R})$ respectivement. On note de plus $S_{w,N}$, S_{w,α_v}, S_{w,N,α_v} des coordonnées des ces points de valeur absolue w-adique maximale.

Soit maintenant ∂^κ un opérateur différentiel de longueur minimale pour lequel

$$\partial^\kappa F\left(\mathbf{F}_{\alpha_v}(\mathbf{R}), \mathbf{F}^{(N)} \circ \mathbf{F}_{\alpha_v}(\mathbf{R})\right)$$

est non nul. Si $|\kappa|$ est supérieur à T_1, on a gagné. Sinon on applique la formule de Leibniz en utilisant que F est bihomogène de bidegré (L, L). On a donc

$$\partial^\kappa F\left(\frac{\mathbf{F}_{\alpha_v}(\mathbf{R})}{S_{\alpha_v}}, \frac{\mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)}{S_{N,\alpha_v}}\right) = \frac{\partial^\kappa F\left(\mathbf{F}_{\alpha_v}(\mathbf{R}), \mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)\right)}{S_{\alpha_v}^L S_{N,\alpha_v}^L}$$

Or ceci est égal à

$$\partial^\kappa F\left(\frac{\mathbf{F}_{\alpha_v}(\mathbf{R})}{S_{w,\alpha_v}}, \frac{\mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)}{S_{w,N,\alpha_v}}\right) \cdot \frac{\left(S_{w,\alpha_v} S_{w,N,\alpha_v}\right)^L}{\left(S_{\alpha_v} S_{N,\alpha_v}\right)^L}.$$

On réécrit alors l'inégalité (3.10) en passant au log, en sommant sur toutes les places w au-dessus de v et en notant n_w les degrés locaux :

$$\sum_{w/v} n_w \log\left(\left|\partial^\kappa F\left(\frac{\mathbf{F}_{\alpha_v}(\mathbf{R})}{S_{\alpha_v}}, \frac{\mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)}{S_{N,\alpha_v}}\right)\right|_w\right) \tag{3.11}$$

$$\leq (T - |\kappa|) \sum_{w/v} n_w \log(|\pi_v|_w) + L \sum_{w/v} n_w \log\left(\frac{|S_{w,\alpha_v} S_{w,N,\alpha_v}|_w}{|S_{\alpha_v} S_{N,\alpha_v}|_w}\right). \tag{3.12}$$

Or

$$\sum_{w/v} n_w \log(|\pi_v|_w) = [k' : k] \log(|\pi_v|_v) \leq -[k' : k] \log\left(\mathrm{N}(v)\right) \tag{3.13}$$

De plus, on peut voir que

$$\sum_{w/v} n_w \log\left(\frac{|S_{w,\alpha_v} S_{w,N,\alpha_v}|_w}{|S_{\alpha_v} S_{N,\alpha_v}|_w}\right) \leq [k' : k]\left(h_{\mathcal{L}}(\alpha_v(R)) + h_{\mathcal{L}}(N\alpha_v(R))\right) \tag{3.14}$$

$$\leq [k' : k]\left(\mathrm{N}(v)\widehat{h}_{\mathcal{L}}(R) + N^2\mathrm{N}(v)\widehat{h}_{\mathcal{L}}(R) + c_{14}\right). \tag{3.15}$$

C'est l'inégalité (21) p. 49 de [19]. En tenant compte du fait que le point R est supposé de hauteur (de Néron-Tate) inférieure à θ, et en injectant ceci dans (3.12), on obtient, en remplaçant les paramètres par leur valeur, l'inégalité

$$-\frac{1}{[k' : k]} \sum_{w/v} n_w \log\left(\left|\partial^\kappa F\left(\frac{\mathbf{F}_{\alpha_v}(\mathbf{R})}{S_{\alpha_v}}, \frac{\mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)}{S_{N,\alpha_v}}\right)\right|_w\right) \geq \frac{1}{2} T \log N_1. \tag{3.16}$$

Il reste à majorer le membre de gauche de cette dernière inégalité. Notons A ce membre de gauche. Par définition de la hauteur (absolue logarithmique) projective, on a

$$A \leq h\left(\left(\partial^\kappa F\left(\frac{\mathbf{F}_{\alpha_v}(\mathbf{R})}{S_{\alpha_v}}, \frac{\mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)}{S_{N,\alpha_v}}\right)\right)^{-1}\right)$$

$$= h\left(\partial^\kappa F\left(\frac{\mathbf{F}_{\alpha_v}(\mathbf{R})}{S_{\alpha_v}}, \frac{\mathbf{F}^{(N)}\left(\mathbf{F}_{\alpha_v}(\mathbf{R})\right)}{S_{N,\alpha_v}}\right)\right),$$

ceci ayant un sens grace à l'hypothèse de non nullité de $\partial^\kappa F(\cdots)$. Il ne reste maintenant plus qu'à majorer cette dernière hauteur. Il s'agit d'un calcul classique (cf. par exemple [19] p. 50). On obtient

$$A \leq c_{15}\left(T_1 \log(T_1+L) + LN^2 \mathrm{N}(v)\theta + h(F)\right). \tag{3.17}$$

Finalement, en mettant ensemble les inégalités (3.16) et (3.17), on obtient

$$T \log N_1 \leq c_{16} T_1 \log(T_1+L) + c_{16} L N^2 N_1 \theta + c_{16} h(F). \tag{3.18}$$

On remplace les différents paramètres par leurs valeurs, et on obtient pour le membre de gauche de l'inégalité,

$$C_0^{g+1} \deg_{\mathcal{L}}(V) \log 2 \deg_{\mathcal{L}}(V) (\log\log 3 \deg_{\mathcal{L}}(V))^{-2},$$

et pour le membre de droite,

$$c_{17} C_0^g \deg_{\mathcal{L}}(V) \log 2 \deg_{\mathcal{L}}(V) (\log\log 3 \deg_{\mathcal{L}}(V))^{-2}.$$

Dès que C_0 est assez grand, on aboutit à une contradiction. □

3.6 Conclusion

On commence par minorer le degré de l'union des variétés transformées de V.

Proposition 14 *Soient A une variété abélienne sur k de dimension $g \geq 1$, $\mathcal{L}$ un fibré en droites ample sur A, et V une sous-k-variété stricte de A, irréductible sur k. On suppose que $V_{\overline{k}}$ n'est pas une réunion de sous-variétés de torsion de A, et que le nombre M de composantes géométriques de $V_{\overline{k}}$ est majoré par $c_3 \deg_{\mathcal{L}}(V)^g$. On considère enfin un ensemble d'isogénies β_v admissibles deux à deux premières entre elles, avec $v \in \mathcal{P}_k^1 = \mathcal{P}_k \cap [\![\frac{N_1}{2}, N_1]\!]$. On a :*

$$\deg\left(\bigcup_{v\in\mathcal{P}_k^1} \beta_v(V)\right) \geq c_4 \frac{\deg_{\mathcal{L}}(V)\ N_1^{g-\dim G_V}}{\log N_1}.$$

Démonstration Soit W une composante géométriquement irréductible de $V_{\overline{k}}$. Pour $v \in \mathcal{P}_k^1$, on a, β_v étant définie sur k,

$$\mathrm{card}\left(\ker(\beta_v) \cap G_{\sigma(W)}\right) = \mathrm{card}\left(\ker(\beta_v) \cap G_W\right).$$

Par ailleurs, comme W n'est pas une sous-variété de torsion de A (sinon $V_{\overline{k}}$ serait réunion de telles sous-variétés), le point (2) du lemme 9 nous indique que l'égalité $\beta_v(W) = \beta_v(\sigma(W))$ (et $W \neq \sigma(W)$) n'est possible que pour au plus $\frac{\log M}{2} \leq c_{17} \log 2 \deg_{\mathcal{L}} V$ éléments v de

$\mathcal{P}_k^1$. Notons $\mathcal{P}_k^{1\star}$ le sous-ensemble de $\mathcal{P}_k^1$ obtenu en enlevant ces éléments. Le théorème de Chebotarev nous indique que

$$\operatorname{card}\left(\mathcal{P}_k^1\right) \geq c_{18}\frac{N_1}{\log N_1}. \tag{3.19}$$

En remplaçant N_1 par sa valeur, on constate que

$$\operatorname{card}\left(\mathcal{P}_k^{1\star}\right) \geq \frac{1}{2}\operatorname{card}\left(\mathcal{P}_k^1\right). \tag{3.20}$$

En utilisant l'additivité du degré et les lemmes précédents, on a

$$\deg_{\mathcal{L}}\left(\bigcup_{v\in\mathcal{P}_k^1}\beta_v(V)\right) \geq \deg_{\mathcal{L}}\left(\bigcup_{v\in\mathcal{P}_k^{1\star},\sigma\in\mathrm{Gal}(\overline{k}/k)}\beta_v(\sigma(W))\right).$$

Par le lemme 9, ceci est supérieur à

$$\sum_{v\in\mathcal{P}_k^{1\star}}\deg_{\mathcal{L}}\left(\bigcup_{\sigma\in\mathrm{Gal}(\overline{k}/k)}\beta_v(\sigma(W))\right).$$

Enfin, le lemme 7 nous donne l'inégalité

$$\deg_{\mathcal{L}}\left(\bigcup_{v\in\mathcal{P}_k^1}\beta_v(V)\right) \geq M\deg_{\mathcal{L}} W\sum_{v\in\mathcal{P}_k^{1\star}}\frac{\mathrm{q}(\beta_v)^{\dim V}}{\mid G_W\cap\ker(\beta_v)\mid}.$$

Le lemme 2.1. (ii) de [19] nous indique que

$$\deg_{\mathcal{L}} G_W = \left[G_W : G_W^0\right]\deg_{\mathcal{L}}(G_W^0) \leq \deg_{\mathcal{L}}(V)^g$$

En particulier on en déduit que

$$\left[G_W : G_W^0\right] \leq \deg_{\mathcal{L}}(V)^g.$$

De plus, les β_v étant premiers entre eux, on a

$$\prod_{v\in\mathcal{P}_k^{1\star}}\mid\ker(\beta_v)\cap G_W\mid = \left|\ker\left(\prod_{v\in\mathcal{P}_k^{1\star}}\beta_v\right)\cap G_W\right|. \tag{3.21}$$

En appliquant le lemme 8, on en déduit

$$\left|\ker\left(\prod_{v\in\mathcal{P}_k^{1\star}}\beta_v\right)\cap G_W\right| \leq \left[G_W : G_W^0\right]\left(\prod_{v\in\mathcal{P}_k^{1\star}}\mathrm{q}(\beta_v)\right)^s. \tag{3.22}$$

En appliquant l'inégalité arithmético-géométrique, on obtient

$$\deg\left(\bigcup_{v\in\mathcal{P}_k^1}\beta_v(V)\right)\geq c_4\deg_{\mathcal{L}}(V)\frac{\operatorname{card}\left(\mathcal{P}_k^{1\star}\right)N_1^{g-1}}{\left(\prod_{v\in\mathcal{P}_k^{1\star}}\mid\ker(\beta_v)\cap G_W\mid\right)^{\frac{1}{\operatorname{card}\left(\mathcal{P}_k^{1\star}\right)}}}\quad . \tag{3.23}$$

En appliquant l'inégalité (3.22) et la minoration du cardinal de $\mathcal{P}_k^{1\star}$, on obtient

$$\deg\left(\bigcup_{v\in\mathcal{P}_k^1}\beta_v(V)\right)\geq c_4\frac{\deg_{\mathcal{L}}(V)\ N_1^g}{\log N_1\,[G_W:G_W^0]^{\frac{\log N_1}{c_{56}N_1}}\prod_{v\in\mathcal{P}_k^{1\star}}\mathrm{q}(\beta_v)^{\frac{g}{\mathcal{P}_k^{1\star}}}}\quad . \tag{3.24}$$

Enfin par définition de $\mathcal{P}_k^1$, on a la majoration $\mathrm{q}(\beta_v)\leq N_1$. En appliquant ceci et la majoration de l'indice de G_W^0 dans G_W, on a

$$\deg\left(\bigcup_{v\in\mathcal{P}_k^1}\beta_v(V)\right)\geq c_4\frac{\deg_{\mathcal{L}}(V)\ N_1^{g-\dim G_V}}{\log N_1}. \qquad \square \tag{3.25}$$

Remarque 16 C'est uniquement pour assurer l'inégalité (3.20) que l'on est conduit à choisir l'exposant du terme $\log\log$ dans N_1 tel qu'indiqué, plutôt que l'exposant $-\frac{1}{g-\dim G_V}$ qui serait plus proche des choix de [3]. Cette amélioration dans [3] est rendue possible par la résolution de deux complications techniques : passage à une hypersurface secondaire explicitement construite, et raffinement galoisien.

Ceci étant, on peut maintenant démontrer le théorème recherché.

Démonstration : on suppose par l'absurde que l'inégalité du théorème à prouver n'est pas vérifiée pour $C_0=c(A/k,\mathcal{L})^{-\frac{1}{g+3}}$ assez grand (i.e. $c(A/k,\mathcal{L})$ suffisamment petit). Dans cette preuve, on considère, pour alléger les notations, la variété abélienne A, comme étant plongée dans $\mathbb{P}_n$. Notons $\mathcal{Z}$ l'hypersurface sur k de $\mathbb{P}_n$ associée à la forme $F\circ\varphi$ de degré $(N^2+1)L$. Par choix de N (à savoir $(N^2+1)>L$), la variété $\mathcal{Z}\cap A$ est une hypersurface de A. De plus, par la proposition 13, on sait que cette hypersurface contient les variétés irréductibles $\alpha_v(V)$ avec une multiplicité supérieure à T_1, pour toute place v de norme comprise entre $\frac{1}{2}N_1$ et N_1. Donc le théorème de Bézout géométrique nous donne :

$$T\deg_{\mathcal{L}}(V)+T_1\deg_{\mathcal{L}}\left(\bigcup_{\frac{N_1}{2}\leq\mathrm{N}(v)\leq N_1}\alpha_v(V)\right)\leq(\deg_{\mathcal{L}}A)L(N^2+1).$$

Cette inégalité implique en particulier que le nombre M de composantes géométriquement irréductibles de V est majoré par une expression de la forme $c_3\deg_{\mathcal{L}}(V)^g$. On peut donc appliquer la proposition 14 avec $\beta_v=\alpha_v$. Celle-ci et l'inégalité obtenue par le théorème de Bézout nous fournissent l'inégalité

$$T_1\frac{\deg_{\mathcal{L}}(V)\ N_1^{g-\dim G_V}}{\log N_1}\leq c_{19}(A)L(N^2+1), \tag{3.26}$$

On remplace maintenant les paramètres par leurs valeurs pour conclure. Si C_0 est assez grand, l'inégalité est contredite : si $s = g - 1$, les deux membres sont du même ordre de grandeur, or, dans le membre de gauche, on a un terme constant de la forme C_0^{2g+2}, alors que dans le membre de droite, le terme constant est de la forme $C_0^{2g+\frac{3}{2}}$; sinon l'ordre de grandeur du membre de gauche est supérieur à celui du terme de droite. (En fait, T_1 est construit exactement pour contredire cette inégalité). □

Deuxième partie

Problème de Lehmer sur les points

Chapitre 4

Problème de Lehmer sur $\mathbb{G}_m$ et méthode des pentes

4.1 Introduction

Soit x un nombre algébrique. On note $h(x)$ sa hauteur de Weil logarithmique absolue. Cette hauteur est un nombre positif et un théorème de Kronecker affirme alors que $h(x) = 0$ si et seulement si x est une racine de l'unité. Le problème de Lehmer consiste à trouver la minoration optimale, en fonction du degré de $\mathbb{Q}(x)$, de la hauteur $h(x)$ quand x n'est pas une racine de l'unité. On a la conjecture

Conjecture 15 (Problème de Lehmer) *Il existe un réel $c > 0$ tel que pour tout point $x \in \overline{\mathbb{Q}}$, de degré D sur $\mathbb{Q}$, qui n'est pas une racine de l'unité, on a*

$$h(x) \geq \frac{c}{D}.$$

Dans cette direction, on doit à E. Dobrowolski le meilleur résultat inconditionnel (au choix de la constante c près) dans l'article [23] :

Théorème 32 (Dobrowolski) *Il existe un réel $c > 0$ tel que pour tout nombre $x \in \overline{\mathbb{Q}}$, de degré D sur $\mathbb{Q}$, qui n'est pas une racine de l'unité, on a*

$$h(x) \geq \frac{c}{D} \left(\frac{\log \log(3D)}{\log(2D)} \right)^3.$$

Dans ce qui suit, on retrouve ce résultat, essentiellement en transcrivant la preuve de E. Dobrowolski dans le formalisme des pentes que J.-B. Bost a introduit dans [15]. L'objectif était ici de voir dans quelle mesure les preuves de transcendance "classiques" concernant le

problème de Lehmer peuvent se traduire en utilisant l'inégalité des pentes. Il serait maintenant intéressant d'essayer d'adapter la preuve du théorème 2 de Laurent dans ce langage. L'idée est que l'inégalité des pentes permet de mieux exploiter la géométrie des objets avec lesquels on travaille. Si ceci n'est pas flagrant dans le cas de $\mathbb{G}_m$, cela le serait certainement plus dans le cas d'une courbe elliptique E, où le formalisme des pentes permettrait d'incorporer directement l'inégalité sur la hauteur de Néron-Tate, sans avoir à passer par l'artifice consistant à plonger E dans $E \times E$ et à considérer un "gros" multiple du point considéré en vue de minimiser la différence entre hauteur de Néron-Tate et hauteur de Weil. On pourrait peut-être obtenir ainsi un parallélisme complet pour le problème de Lehmer sur le groupe multiplicatif et sur les courbes elliptiques à multiplication complexe.

On peut mentionner dans la direction de la conjecture 1.1. l'article de C.J. Smyth [52] qui démontre cette conjecture dans le cas des nombres algébriques non-réciproques, l'article de A. Schinzel [47] qui démontre la conjecture dans le cas des nombres totalement réels, ainsi que le papier de F. Amoroso et S. David [2] qui généralise en dimension supérieure la conjecture de Lehmer et le résultat de Dobrowolski. En corollaire de leur résultat, les auteurs de [2] prouvent la conjecture de Lehmer classique dans le cas où $\mathbb{Q}(x)/\mathbb{Q}$ est une extension galoisienne.

4.2 Notations et préliminaires

Avant de commencer la preuve, rappelons que l'on peut toujours se placer dans le cas où x est un entier algébrique.

Lemme 12 *Si $x \in \overline{\mathbb{Q}} - \overline{\mathbb{Z}}$ est de degré D, alors $h(x) \geq \frac{\log 2}{D}$.*

Désormais on fera toujours l'hypothèse que x est un entier algébrique qui n'est pas une racine de l'unité.

4.2.1 Notations

Soient A un anneau et n un entier. Dans toute la suite, on notera $A^n[X]$ le A-module des polynômes, en une indéterminée, de degré inférieur à n. Par exemple, $\mathbb{Z}_p^n[X]$ dénote le module des polynômes de degré au plus n sur l'anneau des entiers p-adiques $\mathbb{Z}_p$.

Soit φ un morphisme entre deux $\mathbb{Z}$-fibrés hermitiens $\overline{E}$ et $\overline{F}$. Si K est un corps, on note E_K le fibré $E \otimes K$ et φ_K le morphisme déduit de φ par extension des scalaires à K. Enfin, on note $|| \varphi ||_p$ la norme d'opérateur de $\varphi_{\mathbb{Q}_p}$ et $|| \varphi ||_{\mathbb{C}}$ la norme de l'opérateur $\varphi_{\mathbb{C}}$.

Convention Sur $\mathbb{Q}$ on définit la valeur absolue p-adique $|\cdot|_p$ par la convention $|p|_p = p^{-1}$.

Définition 38 Soient $\overline{E}$ est un $\mathbb{Z}$-fibré hermitien de rang 1 et s une section globale non nulle de E. On définit le *degré arithmétique* et on note

$$\widehat{\deg}\ \overline{E} = -\sum_{p \text{ premiers}} \log ||\ s\ ||_p - \log ||\ s\ ||_{\mathbb{C}}\ .$$

La formule du produit assure que cette définition est indépendante du choix de s.
Si $\overline{E}$ est un $\mathbb{Z}$-fibré hermitien de rang supérieur r, on pose

$$\widehat{\deg}\ \overline{E} = \widehat{\deg}\ \left(\ \overline{\bigwedge^{\max} E}\ \right),$$

où on a muni $\bigwedge^{\max} E$ de la métrique déterminant

$$\forall (x_1 \wedge \ldots \wedge x_r, y_1 \wedge \ldots \wedge y_r) \quad \langle (x_1 \wedge \ldots \wedge x_r), (y_1 \wedge \ldots \wedge y_r) \rangle := \det\left(\langle x_i, y_j \rangle_{1 \leq i,j \leq r}\right).$$

Définition 39 Soit $\overline{E}$ un $\mathbb{Z}$-fibré hermitien, on définit sa *pente* et on note

$$\widehat{\mu}\left(\overline{E}\right) = \frac{\widehat{\deg}\ \overline{E}}{\text{rg } E}.$$

Ceci permet de définir la *pente maximale* d'un $\mathbb{Z}$-fibré hermitien $\overline{E}$,

$$\widehat{\mu}_{\max}\left(\overline{E}\right) = \max_{\{0\} \subsetneq F \subset E} \widehat{\mu}\left(\overline{F}\right),$$

où on a muni les sous–fibrés $F \subset E$ de la métrique induite par restriction de E à F.

