OXFORD UNIVERSITY PRESS LTD JOURNAL **00** (0000), 1–51
doi:10.1093/OUP Journal/XXX000

Petits points et multiplication complexe

María Carrizosa
Institut de Mathématiques de Jussieu, Paris 6. 4 place Jussieu, 75252 Paris, France.

Abstract: We provide a lower bound for the canonical height of a point P in a CM abelian variety A/K in terms of the degree of the field generated by P over K^{ab}. This bound is a generalization of results by David, Hindry, Baker, Silverman, Ratazzi and others and is the best known result on the way of proving the relative abelian Lehmer conjecture. Moreover, the given bound allows us to prove some particular cases of Zilber-Pink conjecture.

KEY WORDS Canonical height, abelian varieties, Lehmer conjecture

Received

1 Introduction

La hauteur canonique sur une variété abélienne associée à un fibré en droites ample et symétrique est une fonction à valeurs dans les réels positifs qui s'annule exactement sur les points de torsion.

Lorsque la hauteur ne s'annule pas, peut-on trouver une borne inférieure ?

On peut aborder cette question de plusieurs façons différentes. En regardant l'exemple de $\mathbb{G}_{\mathrm{m}}$, du fait que la hauteur de Weil vérifie $h(x^m) = |m|h(x)$ pour tout entier m, on voit facilement en prenant $x = 2^{\frac{1}{m}}$ que la hauteur peut tendre vers zéro lorsque m tend vers l'infini. Puisque dans cet exemple m est de l'ordre du degré de définition D de x sur $\mathbb{Q}$, on peut imaginer une borne inférieure de la forme $\frac{c}{f(D)}$ où f est une fonction croissante en D et c une constante qui ne dépend pas de x. D'autres approches cherchent plutôt à fixer le corps de définition de x et expliciter la constante c.

"Le Problème de Lehmer" s'inscrit dans la première approche et on peut le formuler de la façon suivante :

Conjecture 1.1. *Il existe une constante $c > 0$ telle que, pour tout α dans $\bar{\mathbb{Q}}^*$ qui n'est pas une racine de l'unité, on ait*

$$h(\alpha) \geq \frac{c}{D}$$

où $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Le meilleur résultat connu jusqu'à présent dans la direction de cette conjecture est un théorème de Dobrowolski (voir (Dob79)), qui démontre la borne désirée pour $h(\alpha)$ "à ϵ près", à savoir

Théorème 1.2 (Dobrowolski)**.** *Il existe une constante $c > 0$ telle que, pour tout $\alpha \in \bar{\mathbb{Q}}^*$ qui n'est pas une racine de l'unité, on ait*

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

Dans d'autres cas particuliers le problème de Lehmer a été résolu ; notamment si α appartient à une extension abélienne de $\mathbb{Q}$. Dans ce contexte Amoroso et Dvornicich ((AD00)) donnent un résultat plus fort :

Théorème 1.3 (Amoroso-Dvornicich)**.** *Pour tout α dans $\mathbb{Q}^{\mathrm{ab}}$ qui n'est pas une racine de l'unité,*

$$h(\alpha) \geq \frac{\log 5}{12}.$$

En dimension supérieure, ces questions se généralisent de façon naturelle aux groupes algébriques commutatifs, donc aux variétés abéliennes. Dans le cadre du problème classique de Lehmer, les généralisations du résultat de Dobrowolski sont des théorèmes de Laurent ((Lau83)) pour le cas d'un point dans une courbe elliptique à multiplication complexe et de David et Hindry (DH00) pour un point dans une variété abélienne à multiplication complexe. Plus précisément ces derniers montrent :

Théorème 1.4 (David-Hindry)**.** *Soit A une variété abélienne définie sur K de dimension g à multiplication complexe, munie d'un fibré $\mathcal{L}$ ample et symétrique et $\hat{h}_{\mathcal{L}}$ la hauteur canonique associée. Il existe une constante $c(A,K,\mathcal{L})$ telle que pour tout $P \in A(\bar{K})$ d'ordre infini modulo toute sous-variété abélienne propre de A,*

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{c(A,K,\mathcal{L})}{D^{\frac{1}{g}}} \left(\frac{\log\log(3D)}{\log(3D)}\right)^{\kappa(g)},$$

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

Les auteurs démontrent en fait un résultat plus fort puisqu'ils ont remplacé le degré par un invariant plus naturel, *l'indice d'obstruction* $\omega_K(P)$ défini comme suit :

$$\omega_K(P) = \min\{\deg_{\mathcal{L}}(Z)^{\frac{1}{\operatorname{codim} Z}}\}$$

où Z parcourt les sous-variétés propres de A, définies sur K et K-irréductibles contenant le point P.

Des résultats équivalents existent pour un tore multiplicatif $\mathbb{G}_{\mathrm{m}}^n$, lorsque les coordonnées d'un point $\alpha \in \mathbb{G}_{\mathrm{m}}^n$ ne sont pas multiplicativement liées (voir (AD99)).

Les résultats d'Amoroso et Dvornicich ont aussi été étendus par Silverman et Baker ((BS04), (Bak03)) au cadre des variétés abéliennes.

La question qu'on se pose ensuite est d'unifier ces deux types de résultats : l'approximation de Dobrowolski et le théorème d'Amoroso et Dvornicich. Amoroso et Zannier (voir (AZ00)) trouvent dans ce sens :

Théorème 1.5 (Amoroso-Zannier)**.** *Soit K un corps de nombres. Alors pour tout nombre algébrique α non nul qui n'est pas une racine de l'unité on a*

$$h(\alpha) \geq \frac{c(K)}{D} \left(\frac{\log\log(5D)}{\log(2D)}\right)^{13}$$

où $D = [K^{\mathrm{ab}}(\alpha) : K^{\mathrm{ab}}]$ et $c(K)$ est une constante strictement positive qui ne dépend que de K.

De récents travaux de Delsinne (Del07) donnent une généralisation de ce théorème* pour un point α dans $\mathbb{G}_{\mathrm{m}}^n$ à coordonnées multiplicativement indépendantes.

Dans le cas abélien, l'équivalent du théorème 1.5 en dimension supérieure reste encore à démontrer. On connaît des résultats en dimension 1, notamment pour une courbe elliptique de type CM (voir (Rat04)).

Théorème 1.6 (Ratazzi)**.** *Soit E/K une courbe elliptique admettant des multiplications complexes. Il existe une constante strictement positive $c(E,K)$ telle que pour tout point $P \in E(\bar{K}) \setminus E_{\mathrm{tors}}$ on a*

$$\hat{h}(P) \geq \frac{c(E,K)}{D} \left(\frac{\log\log 5D}{\log 3D}\right)^{13},$$

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

Dans le cadre général, la meilleure conjecture qu'on peut espérer est la suivante :

Conjecture 1.7 (David)**.** *Soit A une variété abélienne définie sur K munie d'un fibré $\mathcal{L}$ ample et symétrique. Alors il existe une constante strictement positive c telle que, pour tout point P de $A(\bar{K})$ qui n'est pas de torsion sur $\operatorname{End}_{\bar{K}}(A)$, on a*

$$\hat{h}_{\mathcal{L}}(P) \geq cD^{-\frac{1}{g}}$$

où $D = [K_{\mathrm{tors}}(P) : K_{\mathrm{tors}}]$ et $K_{\mathrm{tors}} = K(A_{\mathrm{tors}})$.

Pour voir que cette conjecture est la meilleure possible en fonction de D, on peut regarder une suite de points de n-division P_n de P ($[n]P_n = P$). D'après les propriétés de la hauteur on a $\hat{h}_{\mathcal{L}}(P_n) = n^{-2}\hat{h}_{\mathcal{L}}(P)$ et $D_n = [K_{\mathrm{tors}}(P_n) : K_{\mathrm{tors}}] \leq cn^{2g}$. On en déduit pour un réel x positif

$$D_n^x \hat{h}(P_n) \leq cn^{2(gx-1)}$$

et donc, si $x < \frac{1}{g}$, lorsque n tend vers l'infini on a $D_n^x \hat{h}_{\mathcal{L}}(P_n) \to 0$.

*Dans (Del07) on trouve l'équivalent du théorème de (AZ00) pour un point dans $\mathbb{G}_{\mathrm{m}}^n$ sous une hypothèse technique. Dans une communication personnelle l'auteur m'indique avoir amélioré son résultat et pouvoir maintenant se passer de l'hypothèse technique, quitte à modifier l'exposant du terme en $\log D$.

D'autre part, dire que P est de torsion sur $\mathrm{End}_{\bar{K}}(A)$ revient à dire qu'il appartient à un translaté par un point de torsion d'une sous-variété abélienne B propre de A et on voit facilement que dans ce cas on ne peut pas espérer avoir $-1/g$ en exposant de D mais $-1/g_0$ où g_0 est la dimension de B. En effet il suffit de prendre $A = E \times E$ un produit de courbes elliptiques et $Q_n = (P_n, 0)$ où P_n est un point de n-division de P. Dans ce cas on a $\hat{h}_{\mathcal{L}}(Q_n) = \frac{1}{n^2}\hat{h}_{\mathcal{L}}(P)$ et $[K_{\mathrm{tors}}(Q_n) : K_{\mathrm{tors}}] \leq cn^2$, donc on ne peut pas remplacer $g_0 = 1$ par $g = 2$.

Le résultat principal de cet article donne une preuve de cette conjecture à “epsilon près”, dans le cas où la variété abélienne admet des multiplications complexes, à savoir :

Théorème 1.8. *Soit A une variété abélienne définie sur K à multiplication complexe, munie d'un fibré $\mathcal{L}$ ample et symétrique. Alors pour tout $\epsilon > 0$ il existe une constante positive $c(A, K, \mathcal{L}, \epsilon)$ telle que, pour tout point P de $A(\bar{K})$ qui n'est pas de torsion sur $\mathrm{End}_{\bar{K}}(A)$, on a*

$$\hat{h}_{\mathcal{L}}(P) \geq c(A, K, \mathcal{L}, \epsilon) D^{-\frac{1}{g}-\epsilon}$$

où $D = [K_{\mathrm{tors}}(P) : K_{\mathrm{tors}}]$ et $K_{\mathrm{tors}} = K(A_{\mathrm{tors}})$.

Ce dernier résultat s'applique notamment à la conjecture de Zilber-Pink. Les premiers cas de cette conjecture ont été suggérés par Bombieri, Masser et Zannier dans (BMZ99). Plus tard, des généralisations ont été données indépendamment par Zilber pour les variétés semi-abéliennes et Pink pour les variétés de Shimura mixtes. Dans le cadre des variétés abéliennes on peut l'énoncer ainsi :

Conjecture 1.9. *Soient A une variété abélienne définie sur un corps K de caractéristique 0 et X une sous-variété fermée et intègre qui n'est contenue dans aucun sous-groupe algébrique propre de A. Alors l'ensemble*

$$X(K) \cap \bigcup_{\mathrm{codim} G \geq \dim X+1} G(K)$$

où l'union porte sur tous les sous-groupes algébriques de A vérifiant la condition de dimension, n'est pas dense dans X.

Dans (Rém05) et (Rém07) G. Rémond montre que cette conjecture est vraie sous l'hypothèse plus forte que X est géométriquement non dégénérée et que A vérifie la conjecture 1.7. Dans sa preuve on voit que même un résultat optimal “à epsilon près” suffit pour conclure. En utilisant le théorème 1.8 on a le résultat suivant

Théorème 1.10. *Soient A une variété abélienne CM définie sur un corps de nombres K, X une sous-variété fermée et intègre de A géométriquement non dégénérée et Γ un sous-groupe de rang fini de $A(K)$. Alors l'ensemble $X(K) \cap (\Gamma + \bigcup_{\mathrm{codim} G \geq \dim X+1} G(K))$ n'est pas dense dans X (où l'union porte sur tous les sous-groupes algébriques de A vérifiant la condition de dimension).*

D'après le corollaire 1.1 de (Rém05) et le théorème 1.8 on a en particulier le corollaire suivant :

Corollaire 1.11. *Soit A/K une variété abélienne CM et C une courbe transverse sur A. Alors l'ensemble $C(K) \cap \bigcup_{\mathrm{codim} G \geq 2} G(K)$ est fini, où l'ensemble porte sur tous les sous-groupes algébriques de A vérifiant la condition de dimension.*

Ce théorème implique notamment le résultat de N. Ratazzi (voir théo. 1.7 (Rat08)) obtenu dans le cas où A est une variété abélienne à multiplication complexe, isogène à la puissance d'une variété abélienne simple.

Ces généralisations forment actuellement un sujet très actif de recherche où de nombreuses questions sont ouvertes.

La démonstration du théorème 1.10 de (Rém05) utilise le théorème 1.8 (à ceci près qu'il s'agissait d'une conjecture) indirectement. Il faut d'abord en déduire une minoration d'un produit de hauteurs d'une famille de points auxiliaires (des générateurs bien choisis de $A(K(P))$). Ensuite il faut étudier les relations liant les coordonnées du point P avec les sous-groupes algébriques de A pour en déduire une majoration du degré du plus petit sous-groupe algébrique de A contenant P. Si on dispose d'une borne pour $\hat{h}(P)$ qui tient compte de la plus petite sous-variété de torsion passant par P on pourra simplifier significativement cette preuve. Pour faire ceci on va utiliser un indice d'obstruction différent de celui employé dans (DH00) et (AD99).

Définition 1.12. *Soient $(A, \mathcal{L})$ une variété abélienne polarisée définie sur K, V une sous-variété de A définie sur K et K-irréductible, P un point de $V(\bar{K})$ et K' une extension de K. On appelle indice d'obstruction de P sur K' par rapport à V noté $\omega_{K'}(P, V)$, la quantité*

$$\omega_{K'}(P, V) = \min \left\{ \left(\frac{\deg_{\mathcal{L}}(Z)}{\deg_{\mathcal{L}}(V)} \right)^{\frac{1}{\mathrm{codim}_V Z}}, P \in Z \right\}$$

où Z est une sous-variété propre de V, définie sur K' et K'-irréductible. Lorsque Z est de codimension 0 dans V on utilisera la convention $\left(\frac{\deg_{\mathcal{L}}(Z)}{\deg_{\mathcal{L}}(V)}\right)^{\frac{1}{\operatorname{codim}_V Z}} = +\infty$.