4.2.2 Un morphisme pour l'inégalité des pentes

On se donne un entier algébrique $x \in \overline{\mathbb{Z}}$ de degré D, de polynôme minimal Δ_{-1} unitaire à coefficients entiers. Si p_k est un nombre premier avec $k \geq 0$, on note Δ_{p_k} (ou Δ_k ou Δ_p s'il n'y a aucune confusion possible) le polynôme minimal (qui est unitaire à coefficients entiers) de l'entier algébrique x^{p_k}. Quitte à faire un petit raisonnement par récurrence, on peut supposer que tous les x^p que l'on considère sont de même degré que x :

Lemme 13 *Soit f une fonction de $\mathbb{N}$ dans $\mathbb{R}$, strictement positive et décroissante. Si on a $h(x) \geq \frac{f(D)}{D}$ sous l'hypothèse $[\forall p$ premier $\mathbb{Q}(x^p) = \mathbb{Q}(x)]$. Alors, la même inégalité est vraie sans cette hypothèse.*

Démonstration : On raisonne par récurrence sur $D = [\mathbb{Q}(x) : \mathbb{Q}]$. Si $\mathbb{Q}(x^p) \subsetneq \mathbb{Q}(x)$, alors, x est racine de $X^p - x^p \in \mathbb{Q}(x^p)$. On a alors, deux possibilités : soit ce polynôme est irréductible (cas (i)), soit il ne l'est pas (cas (ii)).
Dans le cas (i), on a $[\mathbb{Q}(x) : \mathbb{Q}(x^p)] = p$ et l'hypothèse de récurrence donne

$$h(x^p) \geq \frac{1}{[\mathbb{Q}(x^p) : \mathbb{Q}]} f([\mathbb{Q}(x^p) : \mathbb{Q}]).$$

Ainsi, on a

$$h(x) = \frac{1}{p}h(x^p) \geq \frac{1}{p[\mathbb{Q}(x^p) : \mathbb{Q}]} f([\mathbb{Q}(x^p) : \mathbb{Q}]) = \frac{1}{D} f([\mathbb{Q}(x^p) : \mathbb{Q}]),$$

et on conclut par décroissance de f.
Dans le cas (ii), alors, on sait que $x^p \in [\mathbb{Q}(x^p)]^p$. Ainsi, il existe $y \in \mathbb{Q}(x^p)$ tel que $y^p = x^p$. Donc, il existe ζ une racine p-ième de l'unité, telle que $y = \zeta x$. Finalement, on en déduit

$$h(x) = h(y) \geq \frac{1}{[\mathbb{Q}(x^p) : \mathbb{Q}]} f([\mathbb{Q}(x^p) : \mathbb{Q}]) \geq \frac{1}{D} f([\mathbb{Q}(x^p) : \mathbb{Q}]),$$

et on conclut là encore par décroissance de f. □

Notons que ce lemme permet de faire l'économie du lemme combinatoire de Dobrowolski. On suppose désormais que $[\mathbb{Q}(x) : \mathbb{Q}(x^p)] = 1$. Par ailleurs, comme x n'est pas une racine de l'unité, on a $h(x) \neq h(x^p)$ donc, pour tous plongements $\sigma,\ \sigma' : K \hookrightarrow \mathbb{C}$, on a $\sigma(x) \neq \sigma'(x^p)$.

Soient L, T et N des paramètres entiers à fixer ultérieurement.

Si Δ est un polynôme de $A^L[X]$, on note (Δ) le sous-A-module de $A^L[X]$ "engendré" par Δ. Plus précisément, on pose

$$(\Delta) = \left\{ P \in A^L[X] / \ \ \exists Q \in A^L[X] \ \ P = \Delta Q \ \ \right\}.$$

Par ailleurs, on note $\mathcal{P}_N = \left\{ p \in [\![\frac{N}{2}, N [\![\ \Big/ \ p \text{ premier} \right\}$, qui est non vide par le Postulat de Bertrand, et on définit deux $\mathbb{Z}$-fibrés :

$$E = \mathbb{Z}^L[X] \simeq \mathbb{Z}^{L+1}, \quad \text{et,} \quad F = \left(E \Big/ (\Delta_{-1}^T) \right) \times \prod_{p \in \mathcal{P}_N} \left(E \Big/ (\Delta_p) \right).$$

Remarque 17 Dans F, on veut quotienter par un module (Δ_{-1}^T) non trivial afin de pouvoir extrapoler dans le corollaire 9. Pour cela, il faut nécessairement que l'inégalité $DT \leq L$ soit vérifiée. On suppose désormais cette inégalité vérifiée.

Remarque 18 Comme Δ_{-1} et Δ_p sont des polynômes unitaires dans $\mathbb{Z}[X]$, on peut effectuer la division euclidienne par Δ_{-1} et Δ_p. Ceci permet d'identifier F et le fibré trivial

$$\mathbb{Z}^{DT + \sum_{p \in \mathcal{P}_N} \deg \Delta_p}.$$

On définit maintenant le morphisme entre $\mathbb{Z}$-fibrés pour lequel on veut appliquer l'inégalité des pentes.

$$\begin{aligned} \varphi : E &\to F \\ P &\mapsto \left(R_{-1}\, ,\, (R_p)_{p \in \mathcal{P}_N} \right) \end{aligned}$$

où R_{-1} est le reste de la division euclidienne par Δ_{-1}^T et où pour tout p, R_p est le reste de la division euclidienne par Δ_p.

4.3 "Lemme de zéros"

Pour appliquer l'inégalité des pentes, il faut que le morphisme φ soit injectif. On note n le cardinal de l'ensemble $\mathcal{P}_N = \{p_1, \cdots, p_n\}$.

Lemme 14 *Si $L < D(T+n)$, alors, le morphisme φ est injectif.*

Démonstration : En effet, dans le cas contraire, un polynôme non nul dans le noyau aurait strictement plus de zéros comptés avec multplicité que son degré. □

Or pour tout N assez grand, le théorème des nombres premiers nous donne

$$n = \sum_{p \in \mathcal{P}_N} 1 \geq \frac{N}{4 \ln N}.$$

On suppose désormais que L vérifie l'encadrement $DT < L < D\left(T + \frac{N}{4 \ln N}\right)$.

4.4 Inégalité des pentes

4.4.1 La filtration

On définit la filtration de F

$$F_n = \{0\} \subset F_{n-1} \subset \cdots \subset F_0 \subset F_{-1} = F, \text{ où,}$$

$$F_0 = \left\{ (P_1, (P_p)_{p \in \mathcal{P}_N}) \ \middle/ \ P_1 = 0 \right\} \text{ et,}$$

$$\forall k \in [\![1, n]\!], \quad F_k = \left\{ (P_1, (P_p)_{p \in \mathcal{P}_N}) \ \middle/ \ P_1 = 0,\ P_{p_1} = 0,\ \cdots,\ P_{p_k} = 0 \right\}.$$

On pose alors pour tout entier k entre 0 et $n-1$,

$$G_{-1} = F_{-1} \Big/ F_0 \simeq \mathbb{Z}^{T \deg \Delta_{-1}} \simeq \mathbb{Z}^{DT}, \quad G_k = F_k \Big/ F_{k+1} \simeq \mathbb{Z}^{\deg \Delta_k} \simeq \mathbb{Z}^D, \quad \text{et,}$$

$$E_{-1} = E, \quad E_k = \varphi^{-1}(F_k).$$

On munit le fibré $E \simeq \mathbb{Z}^{L+1}$ de la métrique du fibré trivial et les sous-fibrés E_k des métriques de restriction de celle de $\overline{E}$. De même, on munit les fibrés G_k des métriques triviales.

Pour k compris entre -1 et $n-1$, on note $\varphi_k : \overline{E_k} \to \overline{G_k}$ et $\widetilde{\varphi_k} : \overline{E_k/E_{k+1}} \to \overline{G_k}$ les morphismes déduits de φ, où E_k/E_{k+1} est muni de la métrique quotient.

Remarque 19 On a, $E_0 = \left\{ P \in E \,\middle/\, P \text{ est nul à un ordre } \geq T \text{ en } x \right\}$ et pour tout entier $k \in [\![1, n]\!]$,

$$E_k = \left\{ P \in E \,\middle/\, P \text{ nul à un ordre } \geq T \text{ en } x, \text{ nul en } x^{p_1}, \cdots, \text{ nul en } x^{p_k} \right\}.$$

Une autre manière de dire, consiste à dire que $E_0 = (\Delta_{-1}^T)$, et $\forall k \geq 0$, $E_k = (\Delta_{-1}^T \Delta_1 \dots \Delta_k)$.

4.4.2 L'inégalité des pentes

Avec nos notations, en notant $\widehat{\deg}$ le degré arithmétique et $\widehat{\mu}_{\max}$ la pente maximale, on peut énoncer une version de l'inégalité des pentes de J.-B. Bost sous la forme :

$$\begin{aligned} \widehat{\deg}_n\, \overline{E} \;\leq\; & \textstyle\sum_{k=-1}^{n-1} \mathrm{rg}\,(E_k/E_{k+1}) \left(\widehat{\mu}_{\max}(\overline{G_k}) + \sum_{p \text{ premiers}} \log \,||\, \varphi_k \,||_p \right) \\ & + \textstyle\sum_{k=-1}^{n-1} \log \,||\, \bigwedge^{\max} \widetilde{\varphi_k} \,||_{\mathbb{C}} \,. \end{aligned} \tag{4.1}$$

C'est le théorème 19 du chapitre 1. Il s'agit essentiellement de l'inégalité (**4.14**) de la *Proposition* **4.6.** de [16] dans laquelle on n'a pas remplacé les termes $||\, \bigwedge^r \varphi^i \,||$ par $||\, \varphi^i \,||^r$ aux places archimédiennes.

Il nous reste maintenant à calculer les différents termes intervenant dans cette inégalité.

4.4.3 Évaluation de $\mathrm{rg}(E_k)$

Par construction, on sait que $E_k/E_{k+1} \hookrightarrow G_k$. Par ailleurs, on calcule facilement le rang de E_k/E_{k+1} :

Si $k = -1$, $\mathrm{rg}(E_k/E_{k+1}) = DT$.

Soit $k_0 = \left[\frac{L}{D} - T\right]$. Pour $k < k_0$, on a

$$\mathrm{rg} E_k = L + 1 - D(T + k),$$

et pour $k > k_0$, on a

$$\mathrm{rg} E_k = 0.$$

4.4.4 Calcul des degrés et des pentes

Le fibré hermitien $\overline{E}$ ainsi que les fibrés hermitiens $\overline{G_k}$ sont isomorphes (comme fibrés hermitiens) à des fibrés triviaux, donc, pour tout entier k entre -1 et $n-1$,

$$\widehat{\deg}\,(\overline{E}) = 0, \text{ et, } \widehat{\mu}_{\max}(\overline{G_k}) = 0.$$

4.4.5 Calcul des $|| \varphi_k ||_p$: l'extrapolation

Dans ce paragraphe, on se donne p un nombre premier et k un entier compris entre -1 et $n-1$. On veut obtenir une majoration de $|| \varphi_k ||_p$.

Calcul des $|| \varphi_k ||_l$, l premier quelconque

Soient $k \geq 0$ et $P \in \mathbb{Z}_l^L[X]$ ($\mathbb{Z}_l$-module des polynômes de degré inférieur à L) de norme 1, i.e., tel que

$$\text{si } P = \sum a_i X^i, \quad \text{alors,} \quad \max_i \mid a_i \mid_l = 1.$$

Dans ce cas, en écrivant la division euclidienne de P par Δ_k, $P = \Delta_k Q_{p_k} + R_{p_k}$, on a

$$|| \varphi_k(P) ||_l = || R_{p_k} ||_l \leq 1, \text{ car } R_{p_k} \text{ est à coefficients } l\text{-entiers.}$$

Le même résultat vaut pour $|| \varphi_{-1}(P) ||_l$. Ainsi, on a

$$\forall\ k \in [\![-1, n-1]\!], \quad || \varphi_k ||_l \leq 1.$$

Raffinement pour $l = p_k$

On considère comme précédemment k compris entre 0 et $n-1$ et on prend cette fois $l = p_k$. On va donner une majoration plus fine de $|| \varphi_k ||_{p_k}$ en utilisant le fait que φ_k est défini sur les polynômes nuls en x à un ordre supérieur à T. On va pour cela énoncer un lemme du type "petit théorème de Fermat".

Lemme 15 *Soient p un nombre premier, Δ_{-1} le polynôme minimal de x et Δ_p le polynôme minimal (supposé unitaire mais de degré éventuellement inférieur à celui de Δ_{-1}) de x^p. Alors, il existe un polynôme $A \in \mathbb{Z}[X]$ et un polynôme $R \in \mathbb{Z}^{\deg \Delta_p - 1}[X]$, tel que*

$$\Delta_{-1} = A\Delta_p + pR,$$

autrement dit, le reste de la division euclidienne de Δ_{-1} par Δ_p est divisible par p.

Démonstration : On commence par démontrer le lemme dans le cas où Δ_p est de même degré que Δ_{-1}. Dans ce cas,

$$\Delta_{-1}(X) = \prod_{\sigma : \mathbb{Q}(x) \hookrightarrow \mathbb{C}} (X - \sigma(x)), \quad \text{et} \quad \Delta_p(X) = \prod_{\sigma : \mathbb{Q}(x) \hookrightarrow \mathbb{C}} (X - \sigma(x)^p).$$

On sait (par division euclidienne dans $\mathbb{Z}[X]$ pour des polynômes unitaires) qu'il existe $S \in \mathbb{Z}[X]$ de degré inférieur à $D-1$ tel que $\Delta_{-1} = \Delta_p + S$. On va calculer S et montrer qu'il est en fait de la forme pR avec $R \in \mathbb{Z}[X]$. En notant x_i pour $i \in [\![1, D]\!]$ les images

de x par tous les $\mathbb{Q}(x)$-plongements dans $\mathbb{C}$ et en notant $s_i(X_1, \ldots, X_D)$ la i-ième fonction symétrique élémentaire, on a (dans $\mathbb{Z}[X]$)

$$\Delta_p(X) = \Delta_{-1}(X) + \sum_{i=0}^{D-1} \left(s_{D-i}(x_1^p, \ldots, x_D^p) - s_{D-i}(x_1, \ldots, x_D)\right) X^i.$$

Ainsi, pour conclure, il reste à voir que

$$\forall i \in [\![0, D-1]\!], \quad s_{D-i}(x_1^p, \ldots, x_D^p) - s_{D-i}(x_1, \ldots, x_D) \in p\mathbb{Z}.$$

Or Δ_{-1} est à coefficients entiers, donc $s_{D-i}(x_1, \ldots, x_D)$ est dans $\mathbb{Z}$ et est donc congru à $A = (s_{D-i}(x_1, \ldots, x_D))^p$ modulo p par le petit théorème de Fermat. Ainsi, il suffit de voir que $s_{D-i}(x_1^p, \ldots, x_D^p)$ est congru à A modulo p. En développant A avec la formule du multinôme, on obtient

$$A = s_{D-i}(x_1^p, \ldots, x_D^p) + pf(x_1, \ldots, x_D),$$

où $f(X_1, \ldots, X_D)$ est un polynôme symétrique à coefficients entiers. Ainsi, il s'exprime comme un polynôme à coefficients entiers en les fonctions symétriques élémentaires et donc (comme $s_{D-i}(x_1^p, \ldots, x_D^p) \in \mathbb{Z}$), on en déduit que le nombre $f(x_1, \ldots, x_D)$ appartient à $\mathbb{Z}$, ce qui conclut la preuve dans le cas où $\deg \Delta_p = \deg \Delta_{-1}$.
Dans le cas général, notons $P = \prod_{\sigma:\mathbb{Q}(x)\hookrightarrow\mathbb{C}}(X - \sigma(x)^p)$. Il existe $A_1 \in \mathbb{Z}[X]$ tel que $A_1\Delta_p = P$. Par le premier cas, on sait que $\Delta_{-1} = P + pR_P$, donc $\Delta_{-1} = A_1\Delta_p + pR_P$ et on conclut en effectuant la division euclidienne de R_P par Δ_p. □

Corollaire 8 *Soient $k \neq -1$ et $P \in \mathbb{Z}[X]$ tel que $P = \Delta_{-1}^T Q$ avec $Q \in \mathbb{Z}[X]$. En notant P_{p_k} le reste de la division euclidienne de P par Δ_k, on a*

$$\exists R \in \mathbb{Z}[X] \quad \textit{tel que} \quad P_{p_k} = p^T R.$$

Démonstration : Par le lemme il existe un polynôme $B \in \mathbb{Z}[X]$ tel que

$$P = \Delta_{-1}^T Q = (A\Delta_k + pR)^T Q = B\Delta_k + p^T R^T Q.$$

On effectue maintenant la division euclidienne de $R^T Q$ par Δ_k pour conclure. □

Corollaire 9 *Soient $k \neq -1$ tel que $E_k \neq \{0\}$ et $P \in E_k \otimes \mathbb{Z}_l$ tel que $P = \Delta_{-1}^T Q$ avec $Q \in \mathbb{Z}_l[X]$. En notant P_{p_k} le reste de la division euclidienne par Δ_k, on a*

$$|| \varphi_k ||_{p_k} = \max_{||P||_{p_k}=1} || \varphi_k(P) ||_{p_k} = \max_{||P||_{p_k}=1} || P_{p_k} ||_{p_k} \leq p_k^{-T}.$$

Démonstration : On applique le corollaire précédent. □

En injectant les estimations précédentes, on peut réécrire l'inégalité des pentes sous la forme

Proposition 15 *Avec les notations précédentes, on a pour tout entier N assez grand et dès que $D(T+n) > L \geq 2DT$,*

$$\frac{LT}{4}\log N \leq \sum_{k=-1}^{n-1} \log || \bigwedge^{max} \widetilde{\varphi_k} ||_{\mathbb{C}} .$$

Démonstration : En effet, si $E_k \neq 0$, on a $\sum_p \log || \varphi_k ||_p \leq -T \log p_k \leq -\frac{T}{2}\log N$ et si $k=-1$, $\log || \varphi_k ||_p \leq 0$. De plus, un processus téléscopique donne

$$-\sum_{k=0}^{n-1} \mathrm{rg}\,(E_k/E_{k+1})\,\frac{T}{2}\log N \leq -\mathrm{rg}\ E_0 \frac{T}{2}\log N$$
$$\leq -(L+1-DT)\frac{T}{2}\log N \leq -\frac{LT}{4}\log N.$$

Ainsi, en sommant sur $k \geq -1$, on obtient

$$\sum_{k=-1}^{n-1} \mathrm{rg}\,(E_k/E_{k+1}) \left(\widehat{\mu}_{\max}(\overline{G_k}) + \sum_{p \text{ premiers}} \log || \varphi_k ||_p \right) \leq -\frac{LT}{2}\log N.$$

En appliquant l'inégalité des pentes (4.1) on obtient le résultat. □

4.5 Calcul d'un bon majorant de $|| \bigwedge^{\mathbf{max}} \widetilde{\varphi_k} ||_{\mathbb{C}}$

On va maintenant s'attacher à donner une "bonne" majoration pour les normes complexes des opérateurs $\bigwedge^{\max} \widetilde{\varphi_k}$. Il faudrait à priori distinguer deux cas : $k=-1$ et $k \neq -1$. En fait on peut les traiter ensembles, le cas $k=-1$ étant essentiellement une généralisation du cas $k \neq -1$. Dans la suite, on pose $T_k = T$ si $k=-1$ et $T_k = 1$ sinon. De même, on notera $N_k = 1$ si $k=-1$ et $N_k = N$ sinon. Par ailleurs, k étant fixé et en posant $p_{-1}=1$, on notera $\{\alpha_i\}_{1\leq i\leq D}$ les différentes racines de $\Delta_k^{T_k}$. Avec ces notations, on va montrer la majoration

Proposition 16 *En notant $C = \frac{1}{2}DT_k \log 2D + DT_k^2 \log(L+T_k) + \frac{1}{2}DT_k \log(L+1) + \frac{1}{2}DT_k \log T_k$ pour tout $k \geq -1$, on a*

$$\log || \bigwedge^{\max} \widetilde{\varphi_k} ||_{\mathbb{C}} \leq C + 2LT_k D N_k h(x).$$

La suite de cette partie est consacrée à la preuve de cette proposition.

4.5.1 Une petite réduction

Soit $k \geq -1$. Dans toute la suite, on cherche une majoration de la norme de

$$\bigwedge \widetilde{\varphi_k} : \bigwedge (E_k/E_{k+1}) \to \bigwedge G_k.$$

On a le carré commutatif

$$\begin{array}{ccc} E_k & \xrightarrow{\quad i \quad} & \mathbb{C}^L[X] \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ E_k/E_{k+1} & \xrightarrow[\quad i \quad]{} & \mathbb{C}^L[X]/(\Delta_k^{T_k}) \end{array}$$

où les deux flèches verticales sont co-isométriques et la flèche horizontale du haut est isométrique. Donc la flèche horizontale du bas l'est aussi. Dans la suite de cette partie, on notera donc (abusivement) $\widetilde{\varphi_k}$ le morphisme de $\mathbb{C}^L[X]/(\Delta_k^{T_k})$ dans G_k.