On remarque que

$$\omega_{K'}(P, A) \leq \omega_{K'}(P) \leq (\deg_{\mathcal{L}} A)\omega_{K'}(P, A)$$

et de même,

$$\omega_{K'}(P, V) \leq \left(\frac{D}{\deg_{\mathcal{L}}(V)}\right)^{\frac{1}{\dim V}} \quad \text{où} \quad D = [K'(P) : K'].$$

Pour voir ceci, il suffit de considérer la variété $W = \{\sigma(P),\ \sigma \in \operatorname{Gal}(\bar{K}'/K')\}$.

Cet indice a de plus la propriété d'avoir le même type d'homogénéité que la hauteur par rapport au fibré choisi. En effet, d'après les propriétés du degré (voir paragraphe 2.2),

$$\begin{aligned}\omega_{\mathcal{L}^{\otimes m}}(P, V) &= \min\left(\frac{\deg_{\mathcal{L}^{\otimes m}}(Z)}{\deg_{\mathcal{L}^{\otimes m}}(V)}\right)^{\frac{1}{\operatorname{codim}_V Z}} = \min\left(\frac{m^{\dim Z}\deg_{\mathcal{L}}(Z)}{m^{\dim V}\deg_{\mathcal{L}}(V)}\right)^{\frac{1}{\operatorname{codim}_V Z}}\\ &= m^{-1}\omega_{\mathcal{L}}(P, V)\end{aligned}$$

ce qui correspond à la formule $\hat{h}_{\mathcal{L}^{\otimes m}}h(P) = m\hat{h}_{\mathcal{L}}(P)$ pour la hauteur (on a noté en indice le fibré par rapport auquel on calcule le degré).

On énonce maintenant une conjecture plus générale qui regroupe tous les énoncés antérieurs :

Conjecture 1.13. *Soit A une variété abélienne de dimension g définie sur un corps de nombres K, munie d'un fibré $\mathcal{L}$ ample et symétrique. Soit H une sous-variété abélienne de A définie sur K et $P \in H(\bar{K})$ d'ordre infini modulo toute sous-variété abélienne propre de H. Alors il existe une constante $c(A, K, \mathcal{L})$ strictement positive telle que*

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{c(A, K, \mathcal{L})}{\omega_{K_{\text{tors}}}(P, H)}.$$

Dans cet énoncé, K_{tors} est l'extension engendrée par tous les points de torsion de A. On remarque que la constante ne dépend pas de H.

On donne à présent un autre énoncé équivalent (voir prop. 2.6) à la conjecture 1.13.

Conjecture 1.14. *Soit A une variété abélienne définie sur un corps de nombres K, munie d'un fibré $\mathcal{L}$ ample et symétrique, P un point de $A(\bar{K}) \setminus A(\bar{K})_{\text{tors}}$ et H la plus petite sous-variété de torsion*[†] *de A définie sur K contenant le point P. Alors il existe une constante $c(A, K, \mathcal{L})$ strictement positive telle que*

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{c(A, K, \mathcal{L})}{\omega_K(P, H)}.$$

On voit immédiatement sur la définition de $\omega_{K_{\text{tors}}}(P, A)$ que la conjecture 1.13 implique la conjecture 1.7. Le but de cette thèse est de montrer la conjecture 1.13 à ϵ-près pour des variétés abéliennes CM. De façon précise on montrera :

Théorème 1.15. *Soit A une variété abélienne définie sur un corps de nombres K à multiplication complexe, munie d'un fibré $\mathcal{L}_0$ ample et symétrique et posons $\mathcal{L} = \mathcal{L}_0^{\otimes 4}$. Soit H une sous-variété abélienne de A définie sur K de dimension $g_0 > 0$ et $P \in H(\bar{K})$ tel que P soit d'ordre infini modulo toute sous-variété abélienne propre de H. Alors il existe une constante ne dépendant que de A, K et $\mathcal{L}$ telle que*

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{c(A, K, \mathcal{L})}{\omega_{K_{\text{tors}}}(P, H)}\left(\frac{\log\log \omega_{K_{\text{tors}}} \deg_{\mathcal{L}}(H)^2}{\log \omega_{K_{\text{tors}}} \deg_{\mathcal{L}}(H)^2}\right)^{\kappa_1(g_0)},$$

où $\omega_{K_{\text{tors}}} = \omega_{K_{\text{tors}}}(P, H)$ et $\kappa_1(g_0) = 2^{2g_0+1}g_0^{4g_0}(g_0+1)!^{2g_0}$.

Remarque 1.16. *L'hypothèse de multiplication complexe est imposée d'une part pour assurer que les endomorphismes de Frobenius se relèvent inconditionnellement en des endomorphismes en caractéristique 0 de A. On pourrait donc penser à une autre hypothèse assurant qu'il y ait "beaucoup" de places v telles que* Frob_v^r *se relève en un endomorphisme de A (pour r fixé) ; c'est le cas si $A = E^n$ où E est une courbe elliptique vérifiant la conjecture de Lang-Trotter (voir (LT76), (FM96), (Elk87)).*

D'autre part, on l'utilise aussi de manière cruciale dans les réductions (paragraphe 3). Il paraît donc peu probable de se passer de cette hypothèse en suivant une preuve similaire.

[†]Une sous-variété de torsion est une union de translatés de sous-variétés abéliennes par des points de torsion.

La démonstration suit les étapes classiques d'une preuve diophantienne qu'on verra ci-dessous.

Dans la première partie (2.2, 2.3, 2.4), on donne tout d'abord quelques rappels concernant la hauteur d'un point dans une variété, le degré géométrique d'une variété et les endomorphismes de Frobenius ainsi que les propriétés associées à ces outils dont on aura besoin. On trouvera les préliminaires nécessaires sur les sous-variétés de torsion et les congruences qu'on utilisera lors de l'extrapolation (paragraphe 2.5).

Dans le paragraphe 3 on expliquera les réductions faites pour simplifier la preuve du théorème 1.15. L'idée de ces réductions a son origine dans l'article de F. Amoroso et U. Zannier (AZ00), paragraphe 2 ; toutefois de nombreuses complications apparaissent. On utilisera des réductions galoisiennes et on étudiera en détail certaines extensions engendrées par des points de torsion de H. On utilisera aussi de façon cruciale le fait que le groupe formel $\hat{A}$ de A est isomorphe comme $\mathrm{Gal}(\bar{K}_v/K_v^{\mathrm{nr}})$-module au tore formel $\hat{\mathbb{G}}_{\mathrm{m}}^g$ et donc $\hat{A}[p^k] \simeq \hat{\mathbb{G}}_{\mathrm{m}}^g[p^k]$ (comme $\mathrm{Gal}(\bar{K}_v/K_v^{\mathrm{nr}})$-modules).

Dans le paragraphe 4 on construit la fonction auxiliaire et dans le paragraphe 5 on procède à l'extrapolation. Il faut séparer deux cas (comme dans (AZ00)) qu'on appelle "peu" ou "très ramifié". Pour le cas peu ramifié, on suit l'approche de (DH00) en extrapolant sur des conjugués de transformés par des endomorphismes de Frobenius du point initial. Dans le cas très ramifié, on suit plutôt l'approche de (Amo) en utilisant des déterminants.

Dans le paragraphe 6, on donne le lemme de zéros qui ne permet pas de conclure immédiatement (contrairement au cas de la dimension 1). Après un choix de paramètres convenable (7), il faut faire un argument de descente (paragraphe 8) proche de celui de (DH00) en rajoutant un nouvel ingrédient : une suite de corps de définition pour les sous-variétés construites. Cette construction produit deux variétés "emboîtées" de même dimension et on compare leurs degrés. Si la descente s'arrête sur un nombre premier peu ramifié, l'argument fonctionne comme dans (DH00) (la comparaison des degrés entraîne une contradition) et on conclut. Si au contraire le premier est très ramifié, la comparaison peut être insuffisante lorsque les variétés sont des translatés d'une sous-variété abélienne B de H. C'est précisément cette situation que les réductions devraient permettre d'exclure. Malheureusement, ce n'est pas le cas. Le point de départ des réductions dans le cas de la dimension 1 ((AZ00) et (Rat04)) était la négation du théorème principal. Dans le contexte des variétés abéliennes il s'agirait de l'existence d'une extension finie $\mathbb{L} \subseteq K_{\mathrm{tors}}$ et d'un point P tels que $\hat{h}(P) < c\left(\frac{\deg H}{[\mathbb{L}(P):\mathbb{L}]}\right)^{\frac{1}{g_0}-\epsilon}$. Dans notre cas, on dispose seulement d'une inégalité de la forme $\hat{h}(P) < \frac{c}{\omega_{K_{\mathrm{tors}}}(P,H)^{1+\epsilon}}$ ce qui est plus faible et ne suffit pas pour effectuer les réductions nécessaires.

Dans le paragraphe 9 on explique comment utiliser les réductions pour contourner le problème cité plus haut. On fait tourner deux fois la construction jusqu'ici exposée. On démontre d'abord un résultat de la forme

$$\hat{h}(P) \geq c\left(\frac{\deg H}{[\mathbb{L}(P):\mathbb{L}]}\right)^{\frac{1}{g_0}-\epsilon} \tag{1}$$

pour tout P et toute extension $\mathbb{L} \subseteq K_{\mathrm{tors}}$, par récurrence sur la dimension de H et en utilisant les réductions du paragraphe 3. On relance la preuve une deuxième fois et si jamais on se retrouve dans le cas défavorable, on montre que $B = 0$ et que l'on dispose d'une majoration de $[\mathbb{L}(P):\mathbb{L}]$ en fonction de $\omega_{\mathbb{L}}(P,H)$. On conclut en remplaçant ce degré dans la borne (1).

2 Résultats préliminaires

2.1 Notations

On fixe une fois pour toutes les notations suivantes :

K un corps de nombres;
$\mathcal{O}_K$ l'anneau des entiers de K;
M_K l'ensemble des places de K;
n_v le degré local $[K_v : \mathbb{Q}_v]$, pour $v \in M_K$;
$N(v)$ le cardinal du corps résiduel de K en v;
$\mathcal{O}_v$ l'anneau des entiers du complété K_v de K en v;
$|\cdot|_v$ la valeur absolue normalisée sur K telle que pour $v|p$, $|p|_v = p^{-1}$ et $|2|_v = 2$ pour $v|\infty$;
h la hauteur absolue logarithmique $h : \mathbb{P}^n(\bar{\mathbb{Q}}) \to \mathbb{R}$, définie par
$h(x_0, ..., x_n) = \dfrac{1}{[K:\mathbb{Q}]} \displaystyle\sum_{v \in M_K} n_v \log \max\{|x_0|_v, ..., |x_n|_v\}$; on notera $h_{\varphi_{\mathcal{L}}}(P)$ ou $h(P)$ s'il n'y a pas de confusions, la hauteur du point $\varphi_{\mathcal{L}}(P)$, où $\varphi_{\mathcal{L}}$ est un plongement de A dans $\mathbb{P}^n$ associé au fibré $\mathcal{L}$;
$\hat{h}_{\mathcal{L}}(P)$ la hauteur canonique associée à $h_{\mathcal{L}}$ définie par
$\hat{h}_{\mathcal{L}}(P) = \lim\limits_{n\to\infty} \dfrac{h_{A,\mathcal{L}}([2^n]P)}{4^n}$
π_v l'idéal premier de $\mathcal{O}_K$ correspondant à la place finie v de K;
$\mathcal{P}$ l'ensemble des nombres premiers >2 qui se décomposent totalement dans K;
t_U l'application translation par le point U;
G_V le stabilisateur de V où V est une sous-variété de A, *i.e*
$G_V = \{P \in A, P + V \subseteq V\}$.
K_{tors} l'extension de K engendrée par les points de torsion de A.

Remarque 2.1.
- *Soit $v \in M_K$, telle que $v|p$, $p \in \mathcal{P}$ et K' une extension galoisienne de K. Soit v' une place de K' au-dessus de v. On sait que l'indice de ramification $e_{v'/v}$ ne dépend pas de v' mais seulement de v, de plus, vu que p se décompose totalement dans K, $e_{v'/v} = e_{v'/p}$.*
- *En général $N(v) = p^{f_v}$, où f_v est le degré résiduel de π_v dans K, donc pour $p \in \mathcal{P}$ et $v|p$ on a $N(v) = p$.*

2.2 Généralités sur les sous-variétés des variétés abéliennes

Soit A une variété abélienne de dimension g munie d'un fibré en droites $\mathcal{L}_0$ ample et symétrique. Dans toute la suite, on va fixer un plongement de A dans un espace projectif $\mathbb{P}^n$ par un choix de sections globales du fibré $\mathcal{L} = \mathcal{L}_0^{\otimes 4}$.

On rappelle qu'un plongement $\rho : A \hookrightarrow \mathbb{P}^n$ est projectivement normal si l'image de A dans $\mathbb{P}^n$ est une variété projectivement normale, c'est à dire si son anneau des coordonnées homogènes est intégralement clos. De façon équivalente, $A \subseteq \mathbb{P}^n$ est projectivement normale si et seulement si elle est normale et pour tout $r \geq 0$, la flèche $\Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(r)) \to \Gamma(A, \mathcal{O}_A(r))$ est surjective (voir (Har77), I.ex. 3.17, ex. 3.18, II.ex. 5.14). De plus, si $\mathcal{L}_0$ est ample alors $\mathcal{L} = \mathcal{L}_0^{\otimes n}$ est projectivement normal pour tout $n \geq 3$ (voir (BL04), chapitre 7.3, p. 187).

Si V est une sous-variété de A, on note $\deg_{\mathcal{L}}(V)$ le degré de V relativement à $\mathcal{L}$, c'est à dire le degré du 0-cycle $c_1(\mathcal{L})^d \cap [V]$ où $d = \dim V$. On a repris ici les notations de (Ful84). Pour les définitions précises, voir (Ful84), chapitre 1.4, p. 11–14, chapitre 2.4 p. 35–41 et chapitre 2.5, pp41-43. Les propriétés principales dont on aura besoin par la suite, sont les suivantes (voir (Ful84) prop. 2.3 et prop. 2.5) :

(i). On note $A_k(X)$ le groupe de k-cycles sur X de dimension k. Il y a un homomorphisme

$$c_1(\mathcal{L}) \cap \_ : A_k(X) \to A_{k-1}(X).$$

(ii). (Additivité) Si $\mathcal{L}$ et $\mathcal{L}'$ sont deux fibrés en droites sur X et V une sous-variété de X, alors

$$c_1(\mathcal{L} \otimes \mathcal{L}') \cap [V] = c_1(\mathcal{L}) \cap [V] + c_1(\mathcal{L}') \cap [V].$$

(iii). (Formule de projection) Si $f : X' \to X$ est un morphisme propre, $\mathcal{L}$ un fibré en droites sur X et V une sous-variété de X, alors

$$f_*(c_1(f^*\mathcal{L}) \cap [V]) = c_1(\mathcal{L}) \cap [f_*(V)].$$

On utilisera le définition suivante :

Définition 2.2. *Soit $\mathcal{R}$ l'anneau des coordonnées de $\mathbb{P}^n$, V une sous-variété de A et L un entier positif. On dit que V est définie incomplètement par des équations de degré $\leq L$ si V est une composante isolée de $A \cap \mathcal{Z}(\mathcal{J})$ où $\mathcal{J}$ est un idéal homogène de $\mathcal{R}$ engendré par des polynômes de degré au plus L et $\mathcal{Z}(\mathcal{J})$ le lieu des zéros de $\mathcal{J}$.*

On rappelle aussi que le stabilisateur de V, noté G_V, est le groupe $\{x \in A,\ x + V \subseteq V\}$.

Par la suite on aura besoin à plusieurs reprises de quelques résultats généraux.

Lemme 2.3. *Soit V une sous-variété de A, plongée dans $\mathbb{P}^n$ via $\mathcal{L}$, G_V son stabilisateur et G_V° la composante connexe contenant l'identité. Supposons V définie incomplètement dans A par des équations de degré au plus L, où L est un entier positif. On a*

(i). pour tout $Q \in A_{\text{tors}}$, on a $\deg(V + Q) = \deg(V)$, et $V + Q$ est définie incomplètement par des équations de degré au plus $2L$.

(ii). $\deg(G_V) = \deg(G_V^\circ)|G_V : G_V^\circ| \leq \deg(V)(2L)^{\dim(V)-\dim(G_V)}$ et G_V est défini incomplètement par des équations de degré $\leq 2L$. Plus généralement on a $\deg(G_V) \leq \deg(V)^{\dim(V)+1}$.

Proof. Voir (DH00), lemme 2.1.

2.3 Généralités sur les sous-variétés de torsion

Soit A une variété abélienne définie sur K, $P \in A(\bar{K}) \setminus A_{\text{tors}}$ et H la plus petite sous-variété de torsion de A définie sur K contenant le point P. On note H° la composante $\bar{K}$-irréductible de $H - P$ passant par l'élément neutre. Puisque H est la plus petite sous-variété de torsion définie sur K on a

$$H = \bigcup_{\sigma \in \mathrm{Gal}(\bar{K}/K)} \sigma(H^\circ + P). \tag{2}$$

On notera par la suite $|H : H^\circ|$ le nombre de composantes irréductibles distinctes dans cette union.

Lemme 2.4. *Soit H la plus petite sous-variété de torsion définie sur K contenant le point P et Z une sous-variété de H définie sur K et K-irréductible passant par P. Soit $Z' = Z \cap (H^\circ + P)$, alors*

$$\deg(Z') = \frac{\deg Z}{|H : H^\circ|}.$$

Proof. D'après (2)

$$Z = \bigcup_{\sigma \in \mathrm{Gal}(\bar{K}/K)} Z \cap \sigma(H^\circ + P) = \bigcup_{\sigma \in \mathrm{Gal}(\bar{K}/K)} \sigma(Z').$$

Par conséquent $\deg(Z) = \deg(Z')|H : H^\circ|$ puisque les $\sigma(Z')$ qui interviennent dans cette union sont disjoints, leur nombre est le nombre de conjugués distincts de $H^\circ + P$ et ils ont tous même dimension et même degré.

Voyons maintenant que les conjectures 1.13 et 1.14 sont équivalentes. Pour cela, on montrera plutôt l'équivalence des théorèmes "à ϵ-près", ce qui paraît plus naturel puisqu'on pourra en déduire le résultat sur les conjectures en oubliant dans la preuve les termes en log.

Le résultat "à ϵ-près" de la conjecture 1.14 qu'on va démontrer est le suivant :

Théorème 2.5. *Soient A une variété abélienne à multiplication complexe définie sur un corps de nombres K, munie d'un fibré $\mathcal{L}_0$ ample et symétrique et P un point de $A(\bar{K}) \setminus A(\bar{K})_{\text{tors}}$. Soient $\mathcal{L} = \mathcal{L}_0^{\otimes 4}$, H la plus petite sous-variété de torsion définie sur K passant par P et H° la composante $\bar{K}$-irréductible de $H - P$ passant par l'élément neutre. Alors il existe une constante $c(A, K, \mathcal{L})$ strictement positive telle que*

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{c(A,K,\mathcal{L})}{\omega_K(P,H)} \left(\frac{\log\log \omega_{K_{\text{tors}}} \deg_{\mathcal{L}}(H^\circ)^2}{\log \omega_{K_{\text{tors}}} \deg_{\mathcal{L}}(H^\circ)^2} \right)^{\kappa_1(g_0)},$$

où $\kappa_1(g_0) = 2^{2g_0+1} g_0^{4g_0} (g_0+1)!^{2g_0}$, $g_0 = \dim H$ et $\omega_{K_{\text{tors}}} = \omega_{K_{\text{tors}}}(P, P + H^\circ)$.

Proposition 2.6. *Le théorème 1.15 est équivalent au théorème 2.5.*

Proof. Voyons d'abord théorème 1.15 $\Rightarrow$ théorème 2.5. Soit $P \in A(\bar{K})$, H la plus petite sous-variété de torsion définie sur K passant par P et $Z \subsetneq H$ contenant P définie sur K telle que

$$\omega_K(P,H) = \left(\frac{\deg Z}{\deg H}\right)^{\frac{1}{\mathrm{codim}_H Z}}.$$

Soit T un point de torsion T tel que $P + H^\circ = T + H^\circ$. On note $Z' = Z \cap (H^\circ + T)$ et on considère la variété $Z' - T$. Elle est définie sur K_{tors} puisque H° est définie sur $K(A[3]) \subseteq K_{\mathrm{tors}}$ (voir (Sil92)), contient le point $P - T$ et est contenue dans H°, donc

$$\left(\frac{\deg(Z'-T)}{\deg H^\circ}\right)^{1/\mathrm{codim}_{H^\circ} Z'-T} \geq \omega_{K_{\mathrm{tors}}}(P-T, H^\circ). \tag{3}$$

D'autre part, on vérifie facilement que $P - T$ est d'ordre infini modulo toute sous-variété abélienne propre de H°. On applique le théorème 1.15 au point $P - T$ et à la sous-variété abélienne H°. Il existe donc une constante $c_1 = c_1(A, K, \mathcal{L})$ telle que

$$\hat{h}(P-T) \geq \frac{c_1}{\omega_{K_{\mathrm{tors}}}(P-T,H^\circ)} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(P-T,H^\circ)\deg(H^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(P-T,H^\circ)\deg(H^\circ)^2}\right)^{\kappa_1(g_0)}$$

où $g_0 = \dim H^\circ$ et $\kappa_1(g_0) = 2^{2g_0+1} g_0^{4g_0}(g_0+1)!^{2g_0}$. Puisque $\hat{h}(P-T) = \hat{h}(P)$ et en utilisant l'inégalité (3) et le lemme 2.4 on obtient

$$\begin{aligned}
\hat{h}(P) &\geq c_1 \left(\frac{\deg(H^\circ)}{\deg(Z'-T)}\right)^{\mathrm{codim}_{H^\circ} Z'-T} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(P-T,H^\circ)\deg(H^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(P-T,H^\circ)\deg(H^\circ)^2}\right)^{\kappa_1(g_0)} \\
&\geq c_1 \left(\frac{\deg(H^\circ)|H:H^\circ|}{\deg Z}\right)^{\mathrm{codim}_H(Z)} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(P-T,H^\circ)\deg(H^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(P-T,H^\circ)\deg(H^\circ)^2}\right)^{\kappa_1(g_0)} \\
&\geq \frac{c_1}{\omega_K(P,H)} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(P,P+H^\circ)\deg(H^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(P,P+H^\circ)\deg(H^\circ)^2}\right)^{\kappa_1(g_0)}.
\end{aligned}$$

Voyons maintenant théorème 2.5 $\Rightarrow$ théorème 1.15. Soit H une sous-variété abélienne de A définie sur K et $P \in H$ d'ordre infini modulo toute sous-variété abélienne propre de H. Soit $\mathcal{L}$ un fibré ample et symétrique sur A et Z une sous-variété de H définie sur K_{tors} contenant P telle que

$$\omega_{K_{\mathrm{tors}}}(P,H) = \left(\frac{\deg_{\mathcal{L}} Z}{\deg_{\mathcal{L}} H}\right)^{1/\mathrm{codim}_H Z}.$$

Notons $K(Z)$ une extension finie de K contenue dans K_{tors} sur laquelle Z est définie. Puisque $A_{\mathrm{tors}} = \bigcup_{N \in \mathbb{N}} A[N]$, il existe $M \in \mathbb{N}$ tel que $K(Z) \subseteq K(A[M])$. On sait que $A[M] \simeq (\mathbb{Z}/M)^{2g}$ donc il existe $T_1, \ldots, T_{2g} \in A[M]$ tels que $K(Z) \subseteq K(T_1, \ldots, T_{2g})$. On pose $Q = (P, T_1, \ldots, T_{2g}) \in A \times \ldots \times A$. On voit facilement que la plus petite sous-variété de torsion contenant le point Q définie sur K est

$$H_Q = \bigcup_{\sigma \in \mathrm{Gal}(\bar{K}/K)} H \times \{\sigma(T_1, \ldots, T_{2g})\}.$$

On pose alors

$$V = \bigcup_{\sigma \in \mathrm{Gal}(\bar{K}/K)} \sigma(Z \times \{(T_1, \ldots, T_{2g})\}),$$

qui est définie sur K contenue dans H_Q et contient Q. Soit $\mathcal{M} = p_1^*\mathcal{L} \otimes \cdots \otimes p_{2g+1}^*\mathcal{L}$ où $p_1, \ldots, p_{2g+1}$ désignent les projections de $A \times \cdots \times A$ dans A sur chaque variable. Avec ces notations on a

$$\begin{aligned}
\deg_{\mathcal{M}}(V) &= [K(T_1, \ldots, T_g):K]\deg_{\mathcal{L}}(Z) \quad \text{et} \\
\deg_{\mathcal{M}}(H_Q) &= [K(T_1, \ldots, T_g):K]\deg_{\mathcal{L}}(H).
\end{aligned}$$

On applique le théorème 2.5 au point Q, donc il existe une constante $c_2 = c_2(A^{2g+1}, K, \mathcal{M}) > 0$ telle que

$$\hat{h}_{\mathcal{M}}(Q) \geq \frac{c_2}{\omega_K(Q,H_Q)} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q)\deg_{\mathcal{M}}(H_Q^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q)\deg_{\mathcal{M}}(H_Q^\circ)^2}\right)^{\kappa_1(g_0)}$$

puisque $g_0 = \dim H = \dim H_Q$. On a finalement

$$\begin{aligned}
\hat{h}_{\mathcal{L}}(P) = \hat{h}_{\mathcal{M}}(Q) &\geq c_2 \left(\frac{\deg_{\mathcal{M}}(H_Q)}{\deg_{\mathcal{M}}(V)}\right)^{\frac{1}{\operatorname{codim}_{H_Q} V}} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q)\deg_{\mathcal{M}}(H_Q^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q)\deg_{\mathcal{M}}(H_Q^\circ)^2}\right)^{\kappa_1(g_0)} \\
&\geq c_2 \left(\frac{[K(T):K]\deg_{\mathcal{L}}(H)}{[K(T):K]\deg_{\mathcal{L}}(Z)}\right)^{1/\operatorname{codim}_H Z} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q)\deg_{\mathcal{M}}(H_Q^\circ)^2}{\log \omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q)\deg_{\mathcal{M}}(H_Q^\circ)^2}\right)^{\kappa_1(g_0)} \\
&\geq \frac{c_2}{\omega_{K_{\mathrm{tors}}}(P,H)} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}}(P,H)\deg_{\mathcal{L}}(H)^2}{\log \omega_{K_{\mathrm{tors}}}(P,H)\deg_{\mathcal{L}}(H)^2}\right)^{\kappa_1(g_0)},
\end{aligned}$$

puisque $\deg_{\mathcal{M}}(H_Q^\circ) = \deg_{\mathcal{L}}(H)$ et

$$\begin{aligned}
\omega_{K_{\mathrm{tors}}}(Q, H_Q^\circ + Q) &\leq \left(\frac{\deg_{\mathcal{M}}(Z \times \{(T_1 \dots, T_{2g})\})}{\deg_{\mathcal{M}} H_Q^\circ}\right)^{1/\operatorname{codim}_H Z} \\
&= \left(\frac{\deg_{\mathcal{L}}(Z)}{\deg_{\mathcal{L}}(H)}\right)^{1/\operatorname{codim}_H Z} \\
&= \omega_{K_{\mathrm{tors}}}(P,H).
\end{aligned}$$

On remarque aussi qu'on a comme corollaire immédiat du théorème 1.15 le théorème 1.8. En effet, si P est d'ordre infini modulo toute sous-variété abélienne propre de A, on applique le théorème 1.15 à P avec $H = A$ et on a le résultat désiré puisque par définition $\omega_{K_{\mathrm{tors}}}(P,A) \leq c(A,K,\mathcal{L})[K_{\mathrm{tors}}(P) : K_{\mathrm{tors}}]^{\frac{1}{g}}$.