4.5.2 Preuve de la proposition 16

Le polynôme $\Delta_k^{T_k}$ est un polynôme scindé sur $\mathbb{C}$, toutes ses racines ayant multiplicité T_k. On peut ainsi écrire $\Delta_k^{T_k}(X) = \prod_{i=1}^{D}(X-\alpha_i)^{T_k}$ où les α_i sont des complexes deux à deux distincts. On note

$$\pi : \mathbb{C}^L[X] \twoheadrightarrow \mathbb{C}^L[X]/(\Delta_k^{T_k}), \quad \text{et} \quad \pi_i : \mathbb{C}^L[X] \twoheadrightarrow \mathbb{C}^L[X]/(X-\alpha_i)^{T_k},$$

pour tout entier i compris entre 1 et D, les projections canoniques. On définit maintenant l'opérateur "restes Chinois"

$$\mathrm{Ch}_D : \mathbb{C}^L[X]/(\Delta_k^{T_k}) \to \prod_{i=1}^{D} \mathbb{C}^L[X]/(X-\alpha_i)^{T_k}$$

par la formule, $\mathrm{Ch}_D(\pi(P)) = (\pi_1(P), \ldots, \pi_D(P))$ pour tout $P \in \mathbb{C}^L[X]$. On définit également l'opérateur d'évaluation en les $(\alpha_i)_{1\leq i\leq D}$,

$$\mathrm{Eval} : \prod_{i=1}^{D} \mathbb{C}^L[X]/(X-\alpha_i)^{T_k} \to \prod_{i=1}^{D} \mathbb{C}^{T_k}$$

qui envoie $(\pi_i(P_i))_{1\leq i\leq D}$ sur $((P_i(\alpha_i), \ldots, P_i^{(T_k-1)}(\alpha_i))_{1\leq i\leq D}$. Enfin, on définit l'isomorphisme "de Lagrange",

$$\mathrm{Lag}_D : \prod_{i=1}^{D} \mathbb{C}^{T_k} \to \mathbb{C}^{T_k D-1}[X],$$

qui à un DT_k-uplet $(x_1, \ldots, x_{T_k}, x_{T_k+1}, \ldots, x_{DT_k})$ associe l'unique polynôme R de degré inférieur à $DT_k - 1$ et tel que $R^{(k-1)}(\alpha_i) = x_{T_k(i-1)+k}$ pour tout $i \in [\![1, D]\!]$ et tout $k \in [\![1, T_k]\!]$.

On a alors le diagramme commutatif

$$\begin{array}{ccccc} \mathbb{C}^L[X]/(\Delta_k^{T_k}) & & \xrightarrow{\qquad\widetilde{\varphi_k}\qquad} & & \\ \downarrow{\scriptstyle \mathrm{Ch}_D} & & & & \\ \prod_{i=1}^D E_i^{\mathrm{quot}} & \xrightarrow[\mathrm{Eval}]{\simeq} & \prod_{i=1}^D \mathbb{C}^{T_k} & \xrightarrow[\mathrm{Lag}_D]{\simeq} & \mathbb{C}^{T_k D-1}[X] \end{array}$$

où $E_i^{\mathrm{quot}} = \mathbb{C}^L[X]/(X-\alpha_i)^{T_k}$ est muni de la métrique quotient de celle sur $\mathbb{C}^L[X]$ et où $\mathbb{C}$ est muni de la métrique hermitienne naturelle. Par ailleurs on met sur le produit, la métrique somme directe

$$\forall (x_1,\ldots,x_D,y_1,\ldots,y_D) \quad \langle (x_1,\ldots,x_D),(y_1,\ldots,y_D)\rangle := \sum_{i=1}^D \langle x_i,y_i\rangle_i.$$

Enfin on met sur les puissances extérieures maximales (D-ièmes) de tous ces fibrés la métrique déterminant déjà définie.

Majorant de $||\bigwedge \mathrm{Ch}_D||$

On se contente ici d'une majoration grossière.

Lemme 16 $\log ||\bigwedge \mathrm{Ch}_D|| \leq \frac{1}{2} dT_k \log D$.

Démonstration : On utilise l'inégalité $||\bigwedge \mathrm{Ch}_D|| \leq ||\mathrm{Ch}_D||^{DT_k}$. Par définition Ch_D n'est autre que l'application définie par $\mathrm{Ch}_D(\pi(P)) = (\pi_1(P),\ldots,\pi_D(P))$ pour tout $P \in \mathbb{C}^L[X]$. En notant $||\cdot||_i$ la norme sur l'espace E_i^{quot} et $||\cdot||_2$ celle sur $\mathbb{C}^L[X]$, on a

$$\begin{aligned} \forall P \in \mathbb{C}^L[X] \quad ||\mathrm{Ch}_D(\pi(P))||^2 &= \sum_{i=1}^D ||\pi_i(P)||_i^2 = \sum_{i=1}^D \inf_{\pi_i(Q)=0} ||P+Q||_2^2 \\ &\leq \sum_{i=1}^D \inf_{\pi(Q)=0} ||P+Q||_2^2 \leq D\,||\pi(P)||^2 . \end{aligned}$$

En passant à la racine carré puis au log, on en déduit la majoration voulue. □

Majorant $||\bigwedge \mathrm{Lag}_D||$

Lemme 17 $\log ||\bigwedge \mathrm{Lag}_D|| \leq 0$.

Démonstration : L'opérateur $\bigwedge \mathrm{Lag}_D$ est une application linéaire entre $\mathbb{C}$-espaces vectoriels de dimension 1. En particulier, si g_D est l'isomorphisme réciproque de Lag_D et si $(\wedge_{i=1}^{T_k} R_i) \wedge \ldots \wedge (\wedge_{i=1}^{T_k} R_{T_k(D-1)+i})$ est non nul dans $\bigwedge^{T_k D} \mathbb{C}^{T_k D-1}[X]$, on a

$$||\bigwedge \mathrm{Lag}_D|| = ||\bigwedge g_D||^{-1} = \frac{||(\wedge_{i=1}^{T_k} R_i) \wedge \ldots \wedge (\wedge_{i=1}^{T_k} R_{T_k(D-1)+i})||}{||(\wedge_{i=1}^{T_k} g_D(R_i)) \wedge \ldots \wedge (\wedge_{i=1}^{T_k} g_D(R_{T_k(D-1)+i}))||}.$$

On prend par exemple pour tout i entier dans $[\![1, DT_k]\!]$, $R_i = X^{i-1}$. On obtient ainsi une base orthonormée de $\mathbb{C}^{T_k D-1}[X]$, donc

$$|| \bigwedge \mathrm{Lag}_D ||=|| (\wedge_{i=1}^{T_k} g_D(R_i)) \wedge \ldots \wedge (\wedge_{i=1}^{T_k} g_D(R_{T_k(D-1)+i})) ||^{-1}.$$

En notant $[\,\cdot\,]$ la partie entière on constate que

$$|| (\wedge_{i=1}^{T_k} g_D(R_i)) \wedge \ldots \wedge (\wedge_{i=1}^{T_k} g_D(R_{T_k(D-1)+i})) ||= \left| \det \left(\left(\alpha^{j-1}_{\left[\frac{i-1}{T_k}\right]+1} \right)_{1\leq i,j\leq DT_k} \right) \right|^2.$$

Or $\det \left(\left(\alpha^{j-1}_{\left[\frac{i-1}{T_k}\right]+1} \right)_{1\leq i,j\leq DT_k} \right)$ est une expression polynômiale symétrique en les α_i à coefficients entiers. Donc on peut l'écrire comme une expression polynmiale à coefficients entiers, en les fonctions symétriques émentaires en les α_i. Or les α_i sont les racines d'un polynôme unitaire à coefficients entiers. Par conséquent en prenant le carré du module on obtient un nombre entier positif, non nul car on est parti d'une base. On conclut en passant au log. □

Majorant de $|| \bigwedge \mathrm{Eval} ||$

Notons $\mathrm{Eval}_i : E_i^{\mathrm{quot}} \to \mathbb{C}^{T_k}$ l'application définie par

$$\mathrm{Eval}_i(\pi_i(P)) = (P^{(k-1)}(\alpha_i))_{1\leq k\leq T_k}.$$

Comme le morphisme Eval est le morphisme diagonal

$$\mathrm{diag}(\bigwedge^{T_k} \mathrm{Eval}_1, \ldots, \bigwedge^{T_k} \mathrm{Eval}_D),$$

on a le résultat suivant :

Lemme 18 *On a l'égalité de normes*

$$|| \bigwedge \mathrm{Eval} ||= \prod_{i=1}^{D} || \bigwedge^{T_k} \mathrm{Eval}_i ||.$$

Démonstration : On rappelle que la métrique sur le produit tensoriel $E \otimes F$ de deux fibrés hermitiens est définie par

$$\langle x \otimes y, z \otimes t \rangle = \langle x, z \rangle_E \cdot \langle y, t \rangle_F.$$

Avec cette définition, on a l'isomorphisme isométrique

$$\bigwedge_{k=1}^{DT_k} \left(\bigoplus_{i=1}^{D} E_i \right) \simeq \bigotimes_{k=1}^{D} \left(\bigwedge_{i=1}^{T_k} E_i \right),$$

valable pour tout espace hermitien E_i de rang T_k. $\square$

Désormais on écrira $\bigwedge$ pour $\bigwedge^{T_k}$. Il reste à calculer la norme de $\bigwedge \mathrm{Eval}_i$ pour tout $i \in [\![1, D]\!]$. Soit donc un tel $i \geq 1$. L'application $\bigwedge \mathrm{Eval}_i$ est un morphisme entre espaces vectoriels de dimension 1, donc

$$\forall g_1 \wedge \ldots \wedge g_{T_k} \in \bigwedge E_i^{\mathrm{quot}} - \{0\},\ || \bigwedge \mathrm{Eval}_i || = \frac{|| \mathrm{Eval}_i(g_1) \wedge \ldots \wedge \mathrm{Eval}_i(g_{T_k}) ||}{|| g_1 \wedge \ldots \wedge g_{T_k} ||}.$$

Par ailleurs, la norme quotient sur E_i est, par définition, la norme qui rend isométrique l'isomorphisme entre E_i et l'orthogonal $\left((X-\alpha_i)^{T_k}\right)_L^{\perp}$, pour la norme hermitienne standard, de $(X-\alpha_i)^{T_k}$ dans $\mathbb{C}^L[X]$.

Lemme 19 *La famille de polynômes*

$$\left\{ g_l = \sum_{v=0}^{L} \binom{v+l}{v} \overline{\alpha_i}^v X^v \right\}_{0 \leq l \leq T_k - 1}$$

constitue une base de $\left((X-\alpha_i)^{T_k}\right)_L^{\perp}$.

Démonstration : Il y a deux choses à voir : tout d'abord que les g_l sont effectivement dans l'orthogonal de $(X-\alpha_i)^{T_k}$ et ensuite que ces T_k éléments forment une famille libre. Soit $l \in [\![0, T_k - 1]\!]$. Dire que $g_l \in \left((X-\alpha_i)^{T_k}\right)_L^{\perp}$ équivaut à dire que pour tout $u \in [\![0, L - T_k]\!]$

$$g_l \perp (X-\alpha_i)^{T_k} X^u \qquad \text{condition } (\star_{u,l}).$$

Ceci étant dit, un simple calcul permet de conclure :

$$\begin{aligned}
(\star_{u,l}) &\iff \sum_{v=0}^{T_k} (-1)^{T_k - v} \frac{(v+u+l)!}{(v+u)!} \binom{T_k}{v} \overline{\alpha_i}^{v+u} \overline{\alpha_i}^{T_k - v} = 0 \\
&\iff \overline{\alpha_i}^{u+T_k} \sum_{v=0}^{T_k} (-1)^{T_k - v} \frac{(v+u+l)!}{(v+u)!} \binom{T_k}{v} = 0 \\
&\iff \sum_{v=0}^{T_k} \binom{T_k}{v} (-1)^{T_k - v} (v+u+l) \times \ldots \times (v+u+1) = 0.
\end{aligned}$$

Soit $f_{u,l}(x) = x^{u+l} \sum_{v=0}^{T_k} \binom{T_k}{v} (-1)^{T_k - v} x^v = x^{u+l}(x-1)^{T_k}$. Alors 1 est racine de $f_{u,l}$ d'ordre T_k et la condition $(\star_{u,l})$ équivaut à dire que $f_{u,l}^{(l)}(1) = 0$. Donc $(\star_{u,l})$ est vraie ce qui prouve que les g_l sont dans l'orthogonal.

Il reste à voir que la famille $\{g_l\}_{0 \leq l \leq T_k - 1}$ est une famille libre. Pour cela, on écrit dans la base canonique la matrice M dont le l-ieme vecteur colonne est formé par g_l. Il suffit de

montrer que M admet une matrice carrée de taille $T_k \times T_k$ dont le déterminant est non nul. Or $M = \left(\binom{v+l}{v}\overline{\alpha_i}^v\right)_{\substack{0\le v\le L\\ 0\le l\le T_k-1}}$. Montrons que la matrice $A = \left(\binom{v+l}{v}\overline{\alpha_i}^v\right)_{0\le v,l\le T_k-1}$ est inversible. En factorisant la v-ieme ligne par $\overline{\alpha_i}^v$ pour tout v dans $[\![0, T_k-1]\!]$, on en conclut que A est inversible si et seulement si $B = \left(\binom{v+l}{v}\right)_{0\le v,l\le T_k-1}$ l'est. Or c'est un exercice de voir que $\det B = 1 \neq 0$. (on remplace la ligne L_{v+1} par $L_{v+1} - L_v$ en commençant par la dernière ligne et en utilisant la formule

$$\binom{v+1+l}{l} - \binom{v+l}{l} = \binom{v+l}{l-1}.$$

On effectue alors un développement selon la première colonne et on se ramène au déterminant de $C = \left(\binom{v+l}{l-1}\right)_{1\le v,l\le T_k-1}$. On itère ceci jusqu'à aboutir au déterminant de la matrice

$$\left(\binom{v+l}{l-(T_k-1)}\right)_{T_k-1\le v,l\le T_k-1}$$

qui vaut 1). Ceci conclut. □

Lemme 20 *On a la majoration*

$$||\bigwedge \mathrm{Eval}_i||^2 \le ||\ g_0 \wedge \ldots \wedge g_{T_k-1}\ ||^{-2}_{\mathrm{quot}}\ (L+T_k)^{2{T_k}^2} {T_k}^{T_k} (L+1)^{T_k} \max\{1, |\alpha_i|\}^{4LT_k}.$$

Démonstration : On veut majorer $|\det A_i|$, où

$$A_i = \left(\sum_{s=0}^{T_k-1} g_u^{(s)}(\alpha_i)\overline{g_v^{(s)}(\alpha_i)}\right)_{0\le u,v\le T_k-1}.$$

Comme $A_i = (a_{uv})$ est une matrice hermitienne définie positive, on a

$$|\det A_i| \le \prod_{u=0}^{T_k-1} a_{uu}.$$

En remplaçant ceci par les valeurs explicites de a_{uu}, on obtient

$$\begin{aligned}|\det A_i| &\le \prod_{u=0}^{T_k-1}\sum_{s=0}^{T_k-1} g_u^{(s)}(\alpha_i)\overline{g_u^{(s)}(\alpha_i)}\\ &\le \prod_{u=0}^{T_k-1}\sum_{s=0}^{T_k-1} \left|g_u^{(s)}(\alpha_i)\right|^2\end{aligned}$$

Or

$$|g_u^{(s)}(\alpha_i)|^2 \le \left(\sum_{r=s}^{L} \frac{(r+u)\times\ldots\times(u+1)}{(r-s)!}|\alpha_i^{2r-s}|\right)^2. \tag{4.2}$$

Finalement, il reste à majorer convenablement le produit de factorielles. Pour cela on distingue deux cas :

si $r > T_k$, alors

$$\begin{aligned}\frac{(r+u)\times\ldots\times(u+1)}{(r-s)!} &\leq \frac{(r+T_k)\times\ldots\times(T_k+1)}{(r-T_k)!}\\ &\leq \frac{(r+T_k)\times\ldots\times(T_k+1)}{(r-T_k)\times\cdots\times(T_k+1)}\\ &\leq (r+T_k)\times\ldots\times(r+1-T_k)\\ &\leq (L+T_k)^{T_k}.\end{aligned}$$

si $s \leq r \leq T_k$, alors

$$\begin{aligned}\frac{(r+u)\times\ldots\times(u+1)}{(r-s)!} &\leq (r+T_k)\times\ldots\times(T_k+1)\\ &\leq (r+T_k)^r \leq (L+T_k)^{T_k}.\end{aligned}$$

Dans tous les cas, on a la majoration

$$\frac{(r+u)\times\ldots\times(u+1)}{(r-s)!} \leq (L+T_k)^{T_k}.$$

En injectant ceci dans la majoration (4.2), on en déduit

$$\begin{aligned}|g_u^{(s)}(\alpha_i)|^2 &\leq (L+T_k)^{2T_k}\left(\sum_{r=0}^{L}|\alpha_i^{2r-s}|\right)^2\\ &\leq (L+T_k)^{2T_k}(L+1)\max\{1,|\alpha_i|\}^{4L-2s}\\ &\leq (L+T_k)^{2T_k}(L+1)\max\{1,|\alpha_i|\}^{4L}\end{aligned}$$

Ainsi, si on reprend la majoration de $|\det A_i|$ on obtient

$$|\det A_i| \leq \left((L+T_k)^{2T_k}T_k(L+1)\right)^{T_k}\max\{1,|\alpha_i|\}^{4LT_k}. \tag{4.3}$$

On divise par $||\ g_0\wedge\ldots\wedge g_{T_k-1}\ ||^2_{\text{quot}}$ pour conclure. □

On en déduit alors la proposition 16 : en regroupant les lemmes 16 17 et 20, on obtient la majoration

$$\begin{aligned}\log||\bigwedge \text{Eval}\ ||\leq{}& 2LT_k\log\prod_{i=1}^{D}\max\{1,|\alpha_i|\}+\frac{1}{2}DT_k\log D\\ &+DT_k{}^2\log(L+T_k)+\frac{1}{2}DT_k\log(L+1)+\frac{1}{2}DT_k\log T_k-\frac{1}{2}\log\left|\prod_{i=1}^{D}\det B_i\right|\end{aligned}$$

où

$$B_i = \left(\sum_{s=0}^{L} \binom{s+u}{s} \binom{s+v}{s} |\alpha_i|^{2s} \overline{\alpha_i}^u \alpha_i^v \right)_{0 \leq u,v \leq T_k - 1}.$$

Or l'expression qui est dans le dernier produit du membre de droite de cette majoration est une expression polynomiale symétrique en les α_i, à coefficients entiers. On sait de plus que $\det B_i \neq 0$. Tout comme dans la preuve du lemme 17, on en déduit donc la minoration

$$\left| \prod_{i=1}^{D} \det B_i \right| \geq 1.$$

Pour conclure, il suffit de remarquer que $\log \prod_{i=1}^{D} \max\{1, |\alpha_i|\} = Dh(x^{p_k}) \leq DN_k h(x)$.

4.6 Conclusion

Finalement avec les notations précédentes, on obtient

Théorème 33 *Pour tout D, T et N assez grand, ainsi que pour tout L vérifiant l'inégalité $D(T+n) > L \geq 2DT$, on a*

$$4LnNDh(x) \geq \frac{LT}{4} \log N - \frac{5}{2} nD \log(L+1) - \frac{3}{2} DT^2 \log(L+T).$$

Démonstration : Il suffit de mettre bout à bout l'inégalité des pentes (proposition 15) ainsi que la proposition 16 appliquée pour tous les $k \in [\![-1, n-1]\!]$. □

On choisit pour conclure les valeurs des paramètres. En notant $[\,\cdot\,]$ la partie entière, on pose

$$\alpha = 18, \quad L = D \left[\frac{N}{4 \log N} \right], \quad T = \left[\frac{\alpha \log 2D}{\log \log 3D} \right] \quad N = \left[\frac{17 \cdot \alpha (\log 2D)^2}{\log \log 3D} \right].$$

Avec ce choix de paramètres le théorème précédent nous donne bien le résultat, à savoir le théorème 32. En effet,

$$\begin{aligned} 4LNnDh(x) &\leq D \cdot \left(\frac{17^3 \cdot \alpha^3 (\log 2D)^6}{(\log \log 3D)^5} \right) Dh(x) \\ &\leq 17^3 \alpha^3 \cdot D^2 \frac{(\log 2D)^6}{(\log \log 3D)^5} h(x). \end{aligned}$$

Par ailleurs,

$$\begin{aligned} 4LNnDh(x) &\geq \frac{LT}{4}\log N - \frac{5}{2}nD\log(L+1) - \frac{3}{2}DT^2\log(L+T) \\ &\geq D\frac{(\log 2D)^3}{(\log\log 3D)^2}\left(\frac{\alpha^2\cdot 17}{4} - \frac{5\cdot\alpha\cdot 17}{4} - \frac{12\cdot\alpha^2}{4}\right) \\ &\geq \frac{D}{4}\frac{(\log 2D)^3}{(\log\log 3D)^2}. \end{aligned}$$

On conclut en mettant ensemble les deux inégalités précédentes.

Remarque 20 On peut se demander ce qu'aurait donnée une preuve du même type obtenue en rajoutant des multiplicitées. En fait, à partir des calculs effectués ici on peut facilement écrire une telle preuve, malheureusement ceci ne permet pas d'obtenir un meilleur résultat.

Chapitre 5

Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe

5.1 Introduction

Soit K un corps de nombres. En notant $\widehat{h}$ la hauteur de Néron-Tate sur une courbe elliptique E/K et en notant K^{ab} la clôture abélienne de K, on montre dans cet article les deux résultats suivants :

Théorème 34 *Si E/K est une courbe elliptique à multiplication complexe, il existe une constante $c(E/K)$ strictement positive, telle que*

$$\forall P \in E(\overline{K})\backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.

Théorème 35 *Soient $c_0 > 0$ et E/K une courbe elliptique à multiplication complexe. Il existe une constante strictement positive $c(E/K, c_0)$, telle que : pour toute extension abélienne F/K et pour tout point $P \in E(\overline{K})\backslash E_{\mathrm{tors}}$ vérifiant $D = [F(P) : F]$, si le nombre de nombres premiers qui se ramifient dans F est borné par $c_0\left(\frac{\log 2D}{\log\log 5D}\right)^2$, alors on a l'inégalité*

$$\widehat{h}(P) \geq \frac{c(E/K, c_0)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{3}.$$

On voit qu'en imposant une contrainte sur l'étendue de la ramification dans l'extension abélienne (théorème 35), on obtient une généralisation d'un précédent résultat de Laurent [31] (cf. le théorème 37 plus loin). Dans le cas général (théorème 34), sans imposer aucune condition, on obtient une minoration optimale aux puissances de log près, avec un exposant légerement dégradé par rapport au cas classique : on a comme puissance de log un exposant 13 au lieu d'un exposant 3 ; toutefois cet exposant 13 est le même que dans le cas multiplicatif dû à Amoroso-Zannier [6] (cf. théorème 38 plus loin). Ce théorème 34, dans le cas des courbes elliptiques à multiplication complexe, généralise au cas D quelconque un précédent résultat de Baker [8] (cf. théorème 39 plus loin). Nous donnons à la fin de l'introduction une application de notre théorème 34.

Ce type de problème remonte aux travaux de Lehmer dans les années 1930 : soit $x \in \mathbb{G}_m(\overline{\mathbb{Q}})\backslash\mu_\infty$ un nombre algébrique qui n'est pas une racine de l'unité. On sait par un théorème de Kronecker que sa hauteur logarithmique absolue $h(x)$ est strictement positive. En 1933 Lehmer énonce la célèbre conjecture

Conjecture 16 (Problème de Lehmer) *Il existe une constante $c > 0$ telle que*

$$\forall x \in \mathbb{G}_m(\overline{\mathbb{Q}})\backslash\mu_\infty, \quad h(x) \geq \frac{c}{D},$$

où $D = [\mathbb{Q}(x) : \mathbb{Q}]$.

Plus exactement, Lehmer se pose plutôt la question inverse : est-il possible de contredire cet énoncé ?

C'est en 1979 , avec le théorème de Dobrowolski [23], qu'est obtenu un résultat optimal à des puissances de log près, en direction de cette conjecture :

Théorème 36 (Dobrowolski) *Il existe une constante $c > 0$ telle que*

$$\forall x \in \mathbb{G}_m(\overline{\mathbb{Q}})\backslash\mu_\infty, \quad h(x) \geq \frac{c}{D}\left(\frac{\log\log 3D}{\log 2D}\right)^3,$$

où $D = [\mathbb{Q}(x) : \mathbb{Q}]$.

Peu de temps après, Laurent a étendu, dans son article [31], la conjecture de Lehmer aux courbes elliptiques sur un corps de nombres, en remplaçant la hauteur sur $\mathbb{G}_m$ par la hauteur de Néron-Tate et il a étendu le résultat de Dobrowolski au cas des courbes elliptiques E/K à multiplication complexe.

Théorème 37 (Laurent) *Soit E/K une courbe elliptique à multiplication complexe. Il existe une constante strictement positive $c(E/K)$ telle que*

$$\forall P \in E(\overline{K})\backslash E_{\text{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 3D}{\log 2D}\right)^3,$$

où $D = [K(P) : K]$.

Dans les articles [5] et [6], Amoroso-Dvornicich et Amoroso-Zannier ont étendu le problème de Lehmer sur $\mathbb{G}_m$ au cas des extensions abéliennes relatives. Précisément, ils énoncent la conjecture et démontrent le théorème suivant :

Conjecture 17 (Amoroso-Zannier) *Soit K un corps de nombres. Il existe une constante strictement positive $c(K)$, telle que*

$$\forall x \in \mathbb{G}_m(\overline{K})\backslash\mu_\infty, \quad h(x) \geq \frac{c(K)}{D},$$

où $D = [K^{\text{ab}}(x) : K^{\text{ab}}]$.

Théorème 38 (Amoroso-Zannier) *Soit K un corps de nombres. Il existe une constante $c(K)$ strictement positive, telle que*

$$\forall x \in \mathbb{G}_m(\overline{K})\backslash\mu_\infty, \quad h(x) \geq \frac{c(K)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

où $D = [K^{\text{ab}}(x) : K^{\text{ab}}]$.

Ce théorème étend le résultat de Amoroso-Dvornicich qui traitait le cas où x appartenait à une extension abélienne de K, *i.e.*, le cas $D = 1$. C'est précisément ce théorème, dans le cas $D = 1$, qui a été étendu aux courbes elliptiques à multiplication complexe, ou ayant un j-invariant non-entier, par Baker dans [8], puis par Silverman [50] dans le cas des courbes elliptiques sans multiplication complexe. Ainsi pour les courbes elliptiques, on a

Théorème 39 (Baker-Silverman) *Soit E/K une courbe elliptique. Il existe une constante strictement positive $c(E/K)$ telle que*

$$\forall P \in E(K^{\text{ab}})\backslash E_{\text{tors}}, \quad \widehat{h}(P) \geq c(E/K).$$

L'objectif du présent article est d'étendre le résultat d'Amoroso-Zannier au cas des courbes elliptiques à multiplication complexe, généralisant ainsi le résultat de Baker au cas D quelconque. Notons que le théorème 34 répond à une conjecture de David dans le cas des courbes elliptiques à multiplication complexe :

Conjecture 18 (David) *Soient A/K une variété abélienne sur un corps de nombres et $\mathcal{L}$ un fibré en droites ample et symétrique sur A. Pour tout $\varepsilon > 0$, il existe une constante strictement positive $c(A/K, \mathcal{L})$ telle que pour tout point $P \in A(\overline{K})$ qui n'est pas de* $\mathrm{End}(A(\overline{K}))$*-torsion, on a*

$$\widehat{h}_{\mathcal{L}}(P) \geq \frac{c(A/K, \mathcal{L})}{D_{\mathrm{tors}}^{\frac{1}{g}+\varepsilon}},$$

où $D_{\mathrm{tors}} = [K(A_{\mathrm{tors}}, P) : K(A_{\mathrm{tors}})]$.

En effet, le théorème 34 étant vrai pour $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$, il l'est en particulier pour $D = [F(P) : F]$ pour toute extension abélienne F/K. De plus, quitte à remplacer K par une extension de degré borné en fonction de E, le résultat reste toujours vrai (on ne change que la constante $c(E/K)$). L'extension $H(E_{\mathrm{tors}})/H$ est abélienne pour $H = K(j)$ corps de classes de Hilbert de E, ce qui conclut.

Le théorème 34 rend naturel de généraliser la conjecture 17 aux courbes elliptiques :

Conjecture 19 *Soit E/K une courbe elliptique. Il existe une constante strictement positive $c(E/K)$, telle que*

$$\forall P \in E(\overline{K}) \backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D},$$

où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.

Le théorème 34 est une première étape en direction de cette conjecture 18, au moins dans le cas de multiplication complexe. On peut indiquer brièvement un des intérêts d'un tel résultat. Pour expliquer cela, on introduit quelques notations : on dit qu'une courbe (intègre) sur une variété abélienne A est *transverse* si elle n'est contenue dans aucun translaté de sous-variété abélienne de A différente de A. Si X est un sous-schéma fermé intègre de A et r un entier, alors $Z_{x,0}^{(r)} \subset X(\overline{K})$ est l'ensemble des points pour lesquels il existe un sous-schéma en groupes G de A avec

$$\dim_P X \cap G \geq \max\{1, r - \mathrm{codim}\ G\}.$$

On dit qu'une variété abélienne simple A est de *type* (g, δ), si elle est de dimension g et si le rang de $\mathrm{End}(A) = 2g/\delta$. Enfin, on note

$$A^{[r]} = \bigcup_{\mathrm{codim}\ G \geq r} G(\overline{K}),$$

où G est un sous-schéma en groupe de codimension indiquée. Dans son article [45], Rémond prouve :

Théorème 40 (Rémond) *Soit A une variété abélienne sur $\overline{K}$. Nous choisissons une isogénie entre A et un produit $A_1^{n_1} \times \cdots \times A_m^{n_m}$ où m est un entier naturel et pour chaque indice i avec $1 \leq i \leq m$ la variété abélienne A_i est simple de type (g_i, δ_i) et $n_i \in \mathbb{N}^*$. Soient X un sous-schéma fermé intègre de A et r, r' deux entiers tels que $0 \leq r \leq r' \leq \dim A$. Nous supposons que l'une des conditions suivantes est vérifiée.*
(C_1) La conjecture (18) est vraie.
(C_2) La variété abélienne A est à multiplication complexe et $r' > (1 + \sum_{i=1}^m g_i)(r-1)$.
(C_3) On a l'inégalité

$$r' > \sum_{i=1}^{m} g_i(n_i + \delta_i)\frac{r-1}{r}.$$

Alors, pour toute hauteur h associée à un fibré ample $\mathcal{L}$ sur A et tout réel H, l'ensemble

$$\left\{P \in \left(X(\overline{K})\backslash Z_{X,0}^{(r)}\right) \cap A^{[r']} \ / \ h(P) \leq H\right\}$$

est fini. Si de plus X est une courbe transverse et $r \geq 2$, alors $X(\overline{K}) \cap A^{[r']}$ est fini.

Notons que notre théorème 34 permet déjà de simplifier la preuve du theorem 2. de Viada [57] suivant :

Théorème 41 (Viada) *Soient E/K une courbe elliptique à multiplication complexe, n un entier non nul et C/K une courbe transverse dans E^n. Pour $r \geq 0$ on considère les ensembles*

$$S_r(C) := \bigcup_{\operatorname{codim} G \geq r} G \cap C(\overline{K})$$

où l'union porte sur les sous-groupes algébriques G de E^n de codimension au moins r. Alors l'ensemble $S_2(C)$ est fini.

La preuve de Viada est calquée sur celle de Bombieri, Masser et Zannier [14] dans le cas de $\mathbb{G}_m^n$. Elle utilise le fait que la hauteur des points de $S_1(C)$ est bornée. Il s'agit du Theorem 1. du même article de Viada qui résulte simplement des propriétés fonctorielles des hauteurs et du théorème du cube pour les variétés abéliennes. Ceci étant acquis on constate, en appliquant le théorème de Northcott, qu'il suffit alors de montrer que le degré des points de $S_2(C)$ est borné. C'est la partie difficile de la preuve. Viada montre ceci en deux étapes : la première consiste à montrer la finitude de l'ensemble $S_3(C)$. La seconde étape consiste à montrer la finitude de $S_2(C)$ en utilisant un subtil argument cohomologique. Nous montrons au chapitre 5 comment éviter cet argument cohomologique en appliquant notre théorème 34. En fait l'utilisation de ce théorème 34 permet de ramener la seconde étape à la première. Nous expliquons ceci dans la dernière partie de cet article.

Dans la suite (dernière partie exceptée) on s'attache à prouver le théorème 34. On explique à la fin comment le théorème 35 s'obtient de la même façon. La preuve est une preuve

classique de transcendance à deux exceptions près : on utilise un lemme de Siegel absolu et il y a en fait deux extrapolations selon que l'on est dans une situation avec beaucoup de ramification ou non. Ceci étant dit, dans le cas non-ramifié, la preuve suit le schéma initié par Dobrowolski, à savoir une extrapolation sur les transformés par le morphisme de Frobenius. Dans le cas ramifié, on suit la preuve du cas multiplicatif de [6] en utilisant encore des transformés par Frobenius. On utilise l'astuce de Laurent [31] consistant à dédoubler les variables pour permettre une plus grande liberté dans le choix des paramètres auxiliaires. La partie 5.2 consiste en des rappels sur la hauteur de Néron-Tate et sur les propriétés dont nous aurons besoin concernant les courbes elliptiques à multiplication complexe. La partie 5.3 consiste en une série de réductions en vue de prouver les théorèmes 34 et 35. La preuve proprement dite se trouve dans les parties 5.5, 5.6 et 5.7.

Dans la preuve on se ramène à travailler avec une extension abélienne F/K finie et avec $D = [F(P) : F]$. Notons que l'hypothèse "F/K est abélienne" sert de manière cruciale dans les deux étapes d'extrapolation : dans l'étape où il y a peu de premiers ayant un grand indice de ramification dans F, *i.e.* l'étape "quasi-classique", l'extrapolation se fait grâce au lemme 30 qui utilise de manière fondamentale l'hypothèse d'abélianité. Dans l'autre extrapolation, *i.e.* le cas compémentaire où beaucoup de premiers ont un grand indice de ramification dans F, l'hypothèse sert à fabriquer le groupe H_p du lemme 29 : on utilise pour cela le théorème de Kronecker-Weber.

5.2 Hauteur et multiplication complexe

5.2.1 Hauteur

Soient K un corps de nombres de degré d, M_K l'ensemble des valeurs absolues (deux à deux non équivalentes) sur K, M_K^0 les valeurs absolues ultramétriques de M_K normalisées par $|p|_v = p^{-1}$ pour toute place finie v au-dessus du nombre premier p et M_K^∞ les valeurs absolues archimédiennes de M_K. On note $d_v = [K_v : \mathbb{Q}_p]$ le degré local et on définit la *hauteur (logarithmique absolue)* sur $\mathbb{P}^n(\overline{\mathbb{Q}})$ par

$$h(x_0 : \ldots : x_n) = \frac{1}{d} \sum_{v \in M_K} d_v \log \max_{0 \leq i \leq n} |x_i|_v.$$

Dans cette définition, la renormalisation par $\frac{1}{d}$ sert juste à faire en sorte que $h(x)$ soit indépendante du choix du corps K contenant x. De plus par la formule du produit, la hauteur est aussi indépendante du choix d'un système de coordonnées projectives.

En plongeant $\mathbb{G}_m^n$ dans $\mathbb{P}^n$ par $(x_1, \ldots, x_n) \mapsto (1 : x_1, \ldots : x_n)$ ceci défini également la hauteur sur $\mathbb{G}_m^n$.

Dans la suite on utilisera également la hauteur h_2 définie sur $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ par

$$h_2(x_1,\ldots,x_n)=\frac{1}{d}\left(\sum_{v\in M_K^0} d_v \log \max_{1\le i\le n}|x_i|_v+\sum_{v\in M_K^\infty} d_v \log\sqrt{\sum_{1\le i\le n}|x_i|_v^2}\right).$$

Soit N un entier. On définit comme le fait Schmidt (voir [48]) la hauteur h_2 d'un sous-$\overline{\mathbb{Q}}$-espace vectoriel S algébrique de dimension d de $\overline{\mathbb{Q}}^{N+1}$ par :

$$h_2(S)=h_2(\mathbf{x}_1\wedge\ldots\wedge\mathbf{x}_d),$$

où $\mathbf{x}_1,\ldots,\mathbf{x}_d$ est une base de S sur un corps de nombres quelconque sur lequel S est défini.

5.2.2 Hauteur de Néron-Tate

Définition 40 Si E/K est une courbe elliptique donnée par une équation de Weierstrass, on définit la *hauteur* $h\ :\ E(\overline{K})\to\mathbb{R}^+$ par $h(P):=h(x(P):1)$, où $h(x:y)$ est la hauteur logarithmique absolue sur $\mathbb{P}^1(\overline{K})$ définie précédemment.

Cette hauteur vérifie un certain nombre de propriétés. Nous indiquons les plus essentielles, qui nous serviront dans la suite. On renvoie par exemple au livre [30] Part B pour tout ce qui concerne les hauteurs.

Proposition 17 *Sur une courbe elliptique E/K, la hauteur h vérifie :*
(i) $\forall P\in E(\overline{K})$ $\quad h([m]P)=m^2h(P)+O(1)$.
(ii) $\forall P,Q\in E(\overline{K})$ $\quad h(P+Q)+h(P-Q)=2h(P)+2h(Q)+O(1)$.
(iii) $\forall h>0$ $\quad$ l'ensemble $\{P\in E(\overline{K})/\ h(P)\le h\}$ est fini.
Dans les affirmations précédentes, la constante $O(1)$ dépend de E et m, mais pas des points P et Q.

À partir de cette hauteur, on peut en construire une plus jolie : la *hauteur de Néron-Tate*, notée $\widehat{h}$. La définition est la suivante :

$$\widehat{h}(P)=\lim_{n\to+\infty}\frac{h([2^n]P)}{4^n}.$$

Les propriétés classiques de cette hauteur sont résumées dans le théorème suivant.

Théorème 42 *La hauteur canonique est une forme quadratique positive semi-définie sur $E(\overline{K})$, telle que*

$$\textit{d'une part } \forall P\in E(\overline{K})\ \widehat{h}(P)=h(P)+O(1),\ \textit{ et d'autre part, }\ \widehat{h}(P)=0\iff P\in E_{\mathrm{tors}}.$$

5.2.3 Multiplication complexe

Soient K un corps de nombres et E/K une courbe elliptique à multiplication complexe par l'ordre d'un corps quadratique imaginaire k. On note $\mathcal{O}_K$ l'anneau d'entiers de K et pour toute place finie v de K on note k_v le corps résiduel associé à v. Quitte à faire une extension de corps ne dépendant que de E/K et quitte à prendre une courbe elliptique isogène à la courbe de départ, on peut supposer que K contient k et que l'anneau des endomorphismes de E/K est exactement $\mathcal{O}_k$, l'anneau des entiers de k. De plus, la courbe est à multiplication complexe, donc elle a bonne réduction potentielle. Ainsi, quitte à remplacer K par une extension de degré borné (en fonction de E/K), on peut également supposer que E/K a bonne réduction en toute place de K. On fait toutes ces hypothèses dans la suite.

On fixe un point $P \in E(\overline{K})\backslash E_{\text{tors}}$ et on note $D = [K^{\text{ab}}(P) : K^{\text{ab}}]$. On choisit alors une extension F/K abélienne finie, telle que $D = [F(P) : F]$, ceci étant possible car K^{ab} est le compositum des extensions abéliennes sur K.

Dans la suite, on fixe un modèle de Weierstrass de E de la forme

$$Y^2 = X^3 + a_4X + a_6,$$

où a_4 et a_6 sont des éléments de K. Si $\wp$ est la fonction de Weierstrass associée, la courbe complexe $E(\mathbb{C})$ est paramétrée par $X = \wp(z)$ et $Y = \wp'(z)$. On rappelle que les points complexes d'une courbe elliptique sont paramétrés par l'isomorphisme de groupes de Lie complexes

$$\mathbb{C}/\Lambda \to E(\mathbb{C}) \ : \ y^2 = x^3 + a_4x + a_6, \quad z \mapsto (\wp(z), \wp'(z)),$$

où $\wp(z)$ est la fonction de Weierstrass définie par la formule

$$\forall z \in \mathbb{C}, \quad \wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Soient p un nombre premier et v une place de K au-dessus de p. On rappelle le théorème fondamental, dû à Deuring [22], concernant la multiplication complexe que l'on va utiliser ici. On renvoie par exemple à [51] Chapter II pour les démonstrations.

Proposition 18 *Soit $E/\mathbb{C}$ une courbe elliptique à multiplication complexe par $\mathcal{O}_k$, anneau d'entiers d'un corps de nombres quadratique imaginaire. Il existe un unique isomorphisme*

$$[\cdot] \ : \ \mathcal{O}_k \to \text{End}(E)$$

tel que pour toute différentielle invariante de E, $\omega \in \Omega_E$ et pour tout $\alpha \in \mathcal{O}_k$, on a

$$[\alpha]^*\omega = \alpha\omega.$$

De plus le degré de $[\alpha]$ est égal à $N_{\mathbb{Q}}^k(\alpha)$.

Théorème 43 (Deuring) *Soit E/K une courbe définie sur le corps de nombres K, à multiplication complexe par le corps quadratique imaginaire k. Soient p un nombre premier et v une place de K au-dessus de p telle que E a bonne réduction en v. Alors il existe un unique $\alpha_v \in \mathcal{O}_k$ tel que $\widetilde{[\alpha_v]} = \mathrm{Frob}_{E_v}$ où E_v est la réduction de E sur $\mathbb{F}_v$.*

De plus au cours de la preuve de ce théorème on montre que $q := N_{\mathbb{Q}}^K(v) = N_{\mathbb{Q}}^K(\alpha)$. Dans les deux lemmes qui suivent, conséquences du théorème précédent, on note π une uniformisante dans k de l'idéal maximal $\mathfrak{M}$ correspondant à la place v.

Lemme 21 *Pour tout élément $\alpha \in \mathcal{O}_k$, il existe deux polynômes R_α et S_α premiers entre eux, à coefficients dans $\mathcal{O}_k$ tels que*

$$\wp(\alpha z) = \frac{R_\alpha(\wp(z))}{S_\alpha(\wp(z))}, \text{ et } \widetilde{S_\alpha} \neq 0.$$

Ces deux polynômes sont définis à multiplication par une même unité de $\mathcal{O}_k$ près. Notamment quand $\alpha = \alpha_v$, on a

$$R_\alpha(X) = uX^q + \pi V(X), \text{ et } S_\alpha(X) = u + \pi W(X),$$

où u est une unité v-adique de $\mathcal{O}_k$ et V et W sont deux polynômes à coefficients dans $\mathcal{O}_k$.

Lemme 22 *Pour tout $\alpha \in \mathcal{O}_k$, les polynômes $\widetilde{R_\alpha}$ et $\widetilde{S_\alpha}$ sont premiers entre eux.*

Démonstration : On trouvera par exemple une preuve de ces deux lemmes dans [31] lemmes 3.1 et 3.2 respectivement. □

Nous aurons également besoin d'un lemme sur les endomorphismes du groupe formel associé à la courbe elliptique E. Si P est un point de la courbe de coordonnées affines (X, Y), on note $t = -\frac{X}{Y}$ et on note $[\alpha_v]$ l'opérateur du groupe formel associé à l'endomorphisme α_v.