2.4 Endomorphismes de Frobenius

Soit A une variété abélienne définie sur K et $\mathcal{O}_K$ l'anneau des entiers de K. De façon générale, on peut construire un modèle de A sur $\operatorname{Spec}(\mathcal{O}_K)$, *i. e.* un schéma $\mathcal{X} \to \operatorname{Spec}(\mathcal{O}_K)$ dont la fibre générique est isomorphe à A. On peut se servir de cette construction pour définir l'endomorphisme de Frobenius associé à une place v de K, qui n'existe que pour un nombre fini de places. Afin de spécifier les places où il n'existe pas, il est plus pratique de construire un modèle particulier, le modèle de Néron. On a le théorème suivant :

Théorème 2.7. *Pour toute variété abélienne A/K, il existe un modèle de Néron $\mathcal{A} \to \operatorname{Spec}(\mathcal{O}_K)$ de A/K. De plus $\mathcal{A}$ est un schéma en groupes sur $\operatorname{Spec}(\mathcal{O}_K)$.*

Proof. Voir (Nér64) pour la preuve originale et (BLR90) et (Art86) pour des reformulations et simplifications.

Soit $\mathcal{A}$ le modèle de Néron de A/K sur $\operatorname{Spec}(\mathcal{O}_K)$, v une place finie de K et k_v le corps résiduel associé. Soit $\mathcal{A}_v = \mathcal{A} \times_{\operatorname{Spec}(\mathcal{O}_K)} k_v$ la fibre de $\mathcal{A}$ en v. Si A a bonne réduction en v alors la flèche

$$\rho_v : \operatorname{End}_{\mathcal{O}_K}(\mathcal{A}) \to \operatorname{End}_{k_v}(\mathcal{A}_v)$$

est injective, voir (Lan83), théorème 3.2, page 45. Par définition du modèle de Néron, tout endomorphisme de A se prolonge en un endomorphisme de $\mathcal{A}$ et ceci de façon unique. On a donc une flèche injective qu'on notera encore ρ_v,

$$\rho_v : \operatorname{End}(A) \to \operatorname{End}(\mathcal{A}_v).$$

Sur la variété $\mathcal{A}_v$ on dispose de l'endomorphisme de Frobenius classique Frob_v correspondant à l'élévation à la puissance $N(v) = \operatorname{Card}(k_v)$ en coordonnées projectives, et on dira que $\alpha_v \in \operatorname{End}_K(A)$ est un *endomorphisme de Frobenius* en v si $\rho_v(\alpha) = \operatorname{Frob}_v$. Si on choisi pour chaque $p \in \mathcal{P}$ une seule place v de M_K au dessus de p, on notera aussi α_p l'endomorphisme de Frobenius (s'il existe) de A en v.

Définition 2.8. *Une variété abélienne simple A est dite à multiplication complexe (ou de type CM) si son anneau d'endomorphismes tensorisé par $\mathbb{Q}$ contient un corps commutatif F de degré $[F : \mathbb{Q}] = 2\dim A$, éventuellement après extension du corps de base. Une variété abélienne est de type CM si elle est isogène à un produit $A_1 \times \ldots \times A_r$ de variétés abéliennes simples de type CM, ou de façon équivalente, si son anneau d'endomorphismes tensorisé par $\mathbb{Q}$ contient un produit de corps commutatifs (après extension éventuelle du corps de base) $F_1 \times \cdots \times F_r$ tels que $\sum_{i=1}^r [F_i : \mathbb{Q}] = 2\dim A$.*

Si A est de type CM, on peut supposer qu'elle possède un endomorphisme de Frobenius en presque toute place grâce au théorème suivant de Shimura et Taniyama (voir (ST61), III.13 théorème 1)

Proposition 2.9. *(Shimura-Taniyama) Soit $A = A_i \times \ldots \times A_r$ avec A_i simple de type CM telles que $\mathrm{End}_{\bar{K}} A_i = \mathcal{O}_{F_i}$ où $F_i = \mathrm{End}_{\bar{K}}(A_1) \otimes \mathbb{Q}$ et $\sum_{i=1}^r [F_i : \mathbb{Q}] = 2 \dim A$. On suppose que le corps K contient tous les F_i. Alors à un nombre fini d'exceptions près, A possède un endomorphisme de Frobenius en toute place finie de K.*

À l'aide du modèle de Néron on peut montrer que les exceptions sont justement les places de mauvaise réduction de la variété abélienne et les places ramifiées dans le corps des multiplications complexes (voir (ST61), III.13).

Il faut voir maintenant qu'on peut en effet se réduire au cas où les hypothèses de la proposition 2.9 sont vérifiées. On sait que toute variété abélienne est isogène à un produit de variétés abéliennes simples et quitte à faire une extension de K de degré borné (cette borne ne dépend que de $\dim(A)$) les autres hypothèses sont aussi vérifiées.

Proposition 2.10. *Soient A/K une variété abélienne, $\mathcal{L}$ un fibré ample et symétrique sur A, H/K une sous-variété abélienne de A et $P \in H(\bar{K})$ un point d'ordre infini modulo toute sous-variété abélienne de H.*

(i). Soit K' une extension finie de K. Si le théorème 1.15 est vrai pour $A_{K'}$, K', $\mathcal{L}_{K'}$, $H_{K'}$ et P, il est vrai pour A, K, $\mathcal{L}$, H et P (on a noté $\mathcal{L}_{K'}$ le fibré sur $A_{K'}$ tiré en arrière de $\mathcal{L}$ par la projection naturelle de $A_{K'}$ sur A).

(ii). Soit $\psi : A \to A'$ une isogénie définie sur K de degré m et $\phi : A' \to A$ l'isogénie duale satisfaisant $\psi \circ \phi = [m]_{A'}$. Si le théorème est vrai pour A', K, $\phi^*\mathcal{L}$, $\psi(H)$ et $\psi(P)$, il est vrai pour A, K, $\mathcal{L}$, H et P.

Proof. (i). D'après le théorème 1.15 il existe une constante $c(A_{K'}, K', \mathcal{L}_{K'})$ telle que

$$\hat{h}_{\mathcal{L}_{K'}}(P) \geq \frac{c(A_{K'}, K', \mathcal{L}_{K'})}{\omega_{K'_{\mathrm{tors}}}(P, H_{K'})} \left(\frac{\log\log \omega_{K'_{\mathrm{tors}}}(P, H_{K'}) \deg(H_{K'})^2}{\log \omega_{K'_{\mathrm{tors}}}(P, H_{K'}) \deg(H_{K'})^2} \right)^{\kappa_1(g_0)}.$$

De plus $\deg_{\mathcal{L}}(H) = \deg_{\mathcal{L}_{K'}}(H_{K'})$ et $K_{\mathrm{tors}} \subset K'_{\mathrm{tors}}$ donc on vérifie facilement

$$\omega_{K_{\mathrm{tors}}}(P, H) \geq \omega_{K'_{\mathrm{tors}}}(P, H_{K'}).$$

Puisque $\hat{h}_{\mathcal{L}_{K'}}(P) = \hat{h}_{\mathcal{L}}(P)$ et K' est une extension fixée de K, il existe une constante $c_3(A, K, \mathcal{L})$ telle que

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{c_3(A, K, \mathcal{L})}{\omega_{K_{\mathrm{tors}}}(P, H)} \left(\frac{\log\log \omega_{K_{\mathrm{tors}}} \deg(H)^2}{\log \omega_{K_{\mathrm{tors}}} \deg(H)^2} \right)^{\kappa_1(g_0)}.$$

(ii). Si P est d'ordre infini modulo toute sous-variété abélienne propre de H alors $\psi(P)$ est d'ordre infini modulo toute sous-variété abélienne propre de $\psi(H)$. De plus $\psi(H)$ est définie sur K puisque H et ψ sont définies sur K. Le théorème 1.15 appliqué à $A', K, \phi^*\mathcal{L}, \psi(H)$ et $\psi(P)$ nous dit qu'il existe une constante $c(A', K, \phi^*\mathcal{L})$ telle que

$$\hat{h}_{\phi^*\mathcal{L}}(\psi(P)) \geq \frac{c(A', K, \phi^*\mathcal{L})}{\omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H))} \left(\frac{\log\log \omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) \deg_{\phi^*\mathcal{L}}(\psi(H))^2}{\log \omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) \deg_{\phi^*\mathcal{L}}(\psi(H))^2} \right)^{\kappa_1(g_0)},$$

où $g_0 = \dim(\psi(H)) = \dim(H)$ (dans l'indice d'obstruction on a mis en évidence le fibré par rapport auquel on calcule le degré).

D'autre part, notons V une sous-variété de H définie sur K_{tors} et passant par P telle que $\omega_{\mathcal{L}}(P, H) = \left(\frac{\deg_{\mathcal{L}}(V)}{\deg_{\mathcal{L}}(H)} \right)^{1/\mathrm{codim}_H V}$. On a $\psi(V) \subset \psi(H)$, $\psi(P) \in \psi(V)$ et $\psi(V)$ est définie sur K_{tors}, d'où

$$\left(\frac{\deg_{\phi^*\mathcal{L}}(\psi(V))}{\deg_{\phi^*\mathcal{L}}(\psi(H))} \right)^{1/\mathrm{codim}_{\psi(H)} \psi(V)} \geq \omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) \tag{4}$$

par définition.

Calculons maintenant $\deg_{\phi^*\mathcal{L}}(\psi(V))$ et $\deg_{\phi^*\mathcal{L}}(\psi(H))$. On a

$$\begin{aligned} \deg_{\phi^*\mathcal{L}}(\psi(V)) &= \frac{1}{\deg \psi_{|V}} \deg_{[m]^*\mathcal{L}}(V) \quad \text{(par la formule de projection)} \\ &= \frac{1}{\deg \psi_{|V}} \deg_{\mathcal{L}^{\otimes m^2}}(V) \quad \text{(puisque } \mathcal{L} \text{ est symétrique)} \\ &= \frac{m^{2d}}{\deg \psi_{|V}} \deg_{\mathcal{L}}(V) \quad \text{(où } d \text{ est la dimension de } V\text{)}. \end{aligned}$$

De la même façon on trouve $\deg_{\phi^*\mathcal{L}}(\psi(H)) = \frac{m^{2g_0}}{\deg \psi_{|H}} \deg_{\mathcal{L}}(H)$. En remplaçant dans (4) on a

$$\begin{aligned}
\omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) &\leq \left(\frac{\deg \psi_{|H} m^{2d} \deg_{\mathcal{L}}(V)}{\deg \psi_{|V} m^{2g_0} \deg_{\mathcal{L}}(H)} \right)^{1/\operatorname{codim}_{\psi(H)} \psi(V)} \\
&\leq \omega_{\mathcal{L}}(P, H) \left(\frac{\deg \psi_{|H} m^{2d}}{\deg \psi_{|V} m^{2g_0}} \right)^{1/\operatorname{codim}_H V} \\
&\leq \omega_{\mathcal{L}}(P, H) \left(\frac{1}{m^{2(g_0-d)-1}} \right)^{1/(g_0-d)} \\
&\leq \omega_{\mathcal{L}}(P, H) \frac{1}{m}.
\end{aligned}$$

On a aussi

$$\omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) \deg_{\phi^*\mathcal{L}}(\psi(H))^2 \leq \omega_{\mathcal{L}}(P, H) \deg_{\mathcal{L}}(H)^2 m^{2(g_0-1)}.$$

Maintenant, d'après des propriétés bien connues des hauteurs, on a $\hat{h}_{\phi^*\mathcal{L}}(\psi(P)) = m^2 \hat{h}_{\mathcal{L}}(P)$ et donc

$$\begin{aligned}
\hat{h}_{\mathcal{L}}(P) &\geq \frac{c(A', K, \phi^*\mathcal{L})}{m^2 \omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H))} \left(\frac{\log\log \omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) \deg_{\phi^*\mathcal{L}}(\psi(H))^2}{\log \omega_{\phi^*\mathcal{L}}(\psi(P), \psi(H)) \deg_{\phi^*\mathcal{L}}(\psi(H))^2} \right)^{\kappa_1(g_0)} \\
&\geq \frac{c(A', K, \phi^*\mathcal{L})}{m \omega_{\mathcal{L}}(P, H)} \left(\frac{\log\log \omega_{\mathcal{L}}(P, H) \deg_{\mathcal{L}}(H)^2 m^{2(g_0-1)}}{\log \omega_{\mathcal{L}}(P, H) \deg_{\mathcal{L}}(H)^2 m^{2(g_0-1)}} \right)^{\kappa_1(g_0)} \\
&\geq \frac{c_4}{\omega_{\mathcal{L}}(P, H)} \left(\frac{\log\log \omega_{\mathcal{L}}(P, H) \deg_{\mathcal{L}}(H)^2}{\log \omega_{\mathcal{L}}(P, H) \deg_{\mathcal{L}}(H)^2} \right)^{\kappa_1(g_0)}
\end{aligned}$$

avec $c_4 = \frac{c(A', K, \phi^*\mathcal{L})}{m \log m}$ qui ne dépend que de A, K et $\mathcal{L}$ puisque m est aussi borné en fonction de ces quantités.

Les endomorphismes de Frobenius possèdent les propriétés des isogénies dites admissibles. On rappelle les résultats principaux ; pour plus de détails et les démonstrations des propriétés, voir (DH00) paragraphe 2.2 et proposition 2.3.

Définition 2.11. *Soit A une variété abélienne et $\mathcal{L}$ un fibré en droites ample sur A. Une isogénie α est dite admissible par rapport à $\mathcal{L}$ si elle vérifie :*
- *il existe un entier $q(\alpha)$ qu'on appelle le poids de α tel que $\alpha^*\mathcal{L} \simeq \mathcal{L}^{\otimes q(\alpha)}$,*
- *α est dans le centre de* $\operatorname{End}(A)$.

Proposition 2.12. *Soit A une variété abélienne de dimension g, $\mathcal{L}$ un fibré en droites très ample sur A, $\iota : A \to \mathbb{P}^n$ un plongement projectivement normal associé à $\mathcal{L}$ et α une isogénie admissible pour $\mathcal{L}$ de poids $q(\alpha)$. Alors*

(i). *α peut être représentée sur $\iota(A)$ par $n+1$ formes de degré $q(\alpha)$.*
(ii). $\operatorname{Card}(\ker(\alpha)) = q(\alpha)^g$.
(iii). *Si V est une sous-variété de A définie sur $\bar{K}$ et G_V son stabilisateur, alors*

$$\deg(\alpha(V)) = \frac{q(\alpha)^{\dim(V)}}{|G_V \cap \ker(\alpha)|} \deg(V),$$

et

$$\deg(\alpha^{-1}(V)) = q(\alpha)^{\operatorname{codim}(V)} \deg(V).$$

(iv). $\hat{h}(\alpha(P)) = q(\alpha)\hat{h}(P)$.

D'après la proposition 3.3 de (DH00) on sait que un endomorphisme de Frobenius α_v pour une place v est admissible, de poids $N(v)$ où $N(v)$ est le cardinal du corps résiduel de K en v.

On aura besoin aussi de l'estimation suivante :

Lemme 2.13. *Soit G un sous-groupe algébrique d'une variété abélienne A et α une isogénie admissible de A de poids $q(\alpha)$. Alors*

$$q(\alpha)^{\dim(G)} \leq \operatorname{Card}(\ker(\alpha) \cap G) \leq |G : G^\circ| q(\alpha)^{\dim(G)}.$$

Proof. C'est le lemme 2.5 de (DH00).

2.5 Congruences

On fixe d'abord quelques notations. Pour chaque $p \in \mathcal{P}$, on choisit une unique place v de M_K telle que $v|p$. Soit $\mathbb{L}$ une extension abélienne de K, $\mathbb{L} \subset K_{\text{tors}}$. Pour tout $p \in \mathcal{P}$, on notera e_p l'indice de ramification de v dans $\mathbb{L}$. Soit w une place de $\mathbb{L}$ au-dessus de $v \in M_K$, la complétion $\mathbb{L}_w$ ne dépend que de p et puisque p est totalement décomposé dans K, $K_v = \mathbb{Q}_p$. On a que $\mathbb{L}_w$ est une extension abélienne de $\mathbb{Q}_p$ et, par conséquent, contenue dans une extension cyclotomique de $\mathbb{Q}_p$. Il existe donc un entier m tel que $\mathbb{L}_w \subset \mathbb{Q}_p(\zeta_m)$. On choisit m minimal avec cette propriété et on notera $m = p^k q$ avec $(p, q) = 1$.

Pour chaque p on va distinguer deux cas suivant que $v|p$ est "peu" ou "très ramifiée" dans $\mathbb{L}$ (hypothèse qu'on quantifiera plus tard).

Dans le cas "peu ramifié" on applique le lemme suivant :

Lemme 2.14. *Soit $p \in \mathcal{P}$ et $v|p$ la place de K fixée auparavant. Il existe $\phi_p \in \mathrm{Gal}(\mathbb{L}/K)$ tel que*

$$|\gamma^p - \phi_p \gamma|_w \leq p^{-1/e_p}$$

pour tout entier $\gamma \in \mathbb{L}$ et toute place w de $\mathbb{L}$ au-dessus de v.

Proof. Voir lemme 3.1 de (AZ00).

Remarque 2.15. *On fixe une fois pour toutes un tel élément ϕ_p satisfaisant le lemme ci-dessus pour chaque $p \in \mathcal{P}$.*

Dans le cas "très ramifié" on utilise le lemme 3.2 de (AZ00). Avec les notations données ci-dessus, ils construisent un sous-groupe G_p de $\mathrm{Gal}(\mathbb{L}/K)$ de la façon suivante : si p ne divise pas m ils posent $G_p = \{\mathrm{Id}\}$.

Si $k \geq 1$ on considère le groupe $\Sigma_p = \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p}))$. La restriction de Σ_p à $\mathbb{L}_w$ est non triviale (à cause de la minimalité de m) et G_p est l'image isomorphe de cette restriction dans $\mathrm{Gal}(\mathbb{L}/K)$ (on peut voir que G_p ne dépend pas de w). Il vérifie les propriétés suivantes :

Lemme 2.16. *Pour tout $p \in \mathcal{P}$ et $v|p$ la place fixée de K au-dessus de p, G_p est un sous-groupe de* $\mathrm{Gal}(\mathbb{L}/K)$ *tel que*

$$\begin{cases} |G_p| \geq e_p \text{ et } |G_p| \text{ divise } |\Sigma_p| = p - 1, & \text{si } k = 1 \\ |G_p| = |\Sigma_p| = p, & \text{si } k \geq 2 \end{cases}$$

et pour tout entier $\gamma \in \mathbb{L}$, toute place $w|v$ de $\mathbb{L}$ et $\sigma \in G_p$ on a

$$|\gamma^p - \sigma\gamma^p|_w \leq p^{-1}.$$

Proof. Voir lemme 3.2 de (AZ00).

Remarque 2.17. *Pour éviter cette dichotomie on pourrait penser à ne travailler qu'avec les places non ramifiées sur l'extension $\mathbb{L}$. On sait qu'une place v au-dessus de p est ramifiée dans $\mathbb{L}$ si et seulement si p divise $|\mathcal{D}_{\mathbb{L}/K}|$ (voir par exemple (CF86), I.5 théorème 1) ; on pourrait donc se restreindre à ces places-là et on disposerait d'une borne sur leur nombre qui dépend de $[\mathbb{L} : K]$. Ce facteur apparaîtrait donc dans la borne du théorème principal et on obtiendrait ainsi un résultat plus faible et qui n'impliquerait pas le "problème de Lehmer abélien" à ϵ près (voir (Rat08)).*

Pour appliquer le lemme de zéros, on aura besoin de compter les composantes isolées parmi des unions de conjugués de certaines variétés. Pour faire ceci on utilise les résultats suivants :

Proposition 2.18. *Soit A une variété abélienne de dimension $g \geq 1$ définie sur un corps de nombres K, munie d'un fibré ample $\mathcal{L}$ et V une sous-variété de A géométriquement irréductible de dimension d définie sur $\bar{K}$. On a*

(i). Pour tous $\alpha, \beta \in \mathrm{End}_K(A)$ isogénies admissibles pour $\mathcal{L}$ et pour tout $\sigma \in \mathrm{Gal}(\bar{K}/K)$ les sous-variétés $\alpha(V)$ et $\beta(\sigma(V))$ sont distinctes sauf peut-être si l'une des conditions suivantes est remplie :
  - *V est un translaté d'une sous-variété abélienne B de A par un point de torsion de A.*
  - *$q(\alpha) = q(\beta)$.*

(ii). Soit $\mathcal{P}$ un sous-ensemble de $\mathrm{End}_K(A)$ *d'isogénies admissibles pour $\mathcal{L}$, deux à deux premières entre elles*[‡]*. Soit $\mathcal{S}$ le sous-ensemble de $\mathcal{P}$:*

$$\mathcal{S} = \{\alpha \in \mathcal{P}, \quad \exists \sigma \in \mathrm{Gal}(\bar{K}/K),\ \sigma(V) \neq V \text{ et } \alpha(\sigma(V)) = \alpha(V)\}.$$

Alors $\mathrm{Card}(\mathcal{S}) \leq \frac{\log M}{\log 2}$ *où M est le nombre de conjugués distincts de V.*

On notera que cette proposition provient d'une idée de Dobrowolski pour un point dans $\mathbb{G}_m$ ((Dob79), lemme 3). Dans la situation d'une sous-variété d'une variété abélienne, c'est la proposition 2.7 de (DH00).

[‡]Deux isogénies admissibles α et β sont dites premières entre elles si $(q(\alpha), q(\beta)) = 1$.

3 Réductions

On commence par introduire quelques définitions dont on aura besoin.

Définition 3.1. *Soit $\mathbb{L}$ une extension abélienne de K, $p \in \mathcal{P}$, $v|p$ et $\mathbb{L}_v$ le complété de $\mathbb{L}$ par rapport à v. Soit m le plus petit entier tel que $\mathbb{L}_v \subseteq \mathbb{Q}_p(\zeta_m)$.*

– *On définit $f_p(\mathbb{L})$ le conducteur local de $\mathbb{L}$ en p comme la plus grande puissance de p divisant m.*
– *On pose $f(\mathbb{L}) = \prod_{p\in\mathcal{P}} f_p(\mathbb{L})$ le conducteur de $\mathbb{L}$.*

On remarque facilement que si $\mathbb{L}' \subseteq \mathbb{L}$ alors $f(\mathbb{L}') \leq f(\mathbb{L})$.

Dans la partie 9 nous serons ramenés à montrer une inégalité similaire à celle du théorème principal. Il s'agit sous les hypothèses du théorème 1.15 de montrer, pour toute extension $\mathbb{L} \subseteq K_{\text{tors}}$ et une constante c_5 fixée ultérieurement, l'inégalité

$$\hat{h}(P) \quad \geq \quad c_5 \left(\frac{\deg H}{D_{\mathbb{L}}(P)}\right)^{1/g_0} \left(\frac{\log\log D_{\mathbb{L}}(P)\deg(H)^2}{\log D_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa(g_0)} \tag{5}$$

avec $\kappa(g_0) = (2g_0(g_0+1)!)^{2g_0}$ et $D_{\mathbb{L}}(P) = [\mathbb{L}(P) : \mathbb{L}]$. Pour prouver cela, on aura besoin d'assurer que, pour certaines isogénies admissibles β, on ait $\tau(\beta(P)) \neq \beta(P)$ pour $\tau \in \text{Gal}(\bar{K}/K)$, $\tau_{|\mathbb{L}} \in G_p \setminus \{\text{Id}\}$. On va voir qu'on peut faire quelques suppositions sur le point P et l'extension $\mathbb{L}$ de départ pour garantir cette condition.

On suppose qu'il existe P qui contredit l'inégalité (5). On a donc

$$\hat{h}(P) < c_5 \left(\frac{\deg H}{D_{\mathbb{L}}(P)}\right)^{1/g_0} \left(\frac{\log\log D_{\mathbb{L}}(P)\deg(H)^2}{\log D_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa(g_0)}$$

pour une extension $\mathbb{L} \subseteq K_{\text{tors}}$. Parmi tous les points de H d'ordre infini modulo toute sous-variété abélienne propre qui contredisent l'inégalité (5) on choisit P et $\mathbb{L}$ de façon que $[\mathbb{L}(P) : \mathbb{L}]$ soit minimal. Ce choix fait, on notera $D = [\mathbb{L}(P) : \mathbb{L}]$.

Lemme 3.2. *Pour tout $T \in H_{\text{tors}}$, et $\mathbb{L}' \subseteq K_{\text{tors}}$, on a $[\mathbb{L}'(P+T) : \mathbb{L}'] \geq D$.*

Proof. D'après les propriétés de la hauteur de Néron-Tate, on sait que $\hat{h}(P+T) = \hat{h}(P)$. D'autre part, $P+T$ est d'ordre infini modulo toute sous-variété abélienne propre de H. Supposons $[\mathbb{L}'(P+T) : \mathbb{L}'] < D$. On a donc

$$\begin{aligned} \hat{h}(P+T) = \hat{h}(P) \quad &< \quad c_5 \left(\frac{\deg H}{D_{\mathbb{L}}(P)}\right)^{1/g_0} \left(\frac{\log\log D_{\mathbb{L}}(P)\deg(H)^2}{\log D_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa(g_0)} \\ &< \quad c_5 \left(\frac{\deg H}{D_{\mathbb{L}'}(P+T)}\right)^{1/g_0} \left(\frac{\log\log D_{\mathbb{L}'}(P+T)\deg(H)^2}{\log D_{\mathbb{L}'}(P+T)\deg(H)^2}\right)^{\kappa(g_0)} \end{aligned}$$

et donc $P+T$ contredit (5). Par minimalité de D on a $[\mathbb{L}'(P+T) : \mathbb{L}] \geq D$.

On définit maintenant

$$\mathcal{A} = \{\mathbb{L}/K,\, \mathbb{L} \subseteq K_{\text{tors}},\, \exists T \in H_{\text{tors}},\, [\mathbb{L}(P+T) : \mathbb{L}] \leq D\}.$$

Cet ensemble est non vide puisque par définition de D on sait qu'il existe une extension $\mathbb{L}$ telle que $[\mathbb{L}(P) : \mathbb{L}] = D$ et on peut prendre $T = 0$.
On définit ensuite

$$f = \min_{\mathbb{L}\in\mathcal{A}} f(\mathbb{L}).$$

Lemme 3.3. *Pour démontrer l'inégalité (5), on peut supposer qu'il existe $\mathbb{L} \in \mathcal{A}$ satisfaisant*

(i). $[\mathbb{L}(P) : \mathbb{L}] = D$;
(ii). $f(\mathbb{L}) = f$;
(iii). $\forall T \in H_{\text{tors}}$ *tel que* $K(P+T) \subseteq K(P)$ *on a* $K(P+T) = K(P)$;
(iv). $K \subseteq \mathbb{L} \subseteq K(P)$.

Proof. Puisque $\mathcal{A} \neq \emptyset$, on choisit $\mathbb{L} \in \mathcal{A}$ de conducteur minimal. D'après le lemme 3.2 et la définition de $\mathcal{A}$ il existe $T \in H_{\text{tors}}$ tel que $[\mathbb{L}(P+T) : \mathbb{L}] = D$. Donc quitte à changer P par $P+T$ les conditions (i) et (ii) sont satisfaites.