Lemme 23 *Il existe une série entière ψ, à coefficients dans $\mathcal{O}_{K_v}$ telle que*

$$[\alpha_v](t) = t^p + \pi_p \psi(t).$$

Démonstration : C'est le lemme 3.3 de [31]. □

5.3 Réductions

On fait maintenant les mêmes réductions que dans le cas multiplicatif dû à Amoroso-Zannier. On note $\mathcal{P}$ l'ensemble des nombres premiers qui se décomposent totalement dans K. Pour chacune des places v de K au-dessus d'un tel premier p, la complétion v-adique de K est $K_v = \mathbb{Q}_p$. Pour $p \in \mathcal{P}$, on notera donc K_p cette complétion dans la suite. Soient $p \in \mathcal{P}$ et F/K une extension abélienne finie, on note $e_p(F)$ l'indice de ramification de p dans F et F_v la complétion v-adique de F en v. On a $K_p = \mathbb{Q}_p$, donc F_v est une extension abélienne de $\mathbb{Q}_p$. Par le théorème de Kronecker-Weber local, elle est donc contenue dans une extension cyclotomique de $\mathbb{Q}_p$ que l'on notera $\mathbb{Q}_p(\zeta_m)$. On pose $m = m_p(F)$ le plus petit entier ayant cette propriété et on définit $\mathfrak{f}_p(F)$ le *conducteur local de F en p* comme étant la plus grande puissance de p divisant m (il s'agit bien du conducteur local au sens de la théorie du corps de classes local). On pose

$$\mathfrak{f}(F) = \prod_{p \in \mathcal{P}} \mathfrak{f}_p(F),$$

le *conducteur de F* et on note que si $F' \subset F$ alors $\mathfrak{f}(F') \leq \mathfrak{f}(F)$.

Soit maintenant P un point de $E(\overline{K}) \backslash E_{\text{tors}}$ contredisant le théorème 34, de degré minimal, *i.e.*, tel que pour tout point $P' \in E(\overline{K}) \backslash E_{\text{tors}}$ de degré $D' < D$ sur K^{ab}, on a

$$\widehat{h}(P') \geq \frac{c(E/K)}{D'} \left(\frac{\log\log 5D'}{\log 2D'} \right)^{13}.$$

Lemme 24 *Pour démontrer le théorème 34, on peut supposer que pour tout point de torsion $T \in E_{\text{tors}}$ on a $[K^{\text{ab}}(P+T) : K^{\text{ab}}] \geq D$.*

Démonstration : La hauteur de Néron-Tate est invariante par translation par un point de torsion. Le résultat découle donc immédiatement de la définition du point P et de la décroissance pour $t \geq 1$ de la fonction $t \mapsto \frac{c(E/K)}{t} \left(\frac{\log\log 5t}{\log 2t} \right)^{13}$. □

Soit $\mathcal{A}$ l'ensemble des extensions abéliennes finies F/K telles qu'il existe un point de torsion $T \in E_{\text{tors}}$ tel que $[F(P+T) : F] \leq D$, *i.e.*, tel que $[F(P+T) : F] = D$ par le lemme précédent. Cet ensemble est non vide, puisque par définition de K^{ab}, on sait qu'il existe une extension abélienne finie F/K telle que $[F(P) : F] = [K^{\text{ab}}(P) : K^{\text{ab}}] = D$. L'extension F et le point $T = 0$ montrent donc que $\mathcal{A}$ est non vide. On définit alors l'entier

$$\mathfrak{f} = \min_{F \in \mathcal{A}} \mathfrak{f}(F).$$

Lemme 25 *Avec les notations précédentes, pour démontrer le théorème 34, on peut supposer que*

$$D = [F(P) : F] \text{ où } F/K \text{ est une extension appartenant à } \mathcal{A}, \text{ contenue dans } K(P). \quad (5.1)$$

On peut également supposer que

$$\mathfrak{f}(F) = \mathfrak{f}. \quad (5.2)$$

Enfin, on peut aussi supposer que

$$\forall T \in E_{\text{tors}} \text{ tel que } K(P+T) \subset K(P), \text{ on a } K(P+T) = K(P). \quad (5.3)$$

Démonstration : Par définition de K^{ab}, il existe une extension abélienne finie F/K telle que $D = [F(P) : F]$, donc appartenant à $\mathcal{A}$. On prend dans $\mathcal{A}$ une extension F/K réalisant le min des $\mathfrak{f}(F)$, *i.e.*, réalisant $\mathfrak{f}$. Montrons qu'on peut supposer (5.3). Soit $T \in E_{\text{tors}}$ tel que $K(P+T) \subset K(P)$, alors, le point T est défini sur le corps de nombres $K(P)$ car $P + T - P = T$. Si pour tous ces T, on a l'égalité $K(P+T) = K(P)$, il n'y a alors rien à montrer. Sinon, on note $\mathcal{T}$ l'ensemble fini des points de torsion tels que $K(P+T) \subsetneq K(P)$. Soient $T \in \mathcal{T}$ et $P_1 = P + T$. L'extension $K(P_1)$ est une sous-extension stricte de $K(P)$. On note $\mathcal{T}_1$ l'ensemble fini des points de torsion tels que $K(P_1+T) \subsetneq K(P_1)$. Si $\mathcal{T}_1$ est non vide, on choisit $T_1 \in \mathcal{T}_1$ et on pose $P_2 = P_1 + T_1$. L'extension $K(P_2)$ est une sous-extension stricte de $K(P_1)$. On construit ainsi une chaîne

$$K(P_n) \subsetneq \ldots \subsetneq K(P_1) \subsetneq K(P).$$

Donc pour n assez grand, on sait que $K(P_{n+1}) = K(P_n)$, autrement dit que l'ensemble $\mathcal{T}_{n+1}$ correspondant est vide, c'est-à-dire que

$$\forall T \in E_{\text{tors}} \text{ tel que } K(P_n+T) \subset K(P_n), \text{ on a } K(P_n+T) = K(P_n).$$

Or par construction, on a $P_n = P + T_n$ où T_n est un point de torsion de E, donc le lemme 24 précédent assure que $[F(P_n) : F] \geq D_n \geq D$. De plus on a

$$D_n = [K^{\text{ab}}(P_n) : K^{\text{ab}}] \leq [F(P_n) : F] \leq [F(P) : F] = D$$

car $K(P_n) \subset K(P)$, donc $D_n = D$. La hauteur de Néron-Tate étant invariante par translation par un point de torsion, on a également $\widehat{h}(P_n) = \widehat{h}(P)$. Enfin, quitte à remplacer F par $F_1 = F \cap K(P_n)$, on voit que l'on peut aussi supposer l'hypothèse (5.1) vraie. La fonction $\mathfrak{f}(\cdot)$ étant croissante, l'hypothèse (5.2) est elle aussi vérifiée, ce qui conclut. □

Dans toute la suite on supposera désormais vraies les hypothèses (5.1), (5.2) et (5.3).

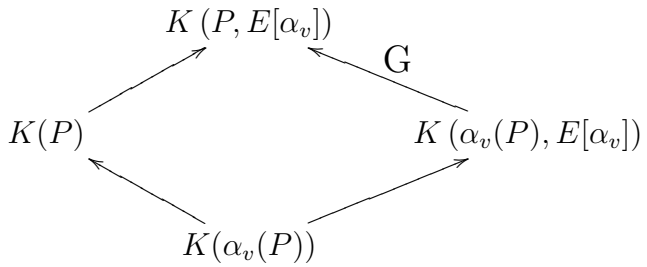
Remarque 21 On note que, comme $K \subset F \subset K(P)$, on a aussi, $F(P) = K(P)$.

On peut maintenant énoncer les deux lemmes de réduction qui nous serviront dans la suite. Le premier est inspiré du Lemma 2.1. (ii) de [6], le second est plus classique dans le cadre du probème de Lehmer.

Lemme 26 *Soient $p \in \mathcal{P}$ et v une place de K au-dessus de p, alors, pour démontrer le théorème 34, on peut supposer que*

$$\textit{soit } K(\alpha_v(P)) = K(P), \ \textit{ soit } [K(P) : K(\alpha_v(P))] = p.$$

Démonstration : On considère le diagramme



L'extension $K(P, E[\alpha_v])/K(\alpha_v(P), E[\alpha_v])$ est galoisienne d'ordre 1 ou p. En effet on a une injection naturelle $\mathrm{Gal}(\overline{K}/K(\alpha_v(P), E[\alpha_v])) \hookrightarrow E[\alpha_v]$: les conjugués de P par l'action de $\mathrm{Gal}(\overline{K}/K(\alpha_v(P), E[\alpha_v]))$ sont parmi les $P+T$, où $T \in E[\alpha_v]$ et α_v est une isogénie cyclique d'ordre p.

Si le groupe de Galois correspondant G est d'ordre p, alors l'extension $K(P)/K(\alpha_v(P))$ est également d'ordre p.

Si G est d'ordre 1, on va montrer qu'il existe $T \in E[\alpha_v]$ tel que $K(P+T) \subset K(\alpha_v(P))$. On regarde l'action de $\mathrm{Gal}(\overline{K}/K(\alpha_v(P))$ sur l'ensemble $\{P + T \ / \ T \in \ker[\alpha_v]\}$. Soit il y a une seule orbite, auquel cas $[K(\alpha_v(P)) : K(P)] = p$; soit l'orbite ω_P, contenant P est de cardinal m strictement inférieur à p, donc premier à p. Dans ce cas, il existe $T' \in E[\alpha_v]$, tel que

$$\sum_{T \in \omega_P} (P + T) = mP + T'$$

est stable sous l'action de $\mathrm{Gal}(\overline{K}/K(\alpha_v(P))$. Par le théorème de Bézout, il existe deux entiers, λ et μ tels que $\lambda m + \mu p = 1$. Par ailleurs, en notant $\alpha_v^\vee$ l'isogénie duale de α_v, on a

$$K\,([p]P) = K\,(\alpha_v^\vee(\alpha_v(P))) \subset K(\alpha_v(P)).$$

Ainsi, on a les inclusions

$$K\,([\lambda]([m]P + T') + [\mu p]P)) = K\,(P + [\lambda]T') \subset K(\alpha_v(P)).$$

On a donc l'inclusion $K(P + [\lambda]T') \subset K(P)$. Par l'hypothèse (5.3) ceci entraîne que

$$K(P) = K(P + [\lambda]T') \subset K(\alpha_v(P)).$$

On en déduit que $K(P) = K(\alpha_v(P))$. □

Lemme 27 *Pour tout $p \in \mathcal{P}$ sauf pour au plus $\frac{1}{2}\log D$ d'entre eux et pour toute place v de K au-dessus de p, on a*

$$F(P) = F(\alpha_v(P)).$$

Démonstration : C'est le lemme combinatoire classique de Dobrowolski [23] (dû à Laurent [31] lemme 4.2 dans le cas des courbes elliptiques). □

Notons que l'on pourrait éviter de recourir à ce lemme combinatoire, en faisant un raisonnement du même type que dans le lemme précédent, comme il est fait dans l'article d'Amoroso-Zannier [6]. Dans la suite on notera $\mathcal{P}^\star$ le sous-ensemble de $\mathcal{P}$ formé des premiers vérifiant le lemme 27 précédent.

5.4 Lemmes d'extrapolation

Dans la partie 5.6 on va faire deux extrapolations différentes, selon qu'il y a beaucoup de places de F au-dessus de $\mathcal{P}^\star$ ayant un gros indice de ramification, ou non, tout ceci étant bien évidemment quantifié. On commence par les lemmes qui nous permettront d'extrapoler dans le cas où il y a beaucoup de ramification.

5.4.1 Lemme ramifié

Lemme 28 *Soient E/K une courbe elliptique à multiplication complexe, v une place de bonne réduction ordinaire et I_v le groupe d'inertie de $\mathrm{Gal}(\overline{K_v}/K_v)$. Alors, pour tout entier $n \geq 1$, on a l'isomorphisme de I_v-module $E[\alpha_v^n] \simeq \mu_{p^n}$.*

Démonstration : C'est le lemme 3.2 de [8]. □

Le lemme suivant est inspiré du lemme 3.2. de [6].

Lemme 29 *Soient $p \in \mathcal{P}^\star$ et e_p son indice de ramification dans F. Il existe un sous-groupe H_p de $\mathrm{Gal}(F/K)$ d'ordre*

$$\mid H_p \mid \geq \min\{e_p, p\},$$

tel que

$$\mid x^p - \sigma x^p \mid_w \leq \frac{1}{p},$$

pour tout $x \in \mathcal{O}_F$, tout $\sigma \in H_p$ et toute place w de F au-dessus de p. De plus, pour toute place v de K au-dessus de p et pour toute extension $\tau \in \mathrm{Gal}(\overline{K}/K)$ de $\sigma \in H_p - \{\mathrm{Id}\}$, on a

$$\tau(\alpha_v(P)) \neq \alpha_v(P).$$

Démonstration : La fabrication de H_p et l'estimation de son cardinal se fait comme dans l'article de Amoroso-Zannier : soient v une place de F étendant p et F_v le complété v-adique de F. On pose $m := m_p(F)$ le plus petit entier m tel que $F_v \subset \mathbb{Q}_p(\zeta_m)$. On décompose m sous la forme $m = \mathfrak{f}_p \cdot n$ où n est premier à p et $\mathfrak{f}_p$ est le conducteur local de F en p.

Si p ne se ramifie pas dans F, alors $e_p = 1$ et $H_p = \{\mathrm{Id}\}$ convient. On peut donc supposer que p se ramifie dans F, donc *a fortiori* dans $\mathbb{Q}(\zeta_m)$. Ainsi p divise le conducteur

local $\mathfrak{f}_p$. On pose Σ_p le groupe de Galois de l'extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p})$. C'est un groupe cyclique d'ordre p ou $p-1$ selon que p^2 divise $\mathfrak{f}_p$ ou non. Par la propriété de minimalité de m, Σ_p ne fixe pas F_v, donc induit par restriction un sous-groupe non-trivial H_v^* de $\mathrm{Gal}(F_v/K_p)$. On note que si p^2 ne divise pas $\mathfrak{f}_p$, alors l'ordre de H_v^* est au moins e_p car l'extension $\mathbb{Q}_p(\zeta_{m/p})/\mathbb{Q}_p$ est non-ramifiée ; alors que si p^2 divise $\mathfrak{f}_p$, nécessairement H_v^* est d'ordre p. On définit H_v comme étant l'image isomorphe de H_v^* dans $\mathrm{Gal}(F/K)$. On peut voir que H_v^* ne dépend pas de v, mais seulement de p. Il en est de même de H_v que l'on note désormais H_p. On a déja obtenu l'estimation de son cardinal.

Montrons la propriété de congruence : soit $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}_p(\zeta_m)$. On a

$$\forall x \in \mathcal{O},\ \forall \sigma \in \Sigma_p \quad x^p \equiv \sigma x^p \mod p\mathcal{O}, \tag{5.4}$$

(cf. par exemple [6] p. 717). Ainsi pour tout $x \in \mathcal{O}_F$ et pour tout $\sigma \in H_p$, l'entier $x^p - \sigma x^p \in F$ est d'ordre supérieur à e_p en v.

Montrons maintenant la dernière propriété. Soient $\sigma \in H_p - \{\mathrm{Id}\}$ et $\tau \in \mathrm{Gal}(\overline{K}/K)$ une extension de σ. Supposons par l'absurde que $\tau(\alpha_v(P)) = \alpha_v(P)$. Soit $\mathbb{E}$ le sous-corps de F fixe par σ. On a $[\mathbb{E}(\alpha_v(P)) : \mathbb{E}] = [F(\alpha_v(P)) : F]$. De plus, par le lemme 27, le point P est défini sur la même extension de F que $\alpha_v(P)$. Donc,

$$[\mathbb{E}(\alpha_v(P)) : \mathbb{E}] = [F(\alpha_v(P)) : F] = [F(P) : F] = D. \tag{5.5}$$

On va maintenant montrer que $\mid \Sigma_p \mid = p$: tout d'abord, comme $\mathbb{E}$ est strictement inclus dans F, on a $[F(P) : \mathbb{E}] > [F(P) : F]$ et donc, d'après (5.5),

$$[F(P) : \mathbb{E}(\alpha_v(P))] = \frac{[F(P) : \mathbb{E}]}{[\mathbb{E}(\alpha_v(P)) : \mathbb{E}]} = \frac{[F(P) : \mathbb{E}]}{[F(P) : F]} > 1. \tag{5.6}$$

Par ailleurs, d'après la remarque 5.3, on a $K(P) = F(P)$ et $K \subset \mathbb{E}(\alpha_v(P)) \subset F(P)$. Ainsi, $[F(P) : \mathbb{E}(\alpha_v(P))]$ divise $[K(P) : K(\alpha_v(P))]$. Si $K(P) = K(\alpha_v(P))$, alors τ fixe $K(P) = F(P)$ donc fixe F ce qui contredit le choix de $\sigma \neq \mathrm{Id}$. Ainsi, par le lemme 26, l'extension $K(P)/K(\alpha_v(P))$ est de degré p. On en déduit que l'extension $F(P)/\mathbb{E}(\alpha_v(P))$ qui est non triviale par (5.6), est de degré p. On a ainsi

$$[F(\alpha_v(P)) : \mathbb{E}(\alpha_v(P))] = \frac{[F(P) : \mathbb{E}(\alpha_v(P))]}{[F(P) : F(\alpha_v(P))]} = [F(P) : \mathbb{E}(\alpha_v(P))] = p \text{ par le lemme 27.}$$

L'extension $F/\mathbb{E}$ étant galoisienne, on en déduit que $\mid H_p \mid = [F : \mathbb{E}] = p$, donc par construction de H_p on obtient $\mid \Sigma_p \mid = p$.

On sait que sur une courbe elliptique à multiplication complexe, on a bonne réduction ordinaire en toutes les places v au-dessus d'un premier $p \in \mathcal{P}$. On peut donc appliquer le lemme 28 dans notre situation. Par ce lemme on sait que les points de α_v^k-torsion sont définis sur $\mathbb{Q}_p(\zeta_{p^k}) \subset \mathbb{Q}_p(\zeta_m)$. Ainsi $F_v(E[\alpha_v^k]) \subset \mathbb{Q}(\zeta_m)$, donc le groupe de Galois Σ_p induit par restriction un sous-groupe non-trivial de $\mathrm{Gal}(F(E[\alpha_v^k])/K)$ qui est cyclique d'ordre p par le paragraphe précédent. Soit donc $\mathbb{F} \subset F(E[\alpha_v^k])$ son sous-corps fixe. Soient $x \in \mathbb{E}$

et $\rho \in G_1 = \mathrm{Gal}(F(E[\alpha_v^k])/\mathbb{F}) - \{\mathrm{Id}\}$. Puisque $[F : \mathbb{E}] = p$, le morphisme σ engendre le groupe $\mathrm{Gal}(F/\mathbb{E})$, donc il existe un entier u tel que $\rho_F = \sigma^u$. Notamment, on en déduit que $\rho(x) = x$, c'est-à-dire que

$$\mathbb{E} \subset \mathbb{F}. \tag{5.7}$$

On va maintenant montrer qu'il existe un point de α_v^k-torsion T tel qu'on ait l'inclusion $\mathbb{F}(P+T) \subset \mathbb{F}(\alpha_v(P))$. Si $\mathbb{F}(P) \subset \mathbb{F}(\alpha_v(P))$, il n'y a rien à montrer. Sinon, on a *a fortiori* l'inclusion stricte

$$\mathbb{F}(\alpha_v(P)) \subsetneq F\left(E[\alpha_v^k], P\right).$$

Les extensions étant galoisiennes, $[F(E[\alpha_v^k], \alpha_v(P)) : \mathbb{F}(\alpha_v(P))]$ divise $[F(E[\alpha_v^k]) : \mathbb{F}] = p$. De plus, par le lemme 27, $F(E[\alpha_v^k], P) = F(E[\alpha_v^k], \alpha_v(P))$, donc on a l'égalité

$$\left[F\left(E[\alpha_v^k], P\right) : \mathbb{F}\left(\alpha_v(P)\right)\right] = p.$$

Ainsi, le morphisme de restriction

$$\mathrm{res} : \mathrm{Gal}\left(F(E[\alpha_v^k], P)/\mathbb{F}(\alpha_v(P))\right) \to \mathrm{Gal}\left(F(E[\alpha_v^k])/\mathbb{F}\right),$$

entre groupes de même cardinaux est un isomorphisme. Soit $\widetilde{\rho}$ un générateur du groupe cyclique $\mathrm{Gal}\left(F(E[\alpha_v^k], P)/\mathbb{F}(\alpha_v(P))\right)$. Il existe un point de α_v-torsion T_1 tel que

$$\widetilde{\rho}(P) = P + T_1.$$

De plus, par le lemme 28, on a l'isomorphisme de I_v-modules, $E[\alpha_v^k] \simeq \mu_{p^k}$, donc si T_2 est un point de $E[\alpha_v^k] \backslash E[\alpha_v^{k-1}]$, alors le point $T_3 = \rho(T_2) - T_2$ est d'ordre p. Finalement, il existe un entier v tel que

$$T_1 = vT_3.$$

On pose $T = -rT_2$. On a alors

$$\rho(P+T) = P + T_1 - v\rho(T_2) = P + vT_3 - vT_3 - vT_2 = P + T.$$

Ceci nous donne bien l'inclusion $\mathbb{F}(P+T) \subset \mathbb{F}(\alpha_v(P))$.

En utilisant (5.5) et (5.7), on obtient

$$[\mathbb{F}(P+T) : \mathbb{F}] \leq [\mathbb{F}(\alpha_v(P) : \mathbb{F}] \leq [\mathbb{E}(\alpha_v(P) : \mathbb{E}] = D.$$

Or par construction, $\mathbb{F}_v \subset \mathbb{Q}_p(\zeta_{m/p})$ et $\mathbb{F} \subset F(E[\alpha_v^k])$, donc

$$\mathfrak{f}_p(\mathbb{F}) \leq \frac{p^k}{p} < \mathfrak{f}_p(F), \text{ et, si } l \neq p, \mathfrak{f}_l(\mathbb{F}) \leq \mathfrak{f}_l(F).$$

On en conclut, que

$$[\mathbb{F}(P+T) : \mathbb{F}] \leq D \text{ et, } \mathfrak{f}(\mathbb{F}) < \mathfrak{f}(F) = \mathfrak{f},$$

ce qui contredit la définition de $\mathfrak{f}$. Ceci conclut la preuve par l'absurde. □

5.4.2 Lemme non-ramifié

On passe maintenant au lemme qui va nous permettre de faire l'extrapolation dans le cas où il n'y a pas beaucoup de ramification. Il s'agit du même lemme que dans le cas multiplicatif.