Pour montrer (iii) on suit le même raisonnement que dans (Rat04). Si pour tout T, $K(P+T) = K(P)$ il n'y a rien à démontrer. Sinon, on note $\mathcal{T}$ l'ensemble des points de torsion de H tels que $K(P+T) \subsetneq K(P)$ et $P_1 = P + T$ pour $T \in \mathcal{T}$. On note $\mathcal{T}_1$ l'ensemble des points de torsion de H tels que $K(P_1 + T) \subsetneq K(P_1)$. Si $\mathcal{T}_1$ est non vide, on choisit un point $T_1 \in \mathcal{T}_1$ et on pose $P_2 = P_1 + T_1$ sinon on pose $P_2 = P_1$. On construit de cette façon une chaîne d'extensions

$$K(P_n) \subsetneq \ldots \subsetneq K(P_1) \subsetneq K(P).$$

Soit n le premier entier tel que $K(P_n) = K(P_{n+1})$, c'est-à-dire si $T \in H_{\text{tors}}$ et $K(P_n + T) \subseteq K(P_n)$, alors $K(P_n + T) = K(P_n)$. Par définition des P_i on a $P_n = P + (T + \ldots + T_{n-1}) = P + T'$ et par le lemme 3.2, $[\mathbb{L}(P+T') : \mathbb{L}] \geq D$. D'autre part, puisque $K(P_n) \subseteq K(P)$, alors $\mathbb{L}(P+T') \subseteq \mathbb{L}(P)$ et donc

$$[\mathbb{L}(P+T') : \mathbb{L}] \leq [\mathbb{L}(P) : \mathbb{L}] = D.$$

On obtient donc $[\mathbb{L}(P+T') : \mathbb{L}] = D$, donc quitte à remplacer P par $P + T'$ la condition (iii) est satisfaite.

Finalement, pour P ainsi construit (assurant (i) à (iii)) on peut remplacer $\mathbb{L}$ par $\mathbb{L} \cap K(P)$. Les conditions (i) et (iii) ne changent pas, (ii) est encore vraie d'après la remarque sur le conducteur et la condition (iv) est aussi satisfaite.

Avant de donner le lemme principal de la réduction on aura besoin de quelques informations sur les extensions engendrées par des points de torsion des variétés abéliennes.

Lemme 3.4. *Soit A une variété abélienne CM simple sur K avec $F = \mathrm{End}_{\bar{K}}(A) \otimes \mathbb{Q} \subset K$ et $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A) = \mathcal{O}_F$. Alors pour tout p totalement décomposé dans F, l'extension galoisienne $K(A[p])/K$ est de degré premier à p.*

Proof. L'idée de la preuve est de montrer que l'image de $\mathrm{Gal}(K(A[p])/K)$ dans $\mathrm{Aut}_{\mathbb{F}_p}(A[p]) \simeq \mathrm{GL}_{2g}(\mathbb{F}_p)$ est contenue dans les matrices diagonales ($\simeq (\mathbb{F}_p^\times)^{2g}$) donc de cardinal premier à p.

On considère le diagramme suivant

$$\begin{tikzcd}
\mathrm{Gal}(\bar{K}/K) \arrow[r] \arrow[d] & \mathrm{Aut}_{\mathbb{Z}_p}(T_p(A)) \subset \mathrm{End}_{\mathbb{Z}_p}(T_p(A)) \arrow[d] \\
\mathrm{Gal}(K(A[p])/K) \arrow[r, hook] & \mathrm{Aut}_{\mathbb{F}_p}(A[p]) \subset \mathrm{End}_{\mathbb{F}_p}(A[p])
\end{tikzcd}$$

Comme $T_p(A)$ est un $\mathbb{Z}_p$-module libre de rang $2g$, il suffit de montrer qu'il existe une base de $T_p(A)$ sur $\mathbb{Z}_p$ telle que $\mathrm{Gal}(\bar{K}/K)$ agit diagonalement.

Maintenant on sait que $T_p(A) \otimes \mathbb{Q}_p$ est un $F \otimes \mathbb{Q}_p$-module libre de rang 1 (voir (Rup) lemme 2) et que cette structure est compatible à l'action galoisienne. D'autre part, grâce à l'hypothèse sur p, on a $F \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}$. Puisque $\mathcal{O}_F$ agit sur $T_p(A)$, $\mathcal{O}_F \otimes \mathbb{Z}_p$ agit sur $T_p(A)$ de manière compatible à Galois donc

$$\begin{tikzcd}
\mathrm{Gal}(\bar{K}/K) \arrow[r] \arrow[dr] & \mathrm{Aut}_{F\otimes\mathbb{Q}_p}(T_p(A) \otimes \mathbb{Q}_p) \arrow[r] & \mathrm{Aut}_{\mathbb{Q}_p}(T_p(A) \otimes \mathbb{Q}_p) \\
& \mathrm{Aut}_{\mathcal{O}_F\otimes\mathbb{Z}_p}(T_p(A)) \arrow[r] \arrow[u, hook] & \mathrm{Aut}_{\mathbb{Z}_p}(T_p(A)) \arrow[u, hook]
\end{tikzcd}$$

Il suffit donc de remarquer que $\mathcal{O}_F \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p^{2g}$ et que $T_p(A)$ est un $\mathcal{O}_F \otimes \mathbb{Z}_p$-module libre de rang 1, et ainsi

$$\mathrm{Aut}_{\mathbb{Z}_p^{2g}}(\mathbb{Z}_p^{2g}) = (\mathbb{Z}_p^{2g})^\times = (\mathbb{Z}_p^\times)^{2g} \hookrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{Z}_p^{2g}) = \mathrm{GL}_{2g}(\mathbb{Z}_p).$$

Remarque 3.5. *D'après la proposition 2.10 pour montrer le théorème 1.15 on peut supposer que A est un produit de variétés abéliennes simples $A_1 \times \cdots \times A_r$ avec multiplication complexe, telles que pour tout $i = 1, \ldots, r$ si $F_i = \mathrm{End}_{\bar{K}}(A_i) \otimes \mathbb{Q}$ on a $\mathrm{End}_{\bar{K}}(A_i) = \mathrm{End}_K(A_i) = \mathcal{O}_{F_i}$ et $\sum_{i=1}^r [F_i : \mathbb{Q}] = 2 \dim A$. En appliquant le lemme ci-dessus aux variétés A_i on a que $K(A_i[p])/K$ est de degré premier à p et donc $K(A[p])/K$ est de degré premier à p.*

On aura aussi besoin du résultat suivant.

Lemme 3.6. *Soient A/K une variété abélienne CM et α_p un endomorphisme de Frobenius en une place $v|p$ de K de bonne réduction ordinaire. Soit K_v^{nr} l'extension maximale non ramifiée de K_v et $\mathcal{O}_v^{\mathrm{nr}}$ son anneau d'entiers. Alors le groupe formel $\hat{A}$ de A est isomorphe sur $\mathcal{O}_v^{\mathrm{nr}}$ à $\hat{\mathbb{G}}_{\mathrm{m}}^g$. En particulier, pour tout $k \geq 1$ $\hat{A}[p^k] \cong \hat{\mathbb{G}}_{\mathrm{m}}^g[p^k] \cong \mu_{p^k}^g$ comme $\mathrm{Gal}(\bar{K}_v/K_v^{\mathrm{nr}})$-modules et donc $A[\alpha_p^k] \cong \mu_{p^k}^g$ comme $\mathrm{Gal}(\bar{K}_v/K_v^{\mathrm{nr}})$-modules.*

Proof. Voir lemmes 3.1 et 3.2 de (Bak03).

Remarque 3.7. *Si A a bonne réduction ordinaire en v on sait que $A[\alpha_p] \subset A[p]$ (voir lemme 3.2 de (Bak03)) et donc le lemme 3.4 s'applique à l'extension $K(A[\alpha_p])$ (on a noté ici $A[\alpha_p] = \ker(\alpha_p)$).*

On donne encore deux lemmes de réduction. Le premier est l'équivalent du lemme 2.1 (ii) de (AZ00) dans le cas d'un point dans $\mathbb{G}_m$ et du lemme 3.3 de (Rat04) pour un point dans une courbe elliptique.

Lemme 3.8. *Soient $p \in \mathcal{P}$, v une place de K au-dessus de p telle que H a bonne réduction ordinaire en v et α_p l'endomorphisme de Frobenius associé à v. Pour démontrer (5), on peut supposer pour toute extension $\mathbb{E}$ telle que $K \subseteq \mathbb{E} \subseteq \mathbb{L}$ qu'on a soit $\mathbb{E}(\alpha_p(P)) = \mathbb{E}(P)$, soit $p \mid [\mathbb{E}(P) : \mathbb{E}(\alpha_p(P))]$.*

Proof. Notons $G_1 = \mathrm{Gal}(\mathbb{E}(P, H[\alpha_p])/\mathbb{E}(\alpha_p(P), H[\alpha_p]))$. Supposons d'abord $p \nmid |G_1|$. On regarde l'action de $G_2 = \mathrm{Gal}(\mathbb{E}(P, H[\alpha_p])/\mathbb{E}(\alpha_p(P)))$ sur l'ensemble

$$S = \{P + T, \quad T \in H[\alpha_p]\}.$$

Pour $\sigma \in G_2$ on vérifie facilement que $\alpha_p(\sigma(P) - P) = 0$ d'où $\sigma(P) = P + T$ avec $T \in H[\alpha_p]$. Puisque $p \nmid |G_1|$ en utilisant le lemme 3.4 on a $p \nmid |G_2|$ et pour toute orbite ω de S/G_2 on a $p \nmid |w|$. On fait la somme de tous les éléments d'une orbite ω et on trouve

$$\sum_{P+T \in \omega} P + T = [r]P + T'$$

avec $(r, p) = 1$ et $T' \in H[\alpha_p]$. Il existe donc des entiers μ, λ tels que $r\mu + \lambda p^g = 1$. De plus $[r]P + T'$ est défini sur $\mathbb{E}(\alpha_p(P))$.

Soit $\alpha_p^\vee$ l'isogénie duale de α_p, on a $\alpha_p^\vee \circ \alpha_p = [p^g]$ et donc

$$\mathbb{E}([p^g](P)) = \mathbb{E}(\alpha_p^\vee \circ \alpha_p(P)) \subseteq \mathbb{E}(\alpha_p(P)).$$

D'autre part $\mathbb{E}([\lambda p^g]P + [\mu]([r]P + T')) \subseteq \mathbb{E}(\alpha_p(P))$ et alors puisque $K(P) = \mathbb{E}(P) = \mathbb{L}(P)$ (d'après le lemme 3.3.(iv)) on a

$$K(P + [\mu]T') \subseteq \mathbb{E}(P + [\mu]T') \subseteq \mathbb{E}(\alpha_p(P)) \subseteq \mathbb{E}(P) = K(P).$$

En utilisant le lemme 3.3.(iii), $K(P + [\lambda]T') = K(P)$ d'où $\mathbb{E}(P) = \mathbb{E}(\alpha_p(P))$.

Supposons maintenant $p \mid [\mathbb{E}(P, H[\alpha_v]) : \mathbb{E}(\alpha_v(P), H[\alpha_v])]$. On a le diagramme suivant :

$$\begin{tikzcd}
 & & K(P, H[\alpha_p]) = \mathbb{E}(P, H[\alpha_p]) \arrow[dll, dash] \arrow[drr, dash] & & \\
K(P) = \mathbb{E}(P) \arrow[drr, dash] & & & & \mathbb{E}(\alpha_p(P), H[\alpha_p]) \arrow[dll, dash] \arrow[d, dash] \\
 & & \mathbb{E}(\alpha_p(P)) \arrow[d, dash] & & \mathbb{E}(H[\alpha_p]) \arrow[dll, dash] \\
 & & K & &
\end{tikzcd}$$

Puisque $p \nmid [K(P, H[\alpha_p]) : K(P)]$ on voit facilement que $p \mid [\mathbb{E}(P) : \mathbb{E}(\alpha_p(P))]$.

On arrive au lemme qui constitue la réduction la plus importante et permettra de conclure au moment de la descente dans les cas plus pathologiques.

Lemme 3.9. *Soit $p \in \mathcal{P}$, v une place de K au-dessus de p et α_p un endomorphisme de Frobenius associé à v tel que $\mathbb{L}(\alpha_p(P)) = \mathbb{L}(P)$. Supposons que A a bonne réduction ordinaire en v. Pour démontrer l'inégalité (5) on peut supposer que, pour toute extension $\tau \in \mathrm{Gal}(\bar{K}/K)$ de $\sigma \in G_p \setminus \{\mathrm{Id}\}$, on a*

$$\tau(\alpha_p(P)) \neq \alpha_p(P).$$

Proof. Supposons $\tau(\alpha_p(P)) = \alpha_p(P)$ pour $\tau \in \mathrm{Gal}(\bar{K}/K)$, $\tau|\mathbb{L} = \sigma \in G_p \setminus \{\mathrm{Id}\}$. On va construire une extension $\mathbb{F} \in \mathcal{A}$ de conducteur strictement inférieur au conducteur de $\mathbb{L}$ pour avoir une contradiction.

On montre dans un premier temps que $|\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p}))| = p$. On applique le lemme 3.8 au sous-corps de $\mathbb{L}$ fixé par σ qu'on note $\mathbb{E}$. Si $\mathbb{E}(P) = \mathbb{E}(\alpha_p(P))$ alors $\mathbb{L}(P) = \mathbb{E}(\alpha_p(P))$ et donc $\mathbb{L}$ est fixé par σ ce qui est impossible. On a donc $p \mid [\mathbb{E}(P) : \mathbb{E}(\alpha_p(P))]$. D'autre part on remarque que $\mathbb{E} = \mathbb{L} \cap \mathbb{E}(\alpha_p(P))$ et donc $[\mathbb{E}(P) : \mathbb{E}(\alpha_p(P))] = [\mathbb{L} : \mathbb{E}]$. On en déduit que p divise $[\mathbb{L} : \mathbb{E}]$. On a $[\mathbb{L} : \mathbb{E}] \leq |G_p|$, mais on sait que $|G_p| \leq p$ d'après le lemme 2.16. On a finalement $|G_p| = p$ et par construction $|\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p}))| = p$.