Lemme 30 *Soit $p \in \mathcal{P}^\star$, il existe $\Phi_p \in \mathrm{Gal}(F/K)$ tel que*

$$| x^p - \Phi_p x |_v \leq p^{-\frac{1}{e_p}},$$

où $x \in \mathcal{O}_F$ et v est une valuation sur $\overline{\mathbb{Q}}$ étendant p.

Démonstration : C'est le lemme 3.1. de [6]. □

5.5 Lemme de Siegel

Dans la suite, on considère un point P_1 qui sera soit P soit $\alpha_v(P)$. On note $\wp(u)$ la coordonnée x de P_1 et on note $\wp(u_1), \ldots, \wp(u_D)$ les différents conjugués de $\wp(u)$ sur F. On dit que les u_i sont *les conjugués de u*.

Soient L et T deux entiers strictement positifs et $N \in]\sqrt{L}, 2\sqrt{L}[$ un nombre premier (qui existe par le "postulat de Bertrand"). On va construire une fonction

$$\varphi(z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) \wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2}$$

avec $p(\lambda_1, \lambda_2) \in \overline{\mathbb{Z}}$ non tous nuls, telle que : φ n'est pas constamment nulle sur $E(\mathbb{C})$, φ est nulle en les conjugués u_i de u avec multiplicité T et les coefficients $p(\cdot, \cdot)$ sont bien controlés. Le premier point est assuré par le choix de N et le fait que les $p(\cdot, \cdot)$ ne sont pas tous nuls, le second découle d'un lemme de Siegel absolu.

Lemme 31 *Soient n un entier et S un sous $\overline{\mathbb{Q}}$-espace vectoriel de dimension d de $\overline{\mathbb{Q}}^n$. Pour tout $\varepsilon > 0$, il existe un vecteur $\boldsymbol{x} \in S$ tel que*

$$h_2(\boldsymbol{x}) \leq \frac{h_2(S)}{d} + \frac{\log d}{2} + \varepsilon.$$

Démonstration : cf. [21] lemme 4.7 et la remarque qui suit. □

Proposition 19 *Soient L, T et k trois entiers positifs tels que $L^2 \geq kT$ et $k^{c_2} > (L + T)^2$ pour une certaine constante absolue $c_2 > 0$. Avec les notations précédentes, on peut*

construire la fonction φ, s'annulant en $u_1, \ldots, u_k$ avec multiplicité supérieure à T, telle que

$$h(\varphi) \leq \frac{ckT}{(L+1)^2 - kT} \left(LN^2 \widehat{h}(P_1) + T \log(T+L) + T \log N + L \right) + \log L,$$

où c est une constante ne dépendant que de E/K.

Démonstration : Par récurrence sur $t \leq T$, on montre qu'il existe un polynôme $Q_{\lambda_1,\lambda_2,t}$ dans $\mathcal{O}_k[X_1, \ldots, X_4]$ de degré partiel en chaque variable majoré par $L + 2t$, à coefficients de valeur absolue majorée par $c_1 k^{c_2 t}$ et tel que

$$\frac{d^t}{dz^t} \left(\wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2} \right) = Q_{\lambda_1,\lambda_2,t} \left(\wp(z), \wp'(z), \wp(Nz), \wp'(Nz) \right).$$

Au rang $t = 0$, le polynôme $Q = X_1^{\lambda_1} X_3^{\lambda_2}$ convient.
Supposons la propriété vraie au rang t et montrons-la au rang $t+1$: en notant abusivement Q_t le polynôme $Q_{\lambda_1,\lambda_2,t}$, on a

$$\begin{aligned} \frac{d^{t+1}}{dz^{t+1}} \left(\wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2} \right) &= \frac{d}{dz} \frac{d^t}{dz^t} \left(\wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2} \right) \\ &= \frac{d}{dz} Q_t \left(\wp(z), \wp'(z), \wp(Nz), \wp'(Nz) \right) \\ &= \frac{\partial Q_t}{\partial X_1} (\cdot)\, \wp'(z) + \ldots + N \frac{\partial Q}{\partial X_4} (\cdot)\, \wp''(Nz). \end{aligned}$$

En utilisant la relation $\wp''(Nz) = 6\wp(Nz)^2 + 2a_4$, on pose donc

$$Q_{t+1} = X_2 \frac{\partial Q_t}{\partial X_1} + \ldots + N(6X_3^2 + 2a_4) \frac{\partial Q_t}{\partial X_4}.$$

On a clairement $\deg_{X_i} Q_{t+1} \leq L + 2(t+1)$. De plus, en notant $q_{i,t}$ les coefficients de Q_t, on a

$$|q_{i,t+1}| \leq 6c_1 N(L+2t) k^{c_2 t} \leq 12 c_1 \sqrt{L}(L+2T) k^{c_2 t} \leq c_1 k^{c_2(t+1)}.$$

Finalement, le système $\forall t \leq T-1$, $\forall i \in [\![1, k]\!]$, $\varphi^{(t)}(u_i) = 0$ s'écrit :

$$\forall t \leq T-1, \quad \forall i \in [\![1,k]\!], \quad \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) Q_{\lambda_1,\lambda_2,t} \left(\wp(u_i), \wp'(u_i), \wp(Nu_i), \wp'(Nu_i) \right) = 0.$$

Pour tout $0 \leq i \leq k$, posons

$$\forall 0 \leq t \leq T-1, \ \forall 0 \leq \lambda_1, \lambda_2 \leq L, \quad \alpha^{(i)}_{(\lambda_1,\lambda_2),t} = Q_{\lambda_1,\lambda_2,t} \left(\wp(u_i), \wp'(u_i), \wp(Nu_i), \wp'(Nu_i) \right).$$

On considère les vecteurs

$$\mathbf{y}_{i,t} = \left(\alpha^{(i)}_{(0,0),t}, \ldots, \alpha^{(i)}_{(L,0),t}, \ldots, \alpha^{(i)}_{(L,L),t} \right) \in \overline{\mathbb{Q}}^{(L+1)^2}.$$

Comme dans [19] p.42 inégalité (18) et suivante, on vérifie que les coefficients du système

$$\mathbf{y}_{i,t} \cdot \mathbf{x} = 0, \quad 0 \leq i \leq k, \quad 0 \leq t \leq T-1$$

avec $\mathbf{x} \in \overline{\mathbb{Q}}^{(L+1)^2}$ sont tous de hauteur au plus

$$c_3 \left(LN^2 \widehat{h}(P_1) + T \log(T+L) + T \log N + L \right).$$

Par ailleurs, le $\overline{\mathbb{Q}}$-espace vectoriel

$$S = \left\{ \mathbf{x} \in \overline{\mathbb{Q}}^{(L+1)^2} \quad / \quad \mathbf{y}_{i,t} \cdot \mathbf{x} = 0, \quad 0 \leq i \leq k, \quad 0 \leq t \leq T-1 \right\}$$

est de dimension $(L+1)^2 - kT$ et les vecteurs $\mathbf{y}_{i,t}$ forment une base de l'orthogonal $S^{\perp}$. De plus, le Lemma IV p.10 de [48], nous indique que

$$h_2(S) = h_2\left(S^{\perp}\right) \leq \sum_{i,t} h_2(\mathbf{y}_{i,t}) \leq c_3 kT \left(LN^2 \widehat{h}(P_1) + T \log(T+L) + T \log N + L \right).$$

On applique le lemme 31 avec $\varepsilon = \frac{1}{2} \log \frac{(L+1)^2}{(L+1)^2 - kT}$. On a ainsi obtenu la fonction voulue, avec des coefficients dans $\overline{\mathbb{Q}}$ et avec la hauteur projective h_2. En fait, en appliquant une remarque de Roy et Thunder [46], on peut également trouver une solution à coefficients entiers algébriques et avec la hauteur h. La remarque consiste à dire que si $x \in \overline{\mathbb{Q}}^n$, il existe $a \in \overline{\mathbb{Q}}$ tel que ax est à coefficients entiers algébriques et tel que $h(ax) = h_2(ax) = h_2(x)$. □

5.6 Extrapolation

Il y a deux cas, selon que l'on a "beaucoup" de premiers ayant "beaucoup" de ramification ou non (ceci étant quantifié). On commence par le cas qui sera utilisé quand il n'y a pas beaucoup de grande ramification.

Proposition 20 *Soient L_1 et T_1 deux entiers strictement positifs d'ordre de grandeur polynomial en D, tels que $L_1^2 \geq DT_1$. On pose $P_1 = P$ et on considère la fonction φ obtenue dans la proposition 19 avec $L = L_1$, $T = T_1$ et $k = D$. Soient $p \in \mathcal{P}^{\star}$ et v une place étendant p sur $\overline{K}$. Pour tout $t \leq \min\{L_1, \frac{T_1}{2}\}$ et pour tout $\tau \in \mathrm{Gal}(\overline{K}/K)$ étendant le morphisme Φ_p du lemme 30, on a*

$$\log \mid \tau(\varphi)^{(t)})(\alpha_p u) \mid_v \leq -\frac{T_1}{2e_p} \log p + 8L_1 \log \max\{1, \mid \wp(N\alpha_v u) \mid_v\}.$$

Démonstration : Il s'agit essentiellement du deuxième pas de [31] à la différence que l'on utilise un lemme de Siegel absolu, ce qui conduit à supposer l'annulation en un point et en tous ses conjugués, ainsi qu'à faire intervenir l'indice de ramification e_p de p dans F. On étend v au corps $\overline{K}(X)$ en posant $\mid X \mid_v = 1$.

Il y a deux cas : soit $\wp(u)$ est un v-entier, soit non.

Cas 1 : on vérifie simplement que l'on peut écrire $\varphi^{(t)}$ comme un polynôme en les variables $\wp(z)$, $\wp(Nz)$, $\frac{\wp'(Nz)}{\wp'(z)}$ de degré partiels en $\wp(Nz)$ et $\frac{\wp'(Nz)}{\wp'(z)}$ respectivement majorés par $3(L_1+t) \leq 6L_1$ et par 1. On en déduit l'existence d'une fraction rationnelle G, telle que $S_N(X)^{8L_1}G(X)$ soit un polynôme à coefficients dans $\mathcal{O}_{\overline{K}}$ et vérifiant

$$G(\wp(z)) = \varphi^{(t)}(z)^2.$$

La fraction rationnelle $G(X)$ admet donc un zéro d'ordre supérieur à T_1 aux points $X = \wp(u_1), \ldots, X = \wp(u_D)$. Notons $\Delta = \sum a_i X^i$ le polynôme minimal unitaire sur F de $\wp(u)$. Par hypothèse sur $\wp(u)$, il est à coefficients entiers algébriques. Ainsi, il existe un polynôme H à coefficients v-entiers, tel que

$$S_N(X)^{8L_1}G(X) = \Delta(X)^{T_1}H(X). \tag{5.8}$$

Si π_p est une uniformisante au-dessus de p dans K et $\pi_{p,F}$ une uniformisante de p dans F, par le petit théorème de Fermat et le lemme 30, on obtient donc

$$\tau(\Delta)(\wp(\alpha_v u)) = \tau(\Delta)(\wp(u)^p) = (\Delta(\wp(u)))^p = 0 \mod \pi_{p,F},$$

et ce, pour tout $\pi_{p,F}$ au-dessus de π_p. En substituant $\wp(\alpha_v u)$ à X dans (5.8) et en appliquant τ aux coefficients des polynômes S, G, H et Δ, on en déduit que le membre de droite de cette égalité transformée par τ est d'ordre en π_p supérieur à $\frac{T_1}{e_p}$. Il reste maintenant à majorer l'ordre en π_p de $\tau(S_N)(\wp(\alpha_v u))$. Or S_N est à coefficients dans K, donc est, de même que R_N, invariant par τ. De plus,

$$\wp(N\alpha_v u) = \frac{R_N(\wp(\alpha_v u))}{S_N(\wp(\alpha_v u))}.$$

D'après le lemme 22, les polynômes R_N et S_N réduits mod π_p sont premiers entre eux. Autrement dit, l'un des deux nombres $R_N(\wp(\alpha_v u))$, $S_N(\wp(\alpha_v u))$ est une unité de $\mathcal{O}_{\overline{K_v}}$. Si c'est $S_N(\wp(\alpha_v u))$, on a fini, sinon, c'est $R_N(\wp(\alpha_v u))$ et donc

$$\mathrm{ord}_{\pi_p}(S_N(\wp(\alpha_v u)) = -\mathrm{ord}_{\pi_p}\wp(N\alpha_v u).$$

Cas 2 : Si $\wp(u)$ n'est pas un v-entier, on fait un changement de carte comme dans le b) du deuxième pas de Laurent [31] : on effectue le changement de variable projectif

$$t = -\frac{X}{Y} \quad \text{et,} \quad s = -\frac{1}{Y}.$$

Alors s s'exprime en fonction du paramètre local t par une série entière $s(t)$ à coefficients v-entiers. On considère cette fois la fonction

$$(\wp'(z)\wp'(Nz))^{-(L_1+t)}\,\varphi^{(t)}(z), \text{ à la place de } \varphi^{(t)}(z)^2.$$

Elle s'écrit comme un polynôme en les variables $-\frac{\wp(z)}{\wp'(z)}$, $-\frac{1}{\wp(z)}$, $-\frac{\wp(Nz)}{\wp'(Nz)}$ et $-\frac{1}{\wp'(Nz)}$. Il existe donc une série entière G, à coefficients v-entiers, telle que

$$G(t) = (\wp'(z)\wp'(Nz))^{-(L_1+t)}\,\varphi^{(t)}(z). \tag{5.9}$$

Soient $\xi = -\frac{\wp(u)}{\wp'(u)}$ le paramètre local associé au point P et Δ le polynôme minimal unitaire de ξ sur F_v. D'après l'hypothèse, le nombre ξ est dans l'idéal maximal $\overline{\mathfrak{m}_v}$, donc tous les coefficients de Δ, sauf le coefficient dominant, sont divisibles par π_p. Le théorème de préparation de Weierstrass montre qu'il existe une série entière H, à coefficients v-entiers, telle que

$$G(t) = \Delta(t)^{(T_1-t)}H(t).$$

Dans cette identité on substitue $t = [\alpha_v](\xi) = \xi^p + \pi_p\psi(\xi)$ par le lemme 23. On conclut alors comme dans le premier cas $\big($il faut savoir majorer

$$\mathrm{ord}_{\pi_p}(\wp'(\alpha_v u)\wp'(N\alpha_v u)) = \mathrm{ord}_{\pi_p}s([\alpha_v](\xi)) + \mathrm{ord}_{\pi_p}s([N\alpha_v](\xi)).$$

Puisque N est premier à p, ces dernières quantités sont toutes deux égales à

$$-\frac{3}{2}\mathrm{ord}_{\pi_p}\wp(N\alpha_v u) \text{ (cf. paragraphes 3 et 6 de [55]).}$$

Remplaçant dans (5.9), z par $\alpha_v u$ et t par $[\alpha_v](\xi)$ on peut alors conclure$\big)$. □

On passe maintenant à la proposition qui nous servira quand il y a beaucoup de grande ramification.

Proposition 21 *Soient L_2 et T_2 deux entiers d'ordre de grandeur polynomial en D et Λ_2 un entier strictement positif, tels que $L_2^2 \geq DT_2\Lambda_2$. On considère la fonction φ obtenue dans la proposition 19 avec $L = L_2$, $T = T_2$, $k = D\Lambda_2$ et avec*

$$\{u_1, \ldots, u_k\} := \{\alpha_v u_i \ / i \in \{1, \ldots, D\} \text{ et } v \text{ décrivant un ensemble } \mathcal{P}_2^\star \text{ de cardinal } \Lambda_2\}\,.$$

Pour tout $t \leq \min\{L_2, \frac{T_2}{2}\}$, pour tout v dans l'ensemble $\mathcal{P}_2^\star$ et pour tout $\tau \in \mathrm{Gal}(\overline{K}/K)$ tel que $\tau_F \in H_p$, $p/v \in \mathcal{P}_2^\star$, on a

$$\log \mid \tau(\varphi^{(t)})(\alpha_p u) \mid_v \leq -\frac{T_2}{2}\log p + 8L_2 \log\max\{1, \mid \wp(N\alpha_v u) \mid_v\}.$$

Démonstration : Là encore il y a deux cas selon que $\wp(u)$ est un v-entier ou non. On commence par le cas où c'est un v-entier. On étend v au corps $\overline{K}(X)$ en posant $\mid X \mid_v = 1$ et on fait la même preuve que précédemment, en montrant cette fois-ci que

$$\tau\left(\Delta_{\alpha_v}\right)\left(\wp(\alpha_v u)\right) = 0 \mod \pi_p,$$

où Δ_{α_v} est le polynôme minimal de $\wp(\alpha_v u)$. Pour montrer ceci, on note $\Delta^{(p)}$ le polynôme minimal de $\wp(u)$ où l'on a élevé les coefficients à la puissance p. On a alors

$$\begin{aligned}
\tau\left(\Delta_{\alpha_v}\right)\left(\wp(\alpha_v u)\right) &= \tau\left(\Delta^{(p)}\right)\left(\wp(\alpha_v u)\right) \mod \pi_p \text{ par le petit théorème de Fermat,} \\
&= \Delta^{(p)}(\wp(\alpha_v u)) \mod \pi_p \text{ par le lemme 29,} \\
&= \Delta^{(p)}(\wp(u)^p) \mod \pi_p, \\
&= (\Delta(\wp(u)))^p \mod \pi_p, \\
&= 0.
\end{aligned}$$

Si $\wp(u)$ n'est pas un v-entier, on utilise le même argument que dans le cas 2 de la proposition 20 précédente pour conclure de la même façon. □

5.7 Conclusion

5.7.1 Le cas du théorème 34

En notant $[\cdot]$ la partie entière, on pose C une constante assez grande (de sorte que les inégalités soient vérifiées) ne dépendant que de E/K et on pose

$$N_1 = \left[C^4 \frac{(\log 2D)^6}{(\log\log 5D)^5}\right] \text{ et } E = \left[C\left(\frac{\log 2D}{\log\log 5D}\right)^2\right].$$

Pour p entre $N_1/2$ et N_1, le théorème de Chebotarev nous indique qu'il y a plus de $\Lambda = \left[\frac{C^4}{2}\left(\frac{\log 2D}{\log\log 5D}\right)^6\right]$ tels p. En notant e_v l'indice de ramification de v dans F, on a : soit il y a plus de $\Lambda_1 = \Lambda/2$ nombres premiers p ayant une place v avec un $e_v \leq E$, soit il y a plus de $\Lambda_2 = \Lambda/2$ nombres premiers p ayant toutes les places v avec un $e_v > E$. On va traiter chaque cas séparément et conclure dans chacun de ces deux cas.

Cas 1 : il y a plein de v ayant peu de ramification, *i.e.*, il y a plus de $\Lambda_1 = \Lambda/2$ nombres premiers p ayant une place v avec un $e_v \leq E$.

Dans ce cas, on note $\mathcal{P}_1^\star$ le sous-ensemble de $\mathcal{P}^\star$ correspondant à Λ_1 et on introduit les paramètres suivants :

$$L_1 = \left[C^3 D \frac{(\log 2D)^5}{(\log\log 5D)^6}\right],\ T_1 = \left[C^{\frac{9}{2}} D \frac{(\log 2D)^7}{(\log\log 5D)^9}\right],\ \text{et, } T_1' = \left[C^3 D \frac{(\log 2D)^4}{(\log\log 5D)^6}\right],$$

et N est un nombre premier tel que $\frac{1}{2}\sqrt{L_1} \leq N \leq \sqrt{L_1}$.

Proposition 22 *Pour tout $p \in \mathcal{P}_1^\star$, pour tout τ étendant Φ_p^{-1} et pour tout $t \leq T_1'$, la fonction $\tau^{-1}\left(\varphi^{(t)}\right)$ de la proposition 20 s'annule en $\alpha_v u$.*

Démonstration : En notant

$$\zeta = \mathrm{N}_{F(P)/F}\left(\tau\left(\varphi^{(t)}\right)(\alpha_v u)\right),$$

on a grâce à la proposition 20,

$$\log \mid \zeta \mid_v \leq -\frac{DT_1 \log p}{2e_v} + 8L_1 \sum_{w/v} D_w \log \max\left(1, \mid \wp(N\alpha_v u \mid_w\right).$$

On en déduit

$$\log \mid \zeta \mid_v \leq -c_{12}\frac{DT_1 \log p}{2E} + DL_1\left(c_{10} + N^2 p\widehat{h}(P)\right).$$

Or par hypothèse sur $\widehat{h}(P)$, on a $N^2 p\widehat{h}(P) \leq N^2 N_1 \widehat{h}(P) \leq c_{11}$. En remplaçant les paramètres par leur valeur, on obtient donc

$$\log \mid \zeta \mid_v \leq -C^{\frac{7}{2}} D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6}.$$

Ainsi, si ζ est non nul,

$$h(\zeta) = h(\zeta)^{-1} \geq \frac{d_v}{d} \log \max\{1, \mid \zeta^{-1} \mid_v\} \geq C^{\frac{7}{2}} D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6}. \tag{5.10}$$

Par ailleurs, un calcul classique (cf. par exemple [19] p.50) permet d'écrire

$$h(\zeta) \leq c_{15} DT_1' \log(T_1' + L_1) + c_{16} DL_1 N^2 p\widehat{h}(P) + c_{17} Dh(\varphi)$$

où $h(\varphi)$ est donnée par la proposition (19) :

$$h(\varphi) \leq \frac{cDT_1}{(L_1+1)^2 - DT_1}\left(L_1 N^2 \widehat{h}(P) + T_1 \log(T_1 + L_1) + T_1 \log N + L_1\right) + \log L_1.$$

en remplaçant les paramètres par leur valeur, on obtient :

$$h(\zeta) \leq c_{15} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6} + c_{16} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6} + c_{17} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6},$$

Soit

$$h(\zeta) \leq c_{18} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6}. \tag{5.11}$$

En comparant les inégalités (5.10) et (5.11), on obtient une contradiction pour C suffisamment grand, ce qui conclut. □

Puisque l'on travaille avec des $p \in \mathcal{P}^\star \subset \mathcal{P}$, on a $[F(\alpha_v(P)) : F] = D$. Donc, on obtient ainsi, en comptant les multiplicités, au moins

$$DT_1'\Lambda_1 \geq \frac{1}{2} C^7 D^2 \frac{(\log 2D)^{10}}{(\log\log 5D)^{12}} \tag{5.12}$$

racines. Or en utilisant la relation

$$\wp(Nz) = \frac{R_N(\wp(z))}{S_N(\wp(z))},$$

on peut écrire φ sous la forme

$$\varphi(z) = F(\wp(z)),$$

où F est une fraction rationnelle de degré majoré par

$$(N^2+1)L_1 \leq 2L_1^2 \leq 2C^6D^2\frac{(\log 2D)^{10}}{(\log\log 5D)^{12}}. \tag{5.13}$$

En comparant (5.12) et (5.13), on en déduit que la fraction F est identiquement nulle. Donc il en est de même pour φ, ce qui est absurde par le choix de N. Le théorème est donc démontré dans ce cas.

Cas 2 : il y a plein de v ayant beaucoup de ramification, *i.e.*, il y a plus de $\Lambda_2 = \Lambda/2$ nombres premiers p ayant toutes les places v avec un $e_v > E$.

Dans ce cas, on note $\mathcal{P}_2^\star$ le sous-ensemble de $\mathcal{P}^\star$ correspondant à Λ_2 et on introduit les paramètres suivants :

$$L_2 = \left[C^{\frac{35}{8}}D\frac{(\log 2D)^7}{(\log\log 5D)^8}\right],\ T_2 = \left[C^{\frac{9}{2}}D\frac{(\log 2D)^7}{(\log\log 5D)^9}\right] \text{ et, } T_2' = \left[C^4D\frac{(\log 2D)^6}{(\log\log 5D)^8}\right],$$

et N est un nombre premier tel que $\frac{1}{2}\sqrt{L_2} \leq N \leq \sqrt{L_2}$.

Proposition 23 *Pour tout $p \in \mathcal{P}_2^\star$, pour tout τ tel que $\tau_F \in H_p$ et pour tout $t \leq T_2'$, la fonction $\tau^{-1}\left(\varphi^{(t)}\right)$ de la proposition 21 s'annule en $\alpha_v u$.*

Démonstration : En notant

$$\zeta = \mathrm{N}_{F(P)/F}\left(\tau\left(\varphi^{(t)}\right)(\alpha_v u)\right),$$

on a grâce à la proposition 21,

$$\log \mid \zeta \mid_v \leq -\frac{DT_2\log p}{2} + 8L_2\sum_{w/v} D_w \log\max\left(1, \mid \wp(N\alpha_v u \mid_w\right).$$

On en déduit

$$\log \mid \zeta \mid_v \leq -c_{12}\frac{DT_2\log p}{2} + DL_2\left(c_{10} + N^2p\widehat{h}(P)\right).$$

Or par hypothèse sur $\widehat{h}(P)$, on a $N^2p\widehat{h}(P) \leq N^2N_1\widehat{h}(P) \leq c_{11}$. En remplaçant les paramètres par leur valeur, on obtient donc

$$\log \mid \zeta \mid_v \leq -c_{13}C^{\frac{9}{2}}D^2\frac{(\log 2D)^7}{(\log\log 5D)^8}.$$

Ainsi, si ζ est non nul, on a

$$h(\zeta) = h(\zeta^{-1}) \geq \frac{d_v}{d} \log \max\{1, \mid \zeta^{-1} \mid_v\} \geq c_{14} C^{\frac{9}{2}} D^2 \frac{(\log 2D)^7}{(\log\log 5D)^8}. \tag{5.14}$$

Par ailleurs, le même calcul que précédemment permet d'écrire

$$h(\zeta) \leq c_{15} D T_2' \log(T_2' + L_2) + c_{16} D L_2 N^2 p\widehat{h}(P) + c_{17} D h(\varphi)$$

où $h(\varphi)$ est donnée par la proposition (19) :

$$h(\varphi) \leq \frac{cD\Lambda_2 T_2}{(L_2+1)^2 - D\Lambda_2 T_2} \Big(L_2 N^2 \widehat{h}(P) + T_2 \log(T_2 + L_2) + T_2 \log N + L_2 \Big) + \log L_2.$$

en remplaçant les paramètres par leur valeur, on obtient :

$$h(\zeta) \leq \left(c_{15} C^4 + c_{16} C^{\frac{35}{8}} + c_{17} C^{\frac{17}{4}} \right) D^2 \frac{(\log 2D)^7}{(\log\log 5D)^8},$$

soit,

$$h(\zeta) \leq c_{18} C^{\frac{17}{4}} D^2 \frac{(\log 2D)^7}{(\log\log 5D)^8}. \tag{5.15}$$

En comparant les inégalités (5.14) et (5.15), on obtient une contradiction, ce qui conclut. □

Puisque l'on travaille avec des $p \in \mathcal{P}^\star \subset \mathcal{P}$, on a $[F(\alpha_v(P)) : F] = D$. Donc, on obtient ainsi, en comptant les multiplicités, au moins

$$EDT_2'\Lambda_2 \geq \frac{1}{2} C^9 D^2 \frac{(\log 2D)^{14}}{(\log\log 5D)^{16}} \tag{5.16}$$

racines. Or en utilisant la relation

$$\wp(Nz) = \frac{R_N(\wp(z))}{S_N(\wp(z))},$$

on peut écrire φ sous la forme

$$\varphi(z) = F(\wp(z)),$$

où F est une fraction rationnelle de degré majoré par

$$(N^2+1)L_2 \leq 2L_2^2 \leq 2C^{\frac{35}{4}} D^2 \frac{(\log 2D)^{14}}{(\log\log 5D)^{16}}. \tag{5.17}$$

En comparant (5.16) et (5.17), on en déduit que la fraction F est identiquement nulle. Donc il en est de même pour φ, ce qui est absurde par le choix de N. Le théorème est donc démontré dans ce cas. Il est donc démontré dans tous les cas. □

5.7.2 Le cas du théorème 35

Pour prouver le théorème 35, on fait essentiellement la même preuve que pour le théorème 34 : on peut faire les mêmes réductions et on a uniquement besoin de la partie non-ramifiée de la preuve précédente. La seule chose qui change est le choix des paramètres permettant de conclure.

En notant $[\cdot]$ la partie entière et C une constante assez grande (de sorte que les inégalités soient vérifiées) ne dépendant que de E/K et de c_0, on pose $E = 1$ et

$$N_1 = \left[3C^2 \frac{(\log 2D)^2}{\log\log 5D}\right].$$

Pour p entre $N_1/2$ et N_1, le théorème de Chebotarev nous indique qu'il y a plus de $\Lambda = \left[\frac{C^2}{2}\left(\frac{\log 2D}{\log\log 5D}\right)^2\right]$ tels p. On note $\mathcal{P}_1^\star$ le sous-ensemble de $\mathcal{P}$ correspondant à Λ et on introduit les paramètres suivants :

$$L_1 = \left[C^2 D \frac{\log 2D}{\log\log 5D}\right],\ T_1 = \left[2CD\frac{\log 2D}{\log\log 5D}\right],\ \text{et, } T_1' = \left[\frac{C^2}{2}D\right],$$

et N est un nombre premier tel que $\frac{1}{2}\sqrt{L_2} \leq N \leq \sqrt{L_2}$.

Le même argument qu'au cas 1 du paragraphe précédent nous permet alors de conclure.

Remarque 22 Notons que bien que la preuve de ce théorème 35 soit moralement la même que celle du théorème de [31], le fait d'utiliser un lemme de Siegel absolu conduit à un choix différent des paramètres pour faire fonctionner l'étape d'extrapolation.

5.8 Application du théorème 34

En fait une version affaiblie du théorème 34 suffit déjà. Précisément, on utilisera le corollaire suivant :

Corollaire 10 *Soient E/K une courbe elliptique à multiplication complexe et ε un réel strictement positif. On note K^{ab} la clôture abélienne de K. Il existe une constante strictement positive $c(E/K, \varepsilon)$ telle que*

$$\forall P \in E(\overline{K})\backslash E_{\mathrm{tors}},\quad \widehat{h}(P) \geq \frac{c(E/K,\varepsilon)}{D^{1+\varepsilon}},$$

où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.

On reprend les notations de l'article [57], et on va montrer comment éviter la seconde partie de la preuve (parties 4.3 et 4.4 et 6 de l'article [57]).

Soient $n \geq r \geq 0$ et $P \in S_{n-r}(C)$. On note $K(P)$ le corps de définition de P. On note $x_i : C \to E$ les applications coordonnées définies par la composition de l'immersion fermée $C \hookrightarrow E^n$ et de la i-ème projection $E^n \to E$. Comme E est à multiplication complexe, on sait que son anneau d'endomorphismes est un ordre $\mathcal{O} = \mathbb{Z}+\tau\mathbb{Z}$ dans un corps quadratique imaginaire. On définit alors n morphismes supplémentaires : $\forall 1 \leq i \leq n$, $x_{n+i} = \tau x_i$. On note

$$\Gamma = \langle x_1, \ldots, x_n \rangle_{\mathrm{End}(E)}$$

le *coordinate module* (définition de [57] p.51) : c'est le $\mathbb{Z}$-module engendré par les x_i avec $1 \leq i \leq 2n$. On considère par ailleurs le $\mathbb{Z}$-module (qui est de rang $2r$ comme il suit du lemma 2. de [57])

$$\Gamma_P := \langle x_1(P), \ldots, x_{2n}(P) \rangle_{\mathrm{End}(E)} .$$

Dans sa proposition 2. de [57], Viada montre que $K\left((\Gamma_P)_{\mathrm{tors}}\right) \subset K(P)$ et elle montre également qu'il existe des éléments $\mathbb{Z}$-linéairement indépendants $g_1, \ldots, g_{2r}$ de Γ_P, définis sur $K(P)$ et engendrant la partie libre de Γ_P. Ainsi on peut écrire pour tout $1 \leq i \leq 2n$,

$$x_i(P) = \sum_{j=1}^{2r} a_{ij} g_j + T_i$$

où T_i est un point de torsion. On pose $\nu_j = (a_{1j}, \ldots, a_{nj})$ et on pose $\mid \nu_j \mid = \max_i \mid a_{ij} \mid$. Avec ces notations on a l'inégalité (19) de [57] :

$$\prod_{i=1}^{2r} \widehat{h}(g_i) \ll \prod_{i=1}^{2r} \mid \nu_i \mid^{-2} . \tag{5.18}$$

Dans son corollary 1. Viada obtient alors l'inégalité

$$d \ll \left(NR \prod_{i=1}^{2r} \mid \nu_i \mid \right)^{\frac{1}{n-r}} \tag{5.19}$$

où $d = [K(P) : K]$ et N et R sont deux entiers tels que $(\Gamma_P)_{\mathrm{tors}} \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/R\mathbb{Z}$. (Ces entiers existent par la proposition 2. de [57].)

Dans son corollary 2. Viada obtient enfin les inégalités

$$(NR)^{1-\varepsilon} \ll d \ll (NR)^{\frac{1}{n-r-1-\varepsilon}}.$$

Ainsi d est borné en fonction de N et si $n - r \geq 3$ on obtient l'inégalité

$$(NR)^{1-\varepsilon} \ll (NR)^{\frac{1}{2-\varepsilon}}$$

Ce qui permet de borner N et donc de conclure. Dans le cas où $n - r = 2$, autrement dit le cas qui nous intéresse réellement, on obtient juste

$$(NR)^{1-\varepsilon} \ll (NR)^{\frac{1}{1-\varepsilon}}$$

ce qui ne permet malheureusement pas de conclure, d'où la nécessité d'une seconde étape assez technique dans l'article [57]. On montre maintenant, et c'est là la nouveauté, comment conclure dans le cas général en utilisant notre corollaire 10 et en réutilisant ce qui a été fait jusqu'à présent. On se place désormais dans le cas où $n - r = 2$. On note $K_N = K\left((\Gamma_P)_{\text{tors}}\right)$. On peut toujours supposer que $K = K(j(E))$, donc K_N/K est une sous-extension abélienne de l'extension abélienne $K\left(E[N]\right)/K$. On pose $D = [K(P) : K_N]$. On a, en utilisant toujours le corollary 2. de [57],

$$D = \frac{d}{[K_N : K]} \ll (NR)^{\frac{1}{1-\varepsilon}}(NR)^{-(1-\varepsilon)} \leq (NR)^{3\varepsilon} \tag{5.20}$$

si ε est suffisamment petit. Par ailleurs, les points $g_1,\ldots,\ g_{2r}$ sont des points d'ordre infini de $E(K(P))$. En appliquant le corollaire 10 puis l'inégalité (5.20), on obtient

$$\prod_{i=1}^{2r} \widehat{h}(g_i) \gg D^{-2r-2r\varepsilon} \gg (NR)^{-6r\varepsilon(1+\varepsilon)} \gg (NR)^{-12n\varepsilon}. \tag{5.21}$$

On a ainsi

$$\begin{aligned}(NR)^{1-\varepsilon} \ll d &\ll \left(NR\prod_{i=1}^{2r} \mid \nu_i \mid\right)^{\frac{1}{2}} \text{ par l'inégalité (5.19)}\\ &\ll (NR)^{\frac{1}{2}}\prod_{i=1}^{2r}\widehat{h}(g_i)^{-\frac{1}{4}} \text{ par l'inégalité (5.18)}\\ &\ll (NR)^{\frac{1}{2}+3n\varepsilon} \text{ par l'inégalité (5.21)}\end{aligned}$$

Ceci permet de conclure la preuve du théorème en prenant ε assez petit.

Chapitre 6

Deux remarques concernant le problème de Lehmer sur les variétés abéliennes

On montre ici que la première partie de la conjecture de Lehmer abélienne (minoration des points engendrant la variété abélienne en terme de l'indice d'obstruction), formulée dans [19] entraîne la seconde partie de cette conjecture (minoration des points non de torsion en fonction du degré du point et de la dimension du plus petit sous-groupe algébrique contenant le point). De même pour le résultat non-conjectural, ce qui permet d'améliorer le précédent meilleur résultat connu, dû à Masser [33], pour la minoration des points d'ordre infini sur les variétés abéliennes de type C.M. Par ailleurs on montre que la conjecture de Lehmer abélienne entraîne la conjecture de Lehmer abélienne multihomogène *a priori* plus forte, telles qu'elles sont énoncées dans [19]. On montre également que toute avancée en direction de la conjecture de Lehmer entraîne une avancée similaire en direction de la conjecture multihomogène. En utilisant le résultat principal de [19] on en déduit, en direction de la conjecture multihomogène, une minoration optimale aux puissances de log près dans le cas des variétés abéliennes de type C.M.

6.1 Sur la conjecture de Lehmer sur les variétés abéliennes

Rappelons la conjecture de Lehmer abélienne, formulée dans [19] conjecture 1.4. On note $\delta_L(P)$ l'indice d'obstruction de P.

Conjecture 20 (David-Hindry) *Soient A/K une variété abélienne de dimension g sur un corps de nombres et L un fibré en droites symétrique ample sur A. Il existe une constante strictement positive $c(A/K, L)$ telle que pour tout point $P \in A(\overline{K})$ d'ordre infini modulo*

toute sous-variété abélienne stricte de A, on a

$$\widehat{h}_L(P) \geq \frac{c(A/K,L)}{\delta_L(P)}. \tag{6.1}$$

De plus, en terme du degré $D = [K(P) : K]$, on a pour tout point $P \in A(\overline{K})$ qui n'est pas de torsion

$$\widehat{h}_L(P) \geq \frac{c(A/K,L)}{D^{\frac{1}{g_0}}}, \tag{6.2}$$

où g_0 est la dimension du plus petit sous-groupe algébrique contenant le point P.

En utilisant le théorème de David et Hindry [19] on obtient un résultat, optimal aux puissances de log près en direction de l'inégalité (6.2) de la conjecture précédente.

Théorème 44 *Si A/K est de type C.M., alors il existe une constante strictement positive $c(A/K,L)$ telle que pour tout point $P \in A(\overline{K})$ d'ordre infini, on a*

$$\widehat{h}_L(P) \geq \frac{c(A/K,L)}{D^{\frac{1}{g_0}}} \left(\log 2D\right)^{-\kappa(g_0)},$$

où $D = [K(P) : K]$, où g_0 est la dimension du plus petit sous-groupe algébrique de A contenant P et où $\kappa(g_0) = (2g_0(g_0+1)!)^{g_0+2}$.

Démonstration : C'est une conséquence immédiate du corollaire 4 de [42] (chapitre 2 de cette thèse) appliqué à la variété $V = \overline{\{P\}}$ image schématique de P dans A sur K. On peut faire une preuve directe (ce qui permet d'utiliser le résultat principal de [19] sans avoir à faire intervenir en plus leur remarque utilisant l'indice d'obstruction) : on commence par le cas où $A = \prod_{i=1}^n A_i^{r_i}$, les A_i étant des variétés abéliennes simples deux à deux non-isogènes et où L est le fibré en droites ample et symétrique associé au plongement

$$A = \prod_{i=1}^n A_i^{r_i} \hookrightarrow \prod_{i=1}^n \mathbb{P}^{r_i}_{n_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^N,$$

les A_i étant plongées dans $\mathbb{P}_{n_i}$ par des fibrés L_i très amples et symétriques. On note G le plus petit sous-groupe algébrique contenant V. On note G^0 la composante connexe de l'identité de G. C'est une sous-variété abélienne de A et elle est donc isogène à $B = \prod_{i=1}^n A_i^{s_i}$ où $0 \leq s_i \leq r_i$. On note alors $\pi : A \to B$ une projection naturelle obtenue par oubli de certaines coordonnées, de sorte que $\pi_{|G}$ est une isogénie. Montrons que l'on est dans les conditions d'application du théorème principal de [19] en prenant comme variété abélienne B et comme point $\pi(P)$.

Si $\pi(P)$ est d'ordre fini modulo une sous-variété abélienne stricte de B, en notant H le plus petit sous-groupe algébrique contenant $\pi(P)$, on a $\dim H < \dim B$. Ainsi $G_1 =$

$G \cap \pi^{-1}(H)$ est un sous-groupe algébrique strict de G (car $\pi_{|G}$ est une isogénie), contenant V. Ceci est absurde.

Si $\pi(P)$ est d'ordre fini, comme π est une isogénie, le point P est aussi d'ordre fini. Ceci est absurde.

Finalement, $\pi(P)$ est un point d'ordre infini modulo toute sous-variété abélienne de B. On peut donc appliquer le théorème principal de [19]. Par ailleurs, la hauteur et le degré sont définis relativement aux plongements

$$A = \prod_{i=1}^{n} A_i^{r_i} \hookrightarrow \prod_{i=1}^{n} \mathbb{P}_{n_i}^{r_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^{N_A} \quad \text{et} \quad B = \prod_{i=1}^{n} A_i^{s_i} \hookrightarrow \prod_{i=1}^{n} \mathbb{P}_{n_i}^{s_i} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^{N_B}.$$

De plus l'application $\overline{\pi} : \prod_{i=1}^{n} \mathbb{P}_{n_i}^{r_i} \to \prod_{i=1}^{n} \mathbb{P}_{n_i}^{s_i}$ est la projection linéaire définie par oubli de coordonnées. Dans ce cas, et pour ces plongements, on a

$$\widehat{h}_{M_B}(\pi(P)) \leq \widehat{h}_M(P) \quad \text{et} \quad \deg \pi(P) \leq \deg P.$$

Ceci nous donne

$$\begin{aligned}
\widehat{h}_M(P) &\geq \widehat{h}_{M_B}(\pi(P)), \quad \text{d'où par le théorème de [19],} \\
&\geq \frac{c(B, M_B)}{(\deg \pi(P))^{\frac{1}{g_0}}} \left(\log 2 \deg \pi(P)\right)^{-\kappa(g_0)} \\
&\geq \frac{c(B, M_B)}{(\deg P)^{\frac{1}{g_0}}} \left(\log 2 \deg P\right)^{-\kappa(g_0)}. \\
&\geq \frac{c'(A, M)}{(\deg P)^{\frac{1}{g_0}}} \left(\log 2 \deg P\right)^{-\kappa(g_0)},
\end{aligned}$$

où on a pris pour $c'(A, M)$ le minimum des $c(B, M_B)$ quand s_i varie dans $[\![0, r_i]\!]$.