On rappelle que $f_p(\mathbb{L}) = p^k$. On affirme qu'il existe un entier q' tel que $(p, q') = 1$ et $\mathbb{L}(H[\alpha_p^k]) \subset \mathbb{Q}_p(\zeta_{p^k q'})$. En effet, $H[\alpha_p^k] \simeq \mu_{p^k}^{g_0}$ comme $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}})$-modules d'après le lemme 3.6 donc $H[\alpha_p^k]$ est défini sur $\mathbb{Q}_p^{\mathrm{nr}}(\zeta_{p^k})$. D'autre part, $\mathbb{Q}_p^{\mathrm{nr}}$ est l'union des $\mathbb{Q}_p(\zeta_{q'})$ avec $p \nmid q'$ et donc $H[\alpha_p^k]$ est défini sur un $\mathbb{Q}_p(\zeta_{q'})(\zeta_{p^k}) = \mathbb{Q}_p(\zeta_{p^k q'})$. Quitte à augmenter q' on a $m | p^k q'$ et on peut donc supposer $\mathbb{L} \subset \mathbb{Q}_p(\zeta_{p^k q'})$.

Posons maintenant $m' = p^k q'$. Soit ρ un générateur de $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{m'})/\mathbb{Q}_p(\zeta_{m'/p}))$ dont la restriction à $\mathbb{L}$ est σ. Puisque ρ fixe $\zeta_{p^{k-1}}$, il existe une racine p-ième primitive de l'unité ξ telle que $\rho(\zeta_{p^k}) = \xi \zeta_{p^k}$. L'application

$$(\rho - 1) : \mu_{p^k}^{g_0} \to \mu_p^{g_0}$$

est donc surjective. De plus ρ est la restriction à $\mathbb{Q}_p(\zeta_{m'})$ d'un élément du groupe d'inertie $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}})$ et donc l'action de ρ commute à l'isomorphisme $H[\alpha_p^k] \simeq \mu_{p^k}^{g_0}$ du lemme 3.6. On en déduit que

$$(\rho - 1) : H[\alpha_p^k] \to H[\alpha_p]$$

est aussi surjective.

Puisque σ est d'ordre p, la restriction de ρ à $\mathbb{L}(H[\alpha_p^k])$ l'est aussi et engendre $\mathrm{Gal}(\mathbb{L}(H[\alpha_p^k])/\mathbb{F})$ où $\mathbb{F}$ est le sous-corps de $\mathbb{L}(H[\alpha_p^k])$ fixé par ρ. On en déduit $[\mathbb{L}(H[\alpha_p^k], \alpha_p(P)) : \mathbb{F}(\alpha_p(P))] = p$ ou 1.

Si cette extension est d'ordre p, puisque $\mathbb{L}(\alpha_p(P)) = \mathbb{L}(P)$, il existe un élément $\tilde{\rho}$ qui engendre $\mathrm{Gal}(\mathbb{L}(H[\alpha_p^k], P)/\mathbb{F}(\alpha_p(P)))$ et qui coïncide avec ρ sur $\mathbb{L}(H[\alpha_p^k])$. On pose $Q = \tilde{\rho}(P) - P$. Par construction de $\tilde{\rho}$, $Q \in H[\alpha_p]$. On peut donc trouver $T \in H[\alpha_p^k]$ tel que $(\tilde{\rho} - 1)(T) = Q$ et alors

$$\tilde{\rho}(P - T) = \tilde{\rho}(P) - \tilde{\rho}(T) = \tilde{\rho}(P) - Q - T = P - T.$$

Le point $P - T$ est défini sur $\mathbb{L}(H[\alpha_p^k], P)$ et il est fixé par $\tilde{\rho}$, donc $\mathbb{F}(P - T) \subseteq \mathbb{F}(\alpha_p(P))$.

Si au contraire $[\mathbb{L}(H[\alpha_p^k], \alpha_p(P)) : \mathbb{F}(\alpha_p(P))] = 1$, en utilisant encore $\mathbb{L}(\alpha_p(P)) = \mathbb{L}(P)$, on a $\mathbb{F}(\alpha_p(P)) = \mathbb{F}(P)$ et on retrouve l'inclusion $\mathbb{F}(P - T) \subseteq \mathbb{F}(\alpha_p(P))$ avec $T = 0$.

Puisque $\mathbb{E} \subseteq \mathbb{F}$ on a dans les deux cas

$$[\mathbb{F}(P - T) : \mathbb{F}] \leq [\mathbb{F}(\alpha_p(P)) : \mathbb{F}] \leq [\mathbb{E}(\alpha_p(P)) : \mathbb{E}] = D.$$

Ceci implique $\mathbb{F} \in \mathcal{A}$ et $\mathbb{F} \subset \mathbb{Q}_p(\zeta_{m'/p})$ et alors $f_p(\mathbb{F}) \leq p^{k-1} < f_p(\mathbb{L})$.

Pour conclure il faut montrer que pour un premier $\ell \neq p$ on a toujours $f_\ell(\mathbb{F}) \leq f_\ell(\mathbb{L})$. Dans ce cas,

$$f(\mathbb{F}) < f(\mathbb{L})$$

ce qui contredit la minimalité du conducteur de $\mathbb{L}$.

D'après le corollaire 2 de (ST68), si A a bonne réduction en w, pour tout n premier à $\ell = \mathrm{char}(k_w)$, l'extension $K(A[n])/K$ est non ramifiée en w. Quitte à prendre une extension de K, on peut supposer que, pour tout $\ell \in \mathcal{P}$, A a bonne réduction. On applique ce résultat à $\ell \in \mathcal{P}$ tel que $\ell \neq p$ et on en déduit que $K(A[p^k])/K$ est non ramifiée en ℓ. Ceci implique que $\mathbb{Q}_\ell(A[p^k])/\mathbb{Q}_\ell$ est non ramifiée et donc $\mathbb{Q}_\ell(A[p^k]) \subseteq \mathbb{Q}_\ell^{\mathrm{nr}}$. Il existe donc un entier r premier à ℓ tel que $\mathbb{Q}_\ell(A[p^k]) \subseteq \mathbb{Q}_\ell(\zeta_r)$. Si on note t le plus petit entier tel que $\mathbb{L}_w \subseteq \mathbb{Q}_\ell(\zeta_t)$ pour $w|\ell$, on a finalement

$$\mathbb{L}(H[\alpha_p^k]) \subseteq \mathbb{L}(A[p^k]) \subseteq \mathbb{Q}_\ell(\zeta_t, \zeta_r) \subseteq \mathbb{Q}_\ell(\zeta_{f_\ell(\mathbb{L})r'})$$

où $(r', \ell) = 1$ et donc $f_\ell(\mathbb{L}(H[\alpha_p^k])) \leq f_\ell(\mathbb{L})$, ce qu'il fallait démontrer.

Le lemme suivant est l'équivalent du lemme 3 de (Dob79) (dans $\mathbb{G}_\mathrm{m}$) et du lemme 4.2 de (Lau83) pour un point dans une courbe elliptique. On peut reprendre cette dernière démonstration ou bien encore utiliser la proposition 2.18 (*ii*) dans le cas particulier où $V = P$.

Lemme 3.10. *Pour tout $p \in \mathcal{P}$ sauf pour au plus $\frac{\log D}{\log 2}$ d'entre eux on a*

$$\mathbb{L}(P) = \mathbb{L}(\alpha_p(P)).$$

4 Lemme de Siegel

La preuve du théorème 1.15 suit les étapes d'une preuve classique d'approximation diophantienne : construction d'une fonction auxiliaire, extrapolation et lemme de zéros. On devra séparer deux cas : "peu ramifié" et "très ramifié". Dans le premier on va construire une fonction auxiliaire grâce à un lemme de Siegel absolu, donc à coefficients dans $\bar{K}$, qui s'annule en un point Q donné et en tous ses conjugués sur $\mathbb{L}$ à un ordre élevé. L'extrapolation nous permettra de montrer que cette fonction s'annule en des transformés de ces points par des endomorphismes de Frobenius à un certain ordre. Dans le deuxième cas on utilisera des déterminants d'interpolation pour arriver à une conclusion similaire : l'existence d'une fonction à coefficients dans $\bar{K}$ nulle en des translatés par des points de torsion des conjugués de Q sur $\mathbb{L}$ à un certain ordre.

Soient A/K une variété abélienne, $\mathcal{L}$ un fibré ample et symétrique sur A et H/K une sous-variété abélienne de A. Soit $Q \in H(\bar{K})$ d'ordre infini modulo toute sous-variété abélienne propre de H et $\mathbb{L} \subseteq K_{\text{tors}}$. On se donne des entiers positifs L, M et T_0. On veut construire un polynôme F bihomogène de bidegré (L, L) à coefficients dans $\bar{K}$, de hauteur bornée, nul en (Q, MQ) et ses conjugués sur $\mathbb{L}$ à l'ordre $> T_0$ le long de $T_{\iota(H)(\mathbb{C})}$ où $\iota : Q \mapsto (Q, MQ)$. Fixons aussi Z une sous-variété propre de H définie sur $\mathbb{L}$ passant par Q telle que

$$\omega_{\mathbb{L}}(Q, H) = \left(\frac{\deg(Z)}{\deg H}\right)^{1/\operatorname{codim}_H Z}.$$

On reprend ici brièvement les notations et résultats de (DH00), paragraphe 4.1 sur les opérateurs différentiels. On rappelle qu'il existe un plongement $\varphi_{\mathcal{L}}$ projectivement normal associé au fibré $\mathcal{L}$, $\varphi_{\mathcal{L}} : A \hookrightarrow \mathbb{P}^n$. Notons $\mathfrak{U}$ l'idéal premier de définition de A dans $K[X_0, \ldots, X_n]$ et $\mathcal{A}$ l'anneau des coordonnées $K[X_0, \ldots, X_n]/\mathfrak{U}$. Soit $u \in A(K)$, $\mathfrak{m}$ son idéal de définition dans A, $\mathcal{A}_{\mathfrak{m}}$ l'anneau local au point u et $\hat{\mathcal{A}}_{\mathfrak{m}}$ son complété pour la topologie $\mathfrak{m}$-adique. On sait que $\hat{\mathcal{A}}_{\mathfrak{m}}$ est isomorphe à $K[[T_1, \ldots, T_g]]$. En particulier pour $u = 0$ on fixe un tel isomorphisme qu'on notera Φ_0. Si on note $s : A \times A \to A$ l'addition dans A et s^* son image réciproque au niveau des K-algèbres, on peut définir pour tout $u \in A(K)$ des isomorphismes Φ_u de $\hat{\mathcal{A}}_{\mathfrak{m}}$ avec $K[[T_1, \ldots, T_g]]$ par

$$\Phi_u = \Phi_0 \circ (\mathrm{Id} \otimes \pi) \circ s^* : \hat{\mathcal{A}}_{\mathfrak{m}} \xrightarrow{\sim} \hat{\mathcal{A}}_{\mathfrak{m}_0} \otimes_K (\hat{\mathcal{A}}_{\mathfrak{m}}/\mathfrak{m}\hat{\mathcal{A}}_{\mathfrak{m}}) \simeq \hat{\mathcal{A}}_{\mathfrak{m}_0},$$

où π désigne la projection canonique $\pi : \hat{\mathcal{A}}_{\mathfrak{m}} \to \hat{\mathcal{A}}_{\mathfrak{m}}/\mathfrak{m}\hat{\mathcal{A}}_{\mathfrak{m}} \simeq K$.

Maintenant, on peut définir une base de l'espace des opérateurs différentiels $\mathrm{Hom}_K(\hat{\mathcal{A}}_{\mathfrak{m}}, K)$ à l'aide des $(\partial^{\boldsymbol{k}}_{\Phi_u})_{\boldsymbol{k} \in \mathbb{N}^g}$, en posant

$$\partial^{\boldsymbol{k}}_{\Phi_u} = \frac{1}{\boldsymbol{k}!} \frac{\partial^{|\boldsymbol{k}|}}{\partial T^{\boldsymbol{k}}}\bigg|_{(T=0)}$$

où on note pour $\boldsymbol{k} = (k_1, \ldots, k_g)$, $|\boldsymbol{k}| = k_1 + \cdots + k_g$ et $\boldsymbol{k}! = k_1! \cdots k_g!$. Soient $\epsilon_1, \ldots, \epsilon_g$ les vecteurs de la base canonique de $\mathbb{R}^g$, alors les $\partial^{\epsilon_i}_{\Phi_u}$ forment une base de l'espace tangent de A en u, $\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, K)$.

On définit maintenant la notion de dérivation d'un polynôme homogène de $K[X_0, \ldots, X_n]$ à l'ordre $\geq T+1$ en un point $u \in A$. Soit P un tel polynôme de degré D, u un point de A et F une forme homogène de $K[X_0 \ldots, X_n]$ de degré D non nulle en u. On note $P_{u,F}$ l'image de $\frac{P}{F}$ dans $\hat{\mathcal{A}}_{\mathfrak{m}}$. On dit que P s'annule à l'ordre $\geq T+1$ au point u si pour toute carte de A de la forme $\{F \neq 0\}$ contenant u on a $\partial^{\boldsymbol{k}}_{\phi_u} P_{u,F} = 0$ pour tout élément $\boldsymbol{k} \in \mathbb{N}^g$ tel que $|\boldsymbol{k}| \leq T$.

On définit aussi pour $\mathcal{V}$ un sous-espace vectoriel de $T_{A(\mathbb{C})}$ de dimension d, la notion d'annulation de P au point u à l'ordre $\geq T+1$ le long de $\mathcal{V}$. Pour faire ceci on choisit une base de $\mathcal{V}$ qu'on complète en une base de $T_{A(\mathbb{C})}$ à l'aide des $\partial^{\epsilon_i}_{\Phi_0}$ et on convient que ces vecteurs sont numérotés de $d+1$ à g. On dit que P est nul en u à un ordre $\geq T+1$ le long de $\mathcal{V}$ si $\partial^{\boldsymbol{k}}_{\Phi_u} P_{u,F} = 0$ pour tout $\boldsymbol{k} \in \mathbb{N}^d$ tel que $|\boldsymbol{k}| \leq T$ et où l'on identifie $\boldsymbol{k} \in \mathbb{N}^d$ à l'élément de $\mathbb{N}^g$ dont les dernières $g-d$ coordonnées sont nulles.