Dans le cas général, la variété abélienne A est donnée avec une isogénie ρ vers la variété abélienne $B = \prod_{i=1}^{n} A_i^{r_i}$. Soit P d'ordre infini de la variété abélienne de A. Le point $Q = \rho(P)$ est un point d'ordre infini de la variété abélienne de B. Il résulte facilement de la preuve de la proposition 14. de [40] qu'il existe $c'(A, L)$ tel que

$$\widehat{h}_L(P) \geq c'(A, L) \widehat{h}_M(Q).$$

Ainsi en appliquant le résultat précédent, on en déduit presque l'inégalité voulue : il faut encore remplacer le degré $\deg Q$ par $\deg P$. Or $\deg Q \leq \deg P$. Ceci permet de conclure.□

Ce résultat améliore le meilleur résultat précédemment connu, dû à Masser qui obtient dans [33], pour tout point P d'ordre infini de $A(\overline{K})$:

$$\widehat{h}_L(P) \geq \frac{c(A/K, L)}{D^2 \log 2D}.$$

En faisant la même preuve et en appliquant la partie (6.1) de la conjecture 20 au lieu du théorème de [19], on obtient le

Corollaire 11 *La partie (6.1) de la conjecture 20 entraîne sa partie (6.2).*

6.2 Sur la conjecture de Lehmer multihomogène sur les variétés abéliennes

Soit A/K une variété abélienne de dimension g. Quitte à augmenter un peu K (cf. par exemple [42] lemme 2), on peut supposer (et on suppose) que tous les endomorphismes de A sont définis sur K. On note $\widehat{h}_L$ la hauteur de Néron-Tate sur $A(\overline{K})$ associée à un diviseur ample et symétrique L. Pour tout entier n on pose $L_n = L^{\boxtimes n}$ fibré en droites symétrique ample sur A^n et on note $\widehat{h}_{L_n}$ la hauteur de Néron-Tate associée. On commence par un lemme.

Lemme 32 *Soit $(P_1, \ldots, P_n)$ un point de $A^n(\overline{K})$. On a*

$$\widehat{h}_{L_n}(P_1, \ldots, P_n) = \sum_{i=1}^{n} \widehat{h}_L(P_i).$$

Démonstration : C'est une conséquence formelle des propriétés de fonctorialité des hauteurs de Weil et de la définition de la hauteur de Néron-Tate. □

En utilisant ce lemme, on démontre le résultat suivant :

Théorème 45 *Si A/K est de type C.M., alors, pour tout entier $n \in \mathbb{N}$ il existe une constante $c(A/K, L, n) > 0$ telle que pour tout point $(P_1, \ldots, P_n) \in A^n(\overline{K})$ d'ordre infini modulo toute sous-variété abélienne stricte de A^n, on a :*

$$\prod_{i=1}^{n} \widehat{h}_L(P_i) \geq \frac{c(A/K, L, n)}{D^{\frac{1}{g}}} \left(\log 2D\right)^{-n\kappa(g)},$$

où $D = [K(P_1, \ldots, P_n) : K]$.

Démonstration : Soient $A_1, \ldots, A_n$ des entiers strictement positifs et $Q_1, \ldots, Q_n$ des points de $A(\overline{K})$ tels que pour tout i, $P_i = A_i Q_i$. On a

$$\widehat{h}_{L_n}(Q_1, \ldots, Q_n) = \sum_{i=1}^{n} \widehat{h}_L(Q_i) = \sum_{i=1}^{n} A_i^{-2} \widehat{h}_L(P_i),$$

et,

$$[K(Q_1, \ldots, Q_n) : K]^{\frac{1}{ng}} \leq \left(A_1^{2g} \times \cdots \times A_n^{2g} D\right)^{\frac{1}{ng}}.$$

Le théorème de David-Hindry nous donne alors

$$\sum_{i=1}^{n} A_i^{-2}\widehat{h}_L(P_i) \geq \frac{c(A/K,L,n)}{\left(\prod_{i=1}^{n} A_i^{\frac{2}{n}}\right) D^{\frac{1}{gn}}} \left(\log\left((\prod_{i=1}^{n} A_i)D\right)\right)^{-\kappa(g)}.$$

On pose maintenant, pour tout $1 \leq i \leq n$,

$$x_i = \frac{13\widehat{h}(P_i)}{4\min_j \widehat{h}(P_j)}, \text{ et } A_i = [\sqrt{x_i}].$$

Pour tout i, on a $x_i \geq \frac{13}{4}$ et $x_i \geq A_i^2 \geq \frac{x_i}{3}$. Ainsi,

$$\sum_{i=1}^{n} A_i^{-2}\widehat{h}_L(P_i) \leq \frac{3\times 4}{13} n \min_j \widehat{h}_L(P_j),$$

et

$$\prod_{i=1}^{n} A_i^2 \leq \left(\frac{13}{4\min_j \widehat{h}_L(P_j)}\right)^n \prod_{i=1}^{n} \widehat{h}_L(P_i).$$

Donc,

$$\begin{aligned}
\min_j \widehat{h}_L(P_j) &\geq c_{10}(A/K,L,n) \sum_{i=1}^{n} A_i^{-2}\widehat{h}_L(P_i) \\
&\geq \frac{c_{11}(A/K,L,n)}{\left(\prod_{i=1}^{n} A_i^{\frac{2}{n}}\right) D^{\frac{1}{gn}}} \left(\log 2D\prod_{i=1}^{n} A_i\right)^{-\kappa(g)} \\
&\geq \frac{4c_{11}(A/K,L,n)\min_j \widehat{h}_L(P_j)}{13\prod_{i=1}^{n} \widehat{h}_L(P_i)^{\frac{1}{n}} D^{\frac{1}{gn}}} \left(\log 2D\prod_{i=1}^{n} A_i\right)^{-\kappa(g)}.
\end{aligned}$$

Par ailleurs, on a la majoration

$$\log\prod_{i=1}^{n} A_i \leq n\log\left(\frac{13}{2\min_j \widehat{h}_L(P_j)}\right) + 2\log\prod_{i=1}^{n} \widehat{h}_L(P_i).$$

Or on peut toujours supposer que les $\widehat{h}_L(P_i)$ sont inférieurs à 1, donc,

$$\log\prod_{i=1}^{n} A_i \leq n\log\left(\frac{13}{2\min_j \widehat{h}_L(P_j)}\right).$$

Ainsi,

$$\log 2D\prod_{i=1}^{n} A_i \leq n\log\left(\frac{13D^{\frac{1}{n}}}{2\min_j \widehat{h}_L(P_j)}\right).$$

On en déduit que

$$\prod_{i=1}^{n} \widehat{h}_L(P_i)^{\frac{1}{n}} \geq \frac{c_1(A/K,n)}{D^{\frac{1}{ng}}} \left(\log \frac{D^{\frac{1}{n}}}{\min_j \widehat{h}_L(P_j)} \right)^{-\kappa(g)}.$$

Le point $(P_1, \ldots, P_n)$ étant d'ordre infini modulo toute sous-variété abélienne, les points P_i sont en particulier d'ordre infini sur A. Le résultat inconditionnel de Masser sur la minoration de la hauteur des points sur les variétés abéliennes, theorem de [35], nous donne donc :

$$\log \frac{D^{\frac{1}{n}}}{\min_j \widehat{h}_L(P_j)} \leq c_2(A/K,L,n) \log 2D.$$

Ainsi, on en déduit

$$\prod_{i=1}^{n} \widehat{h}_L(P_i) \geq \frac{c_3(A/K,L,n)}{D^{\frac{1}{g}}} (\log 2D)^{-n\kappa(g)}$$

ce qui conclut. □

Remarque 23 Si au lieu de faire appel au théorème 1.5. de [19] dans la preuve du théorème 45 on applique la conjecture 20, alors on en déduit le résultat suivant :

Théorème 46 *Soient A/K une variété abélienne de dimension g sur le corps de nombres K et L un fibré en droites symétrique ample sur A. Si la conjecture 20 est vraie pour $(A/K, L)$ alors, pour tout entier $n \in \mathbb{N}$ il existe une constante $c(A/K,L,n) > 0$ telle que pour tout point $(P_1, \ldots, P_n) \in A^n(\overline{K})$ d'ordre infini modulo toute sous-variété abélienne stricte de A^n, on a :*

$$\prod_{i=1}^{n} \widehat{h}_L(P_i) \geq \frac{c(A/K,L,n)}{D^{\frac{1}{g}}},$$

où $D = [K(P_1, \ldots, P_n) : K]$.

Remarque 24 En fait dans leur article [19], les auteurs formulent également une conjecture multihomogène du problème de Lehmer abélien. Plutôt que de supposer le point $(P_1, \ldots, P_n)$ d'ordre infini modulo toute sous-variété abélienne stricte de A^n, il supposent les points P_i linéairement indépendants dans A. Précisément ils donnent la conjecture 1.6 suivante :

Conjecture 21 (David-Hindry) *Soient A/K une variété abélienne de dimension g sur un corps de nombres et L un fibré en droites symétrique ample sur A. Pour tout entier $n \in \mathbb{N}$ il existe une constante $c(A/K,L,n) > 0$ telle que pour tout n-uplet $(P_1, \ldots, P_n)$ de points d'ordre infini dans $A(\overline{K})$, End(A)-linéairement indépendants, on a :*

$$\prod_{i=1}^{n} \widehat{h}_L(P_i) \geq \frac{c(A/K,L,n)}{D^{\frac{1}{g}}},$$

où $D = [K(P_1, \ldots, P_n) : K]$.

Dans la formulation de la conjecture 21 qu'ils donnent, David-Hindry écrivent "linéairement indépendants" sans préciser s'il s'agit de $\mathbb{Z}$-linéairement ou de $\mathrm{End}(A)$-linéairement indépendants. Il paraît préférable de préciser. En effet, si on comprend l'assertion "linéairement indépendants" comme $\mathbb{Z}$-linéairement indépendants, alors la conjecture 21 est fausse comme le montre l'exemple suivant : on prend E/K une courbe elliptique à multiplication complexe par un corps quadratique imaginaire contenu dans K. On se donne $\alpha \in \mathrm{End}(E)$ un endomorphisme qui n'est pas la multiplication par un entier, on se donne également un point P_1 d'ordre infini dans $E(\overline{K})$ et pour tout $n \geq 1$, on choisit des points P_n tels que $nP_n = P_1$. Enfin on pose $Q_n = \alpha(P_n)$. Puisque P_1 est d'ordre infini, les points P_n et Q_n sont $\mathbb{Z}$-linéairement indépendants. De plus on a

$$\widehat{h}(P_n)\widehat{h}(Q_n) = \frac{\mathrm{N}(\alpha)}{n^4}\widehat{h}(P_1)^2,$$

et,

$$D_n := [K(P_n, Q_n) : K] = [K(P_n) : K] \leq cn^2.$$

Donc,

$$\widehat{h}(P_n)\widehat{h}(Q_n) \leq \frac{c'}{D_n^2}.$$

Ceci montre que l'hypothèse "$\mathbb{Z}$-linéairement indépendants" est insuffisante.

Par contre en supposant les points $\mathrm{End}(A)$-linéairement indépendants, la situation est bien meilleure. Précisément, on a le

Théorème 47 *La conjecture 20 entraîne la conjecture 21.*

Démonstration : Soit $n > 0$ un entier. Au vu du théorème 46, la seule chose à prouver, est de montrer que l'hypothèse (i) : "les points $(P_1, \ldots, P_n)$ sont $\mathrm{End}(A)$-linéairement indépendants", entraîne l'hypothèse (ii) : "le point $\mathbf{P} = (P_1, \ldots, P_n)$ est d'ordre infini modulo toute sous-variété abélienne stricte de A^n." On va plutôt montrer que non(ii) implique non(i). Si non(ii) est vraie, alors, il existe un endomorphisme φ, non-nul, de A^n tel que $\varphi(\mathbf{P}) = 0$. Or on peut écrire $\varphi(\mathbf{P}) = (\varphi_1(\mathbf{P}), \ldots, \varphi_n(\mathbf{P}))$, où les φ_i sont des morphismes de A^n vers A non tous nuls. On suppose par exemple que φ_1 est non-nul. En notant ψ_i la restriction de φ_1 à la i-eme composante de A^n, on obtient ainsi n endomorphismes de A, $\psi_1, \ldots, \psi_n$, non tous nuls et tels que

$$\sum_{i=1}^{n} \psi_i(P_i) = \varphi_1(\mathbf{P}) = 0.$$

Autrement dit, les points $P_1, \ldots, P_n$ sont $\mathrm{End}(A)$-linéairement dépendants. □

Enfin la même preuve permet de constater que le théorème 46 entraîne un énoncé analogue en remplaçant l'hypothèse "d'ordre infini modulo toute sous-variété abélienne stricte" par "$\mathrm{End}(A)$-linéairement indépendants". Ce dernier résultat à également été montré par Viada [57] proposition 4. dans le cas particulier où A est une courbe elliptique.

Bibliographie

[1] A. Abbes. Hauteurs et discrétude [d'après L. Szpiro, E. Ullmo et S. Zhang]. In *Séminaire Bourbaki Exposé no. 825*. Astérisque, 1997.

[2] F. Amoroso and S. David. Le problème de lehmer en dimension supérieure. In *J. reine angew. Math.*, volume 513, pages 145–179, 1999.

[3] F. Amoroso and S. David. Minoration de la hauteur normalisée des hypersurfaces. In *Acta Arith.*, volume 92, pages 339–365, 2000.

[4] F. Amoroso and S. David. Densité des points à coordonnées multiplicativement indépendantes. In *Ramanujam J.*, volume 5, pages 237–246, 2001.

[5] F. Amoroso and R. Dvornicich. A Lower Bound for the height in Abelian Extensions. In *J. Number Theory*, volume 80, pages 260–272, 2000.

[6] F. Amoroso and U. Zannier. A Relative Dobrowolski Lower Bound over Abelian Extensions. In *Ann. Scuola Norm. Pisa Cl. Sci. (4)*, volume XXIX, pages 711–727, 2000.

[7] S. Ju. Arakelov. Intersection theory of divisors on arithmetic surface. In *Math. USSR Izvstija*, volume 8, pages 1167–1180, 1974.

[8] M. Baker. Canonical heights on elliptic curves over abelian extensions. In *Internat. Math. Res. Notices*, volume 29, pages 1571–1589, 2003.

[9] M. Baker and J. Silverman. A lower bound for the canonical height on abelian varieties over abelian extensions. Disponible sur Mathematics ArXiv à l'adresse : http ://front.math.ucdavis.edu/math.NT/0312393, 2003.

[10] D. Bertrand. Minimal heights and polarizations on group varieties. In *Duke Math. J.*, volume 80, no. 1, pages 223–250, 1995.

[11] D. Bertrand. Minimal heights and polarizations on abelian varieties. Preprint of the MSRI, Berkeley, California, June, 1987.

[12] D. Bertrand and P. Philippon. Sous-groupes algébriques de groupes algébriques commutatifs. In *Illinois J. Math.*, volume 32, pages 263–280, 1988.

[13] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren Der Mathematischen Wissenschaften*. Springer-Verlag, 1992.

[14] E. Bombieri, D. Masser, and U. Zannier. Intersecting a Curve with Algebraic Subgroups of Multiplicative Groups. In *Internat. Math. Res. Notices*, volume 20, pages 1119–1139, 1999.

[15] J. B. Bost. Périodes et isogénies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz). In *Séminaire Bourbaki*, volume 237, pages 115–161. Astérisque, 1996.

[16] J.-B. Bost. Algebraic leaves of algebraic foliations over number fields. In *Publications mathématiques de l'IHÉS*, volume 93, pages 161–221, 2001.

[17] J.-B. Bost, H. Gillet, and C. Soulé. Heights of projective varieties and positive Green forms. In *J. Amer. Math. Soc.*, volume 7, pages 903–1022, 1994.

[18] N. Bourbaki. *Éléments de mathématiques - Algèbre commutative*. Chapitre II. Hermann, 1961.

[19] S. David and M. Hindry. Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M. In *J. Reine Angew. Math.*, volume 529, pages 1–74, 2000.

[20] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes. In *Number theory (Tiruchirapalli, 1996) Contemp. Math., Contemp. Math., Amer. Math. Soc., Providence, RI, (1998).*, volume 210, pages 333–364, 1996.

[21] S. David and P. Philippon. Minoration des hauteurs normalisées des sous-variétés des tores. In *Ann. Scuola Norm. Pisa Cl. Sci. (4)*, volume 28, pages 489–543, 1999.

[22] M. Deuring. Die Zetafunktion einer algebräischen Kurve vom Geschlechte Eins. In *Nachrichten Alad. Wiss.* Göttingen, pages 85–94 (1953), 13–42 (1955), 37–76 (1956), 55–80, (1957).

[23] E. Dobrowolski. On a question of Lehmer and the number of irreductible factors of a polynomial. In *Acta Arith.*, volume 34, pages 391–401, 1979.

[24] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. In *Invent. Math.*, volume 73, pages 349–366, 1983.

[25] W. Fulton. *Intersection Theory*. Springer, seconde edition, 1998.

[26] É. Gaudron. Mesure d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif. Thèse de mathématiques de l'Université Jean Monnet de Saint Étienne, décembre 2001.

[27] H. Gillet and C. Soulé. Arithmetic intersection theory. In *Publ. IHES*, volume 72, pages 94–174, 1990.

[28] H. Gillet and C. Soulé. Characteristic classes for algebraic vector bundles with hermitian metrics I,II. In *Ann. of Math.*, volume 131, pages 163–203 et 205–238, 1992.

[29] M. Hindry. Autour d'une conjecture de Serge Lang. In *Invent. Math.*, volume 94, pages 575–603, 1988.

[30] M. Hindry and J. Silverman. *Diophantine Geometry An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[31] M. Laurent. Minoration de la hauteur de Néron-Tate. In M.-J. Bertin, editor, *Séminaire de théorie des nombrs de* P*aris, 1981-1982*, volume 38, pages 137–152. Progr. Math., 1983.

[32] H. Lehmer. Factorisation of some cyclotomic functions. In *Ann. of Math.*, volume 34, pages 461–479, 1933.

[33] D. Masser. Lettre à Daniel Bertrand du 10 novembre 1986.

[34] D. Masser. Small values of the quadratic part of the néron-tate height. In *Progr. Math.*, volume 12, pages 213–222. Birkhäuser, 1981.

[35] D. Masser. Small values of the quadratic part of the Néron-Tate height on an abelian variety. In *Compositio Math.*, volume 53, no. 2, pages 153–170, 1984.

[36] D. Masser and G. Wüstholz. Periods and minimal abelian subvarieties. In *Ann. of Math. (2)*, volume 137, pages 407–458, 1993.

[37] L. Moret-Bailly. *Pinceaux de variété abéliennes*, volume 129. Astérisque, 1986.

[38] P. Philippon. Sur des hauteurs alternatives I. In *Math. Ann.*, volume 289, pages 255–283, 1991.

[39] P. Philippon. Sur des hauteurs alternatives II. In *Ann. Inst. Fourier (Grenoble)*, volume 44, pages 1043–1065, 1994.

[40] P. Philippon. Sur des hauteurs alternatives III. In *J. Math. Pures Appl.*, volume 74, pages 345–365, 1995.

[41] P. Philippon and M. Waldschmidt. Formes linéaires de logarithmes sur les groupes algébriques commutatifs. In *Illinois J. Math.*, volume 32, pages 281–314, 1988.

[42] N. Ratazzi. Densité de points et minoration de hauteur. In *J. Number Theory*, volume 106/1, pages 112–127, 2004.

[43] N. Ratazzi. Problème de Lehmer pour les hypersurfaces de variétés abéliennes de type C.M. In *Acta Arith.*, volume 113, pages 273–290, 2004.

[44] M. Raynaud. Courbes sur une variété abélienne et points de torsion. In *Invent. Math.*, volume 71, pages 207–234, 1983.

[45] G. Rémond. Intersection de sous-groupes et de sous-variétés I. Prépublication de l'Institut Fourier no. 626, octobre 2003.

[46] D. Roy and J.-L. Thunder. An absolute Siegel's lemma. In *J. Reine Angew. Math.*, volume 476, pages 1–26, 1996.

[47] A. Schinzel. On the products of the conjugates outside the unit circle of an algebraic number. In *Acta Arith.*, volume 24, pages 385–399, 1973.

[48] W. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Matematics*. Springer-Verlag, 1991.

[49] G. Shimura and Y. Taniyama. Complex multiplication of abelian varieties and its applications to number theory. In *Publ. Math. Soc. Japan*, volume 6, 1961.

[50] J. Silverman. A Lower Bound for the Canonical Height on Elliptic Curves over Abelian Extensions. In *J. Number Theory*, volume 104, pages 353–372, 2004.

[51] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 156. Springer, 1999.

[52] C.J. Smyth. On the product of conjugates outside the unit circle of an algebraic integer. In *Bulletin of the London Math. Soc.*, volume 3, pages 169–175, 1971.

[53] C. Soulé. Géométrie d'Arakelov et théorie des nombres transcendants. In *Journées Arithmétiques, 1989 (Luminy), Astérique*, volume 198-200, pages 355–371, 1992.

[54] L. Szpiro, E. Ullmo, and S. Zhang. équidistribution des petits points. In *Invent. Math.*, volume 127, pages 337–347, 1997.

[55] J. Tate. The arithmetic of elliptic curves. In *Invent. Math.*, volume 23, pages 179–206, 1974.

[56] E. Ullmo. Positivité et discrétion des points algébriques sur les courbes. In *Annals of Math.*, volume 147, pages 167–179, 1998.

[57] E. Viada. The intersection of a curve with algebraic subgroups in a product of elliptic curves. In *Ann. Scuola Norm. Pisa Cl. Sci.* Série *(V)*, volume 2, pages 47–75, 2003.

[58] C. Voutier. An effective lower bound for the height of algebraic umbers. In *Acta. Arith.*, volume 74, no. 1, pages 81–96, 1996.

[59] S. Zhang. Positive line bundles on arithmetic varieties. In *J. Amer. Math. Soc.*, volume 8, pages 187–221, 1995.

[60] S. Zhang. Small points and adelic metrics. In *J. Algebraic Geom.*, volume 4, pages 281–300, 1995.

[61] S. Zhang. Equidistribution of small points on abelian varieties. In *Annals of Math.*, volume 147, pages 159–165, 1998.