Soit α une isogénie admissible de degré $q(\alpha)$, on note α^* le morphisme d'algèbres déduit de α :

$$\begin{aligned} \alpha^* : \mathcal{A} &\longrightarrow \mathcal{A}, \\ P &\longmapsto P(P_{0,\alpha}, \ldots, P_{n,\alpha}), \end{aligned}$$

où $(P_{0,\alpha}, \ldots, P_{n,\alpha})$ est une famille de polynômes homogènes de degré $q(\alpha)$ représentant l'action de α sur A. Soit $u \in A$ et $s^*_u : \mathcal{A} \to \mathcal{A} \otimes \hat{\mathcal{A}}_{\mathfrak{m}}$ le morphisme d'algèbres déduit de l'addition dans A au voisinage de $(0, u)$.

Définition 4.1. *Soient $u \in A$, α une isogénie admissible et $\boldsymbol{k} \in \mathbb{N}^g$. Pour tout $P \in \mathcal{A}$, on note $\partial^{\boldsymbol{k}}_{u,\alpha}(P)$ le coefficient du monôme $T^{\boldsymbol{k}}$ de*

$$(\mathrm{Id} \otimes \Phi_u) \circ \alpha^* \otimes \mathrm{Id} \circ s^*_u(P) \in \mathcal{A} \otimes K[[T_1, \ldots, T_g]].$$

La série de Taylor $\sum_{\boldsymbol{k}\in\mathbb{N}^n} \partial^{\boldsymbol{k}}_{u,\alpha}(P)\mathbf{T}^{\boldsymbol{k}}$ *est l'image de* P *par l'application :*

$$\mathcal{A} \xrightarrow{s_u^*} \mathcal{A}\otimes\hat{\mathcal{A}}_{\mathfrak{m}} \xrightarrow{\alpha^*\otimes\mathrm{Id}} \mathcal{A}\otimes\hat{\mathcal{A}}_{\mathfrak{m}} \xrightarrow{\mathrm{Id}\otimes\Phi_u} \mathcal{A}\otimes K[[T_1,\dots,T_g]].$$

On vérifie facilement que $\partial^{\boldsymbol{k}}_{u,\alpha}(P)\in\mathcal{A}$ et, au voisinage de l'origine, la nullité de $\partial^{\boldsymbol{k}}_{u,\alpha}(P)$ ne dépend pas du choix des formes représentant l'addition ou l'isogénie α.

Soit k un entier positif, $\mathcal{V}$ un sous-espace vectoriel de $T_{A(\mathbb{C})}$ de dimension d et $\mathfrak{J}$ un idéal homogène de $\mathcal{A}$. On note $\partial^{k,\mathcal{V}}_{u,\alpha}\mathfrak{J}$ l'idéal

$$(\partial^{\boldsymbol{k},\mathcal{V}}_{u,\alpha}(Q), \boldsymbol{k}\in\mathbb{N}^d, |\boldsymbol{k}|\le k, Q\in\mathfrak{J})$$

où l'on considère $\boldsymbol{k}\in\mathbb{N}^d$ comme un élément de $\mathbb{N}^k$ dont les d premières directions de dérivation correspondent à une base de $\mathcal{V}$.

Le lemme suivant relie les notations qu'on a introduites plus haut :

Lemme 4.2. *Soient* $u,h\in A$, α *une isogénie admissible,* $k\in\mathbb{N}$, $\mathfrak{J}$ *un idéal homogène de* $\mathcal{A}$ *et* $\mathcal{V}$ *un sous-espace vectoriel de dimension* d *de* $T_{A(\mathbb{C})}$. *Les propriétés suivantes sont équivalentes :*

(i). $h\in\mathcal{Z}(\partial^{k,\mathcal{V}}_{u,\alpha}\mathfrak{J})$.

(ii). Tout polynôme de $\mathfrak{J}$ *s'annule à un ordre* $\ge k+1$ *en* $u+\alpha(h)$ *le long de* $\mathcal{V}$.

Proof. C'est le lemme 4.6 de (DH00).

4.1 Majoration du rang du système

On considère le plongement

$$\begin{aligned}\iota : A &\longrightarrow A\times A\\ P &\longmapsto (P, MP)\end{aligned}$$

et $\varphi_{\mathcal{L}}$ un plongement projectivement normal associé au fibré $\mathcal{L}=\mathcal{L}_0^{\otimes 4}$. On pose $\mathcal{M}=\pi_1^*\mathcal{L}\otimes\pi_2^*\mathcal{L}$ le fibré sur $A\times A$ construit à l'aide des projections sur les premier et deuxième facteurs. On va construire un élément F de $\Gamma(H\times H,\mathcal{M}^{\otimes L}_{|H\times H})$. Soit $s_0,\dots,s_l$ une base du K-espace vectoriel $\Gamma(H\times H,\mathcal{M}_{|H\times H})$ et $f_1,\dots,f_m$ des monômes de degré L en les s_i, formant une base de $\Gamma(H\times H,\mathcal{M}^{\otimes L}_{|H\times H})$. Le polynôme F sera donc de la forme

$$F=\sum_{i=1}^m b_i f_i$$

où les coefficients b_i sont dans $\bar{K}$. On fixe une base $\partial^{\epsilon_1}_{\Phi_0},\dots,\partial^{\epsilon_{2g_0}}_{\Phi_0}$ de l'espace tangent à l'origine de $H\times H$. Alors, l'espace tangent à l'origine de $\iota(H)$ a pour base les opérateurs

$$\delta_i=\partial^{\epsilon_i+M\epsilon_{g_0+i}}_{\Phi_0},\quad i=1,\dots,g_0$$

et on note $\delta^{\boldsymbol{k},T_{\iota(H)}}_{(Q,MQ)}$ l'opérateur

$$\left(\partial^{\epsilon_1+M\epsilon_{g_0+1}}_{\Phi_{(Q,MQ)}}\right)^{k_1}\circ\cdots\circ\left(\partial^{\epsilon_{g_0}+M\epsilon_{2g_0}}_{\Phi_{(Q,MQ)}}\right)^{k_{g_0}}=\left(\delta_1\circ t^*_{(Q,MQ)}\right)^{k_1}\circ\cdots\circ\left(\delta_{g_0}\circ t^*_{(Q,MQ)}\right)^{k_{g_0}}$$

où $\boldsymbol{k}=(k_1,\dots,k_{g_0})\in\mathbb{N}^{g_0}$. Le système qu'on cherche à résoudre s'écrit simplement

$$\delta^{\boldsymbol{k},T_{\iota(H)(\mathbb{C})}}_{(Q,MQ)}F=0,\quad\forall\,\boldsymbol{k}\in\mathbb{N}^{g_0},\ \ |\boldsymbol{k}|\le T_0. \tag{6}$$

En fait, puisque $Q\in Z$ et Z est défini sur $\mathbb{L}$, il suffit que F soit nulle sur tous les points de la sous-variété $\iota(Z)$. Notons $\mathcal{D}$ l'idéal de définition de $\iota(Z)$ et $d=\dim(Z)$. On a le résultat suivant pour la majoration du rang du système :

Lemme 4.3. *Il existe une constante positive* c_6 *telle que le rang du système (6) soit majoré par*

$$c_6T_0^{g_0-d}\omega_{\mathbb{L}}(Q,H)^{g_0-d}\deg H(LM^2)^d.$$

Proof. (Esquisse) C'est le lemme 5.1 de (DH00) où l'on tient compte du fait que l'on travaille sur la sous-variété $H \times H$ et non $A \times A$, du fait que la variété Z est définie sur $\mathbb{L}$ et qu'on s'intéresse à une solution dans $\bar{K}$. L'idée de la preuve est de se ramener à d'autres systèmes pour lesquels on peut calculer plus facilement et de façon plus précise le rang.

En notant $\mathcal{D}$ l'idéal de définition de $\iota(Z)$ et W l'espace tangent à l'origine de $\iota(H)$, on considère le système

$$\partial_{u,\mathrm{Id}}^{\boldsymbol{k},W} F \in t_{-u}^*(\mathcal{D}), \quad \forall u \in \iota(Z), \forall \boldsymbol{k} \in \mathbb{N}^{g_0}, |\boldsymbol{k}| \leq T_0. \tag{7}$$

On montre ensuite que toute solution F de (7) est une solution de (6). En effet, si F est solution de (7), on pose $u = \iota(Q)$ et on trouve qu'en particulier F est nulle en $\iota(0)$, d'où $\delta_{(Q,MQ)}^{\boldsymbol{k},W} F = 0$.

Ensuite, quitte à renuméroter les indices, on peut supposer qu'il existe un ouvert Ω de Z sur lequel les opérateurs $\partial_{\Phi_{\iota(x)}}^{\epsilon_1+M\epsilon_{g_0+1}}, \ldots, \partial_{\Phi_{\iota(x)}}^{\epsilon_{g_0-d}+M\epsilon_{2g_0-d}}$ se projettent sur une base de l'espace normal à $\iota(Z)$ en $\iota(x)$, pour tout $x \in \Omega$. Quitte à restreindre Ω, on peut supposer que si $\partial_{\iota(x),\mathrm{Id}}^{\epsilon_i+M\epsilon_{g_0+i}}(F)$ est nulle sur $\iota(0)$, alors $\partial_{\Phi_{\iota(x)}^{\epsilon_i+M\epsilon_{g_0+i}}} F = 0$ pour tout $x \in \Omega$, pour tout $i = 1 \ldots, g_0$ et toute forme F de $\mathcal{H}'$ l'anneau des coordonnées de $H \times H$ plongé dans un espace projectif *via* le fibré $\mathcal{M}_{|H\times H}$. On note W' le sous-espace linéaire de W engendré par les vecteurs $\epsilon_1 + M\epsilon_{g_0+1}, \ldots, \epsilon_{g_0-d} + M\epsilon_{2g_0-d}$ et on fixe $\iota(x)$ dans $\iota(\Omega)$. On considère le système

$$\partial_{\iota(x),\mathrm{Id}}^{\boldsymbol{k},W'} F \in t_{-\iota(x)}^*(\mathcal{D}), \quad \forall \boldsymbol{k} \in \mathbb{N}^{g_0-d}, |\boldsymbol{k}| \leq T_0. \tag{8}$$

On montre ensuite que les systèmes (7) et (8) sont équivalents (voir (DH00), p. 39–40).

On peut donc majorer le rang du système (6) par le rang du système (8). Dire que $\partial_{-\iota(x),\mathrm{Id}}^{\boldsymbol{k},W'} F \in t_{\iota(x)}^*(\mathcal{D})$ revient à dire que l'image de $\partial_{\iota(x),\mathrm{Id}}^{\boldsymbol{k},W'} F$ dans $\mathcal{H}'/t_{-\iota(x)}^*(\mathcal{D})$ est nulle. Le nombre de conditions à écrire est donc $\leq \dim_{\bar{K}}(\mathcal{H}'/t_{-\iota(x)}^*(\mathcal{D}))_L$. D'après le théorème de (Cha89),

$$\dim_{\bar{K}}(\mathcal{H}'/t_{-\iota(x)}^*(\mathcal{D}))_L \leq c_7 \binom{L+d}{d} \deg(\iota(Z)) \leq c_8 L^d \deg(\iota(Z)),$$

d'où le rang r du système (8) est majoré par

$$c_8 T_0^{g_0-d} \deg(\iota(Z)) L^d.$$

Puisque $\deg(\iota(Z)) = (M^2+1)^d \deg(Z)$ (voir (Phi95) prop. 7) on a

$$\begin{aligned} r &\leq c_9 T_0^{g_0-d} (LM^2)^d \deg(Z) \\ &\leq c_{10} T_0^{g_0-d} (LM^2)^d \omega_{\mathbb{L}}(Q,H)^{g_0-d} \deg(H). \end{aligned}$$

4.2 Hauteur des équations et nombre d'inconnues

Soit $F = \sum_i b_i \mathbf{X}^i$ un polynôme à coefficients dans $\bar{K}$. On définit sa hauteur $h(F)$ comme la hauteur logarithmique de Weil du point projectif défini par ses coefficients et 1.

Lemme 4.4. *La hauteur de chaque coefficient du système (6) est majorée par*

$$c_{11}(LM^2 \hat{h}(Q) + T_0 \log(T_0 + L) + T_0 \log M + L).$$

Proof. On reprend les estimations de (DH00), p. 41–42. On rappelle que les opérateurs $\delta_{(Q,MQ)}^{\boldsymbol{k}}$ sont définis comme $\left(\delta_1 \circ t_{(Q,MQ)}^*\right)^{k_1} \circ \cdots \circ \left(\delta_{g_0} \circ t_{(Q,MQ)}^*\right)^{k_{g_0}}$. On montre dans une première partie, que si δ est un monôme de poids k en les $\delta_{\Phi_0}^{\epsilon_j}$ pour $1 \leq j \leq 2g_0$ et $G \in \Gamma(H \times H, \mathcal{M}_{|H\times H}^{\otimes L})$, alors $\delta(G)$ est un polynôme de degré $\leq L + k$ et

$$h(\delta(G)) \leq h(G) + c_{12}(k + k\log(k+L) + k\log(M)),$$

voir (Dav91) théorème 4.1. On applique ceci à l'opérateur $\delta_i \circ \cdots \circ \delta_{g_0}$ et on obtient

$$h(\delta_1 \circ \cdots \circ \delta_{g_0}(G)) \leq h(G) + c_{13}(k\log(k+L) + k\log(M)).$$

Ensuite, on utilise le fait que les translations peuvent être représentées par des formes de bidegré $(2,2)$ (voir (LR85), théorème p. 603) pour déduire que $t_{(Q,MQ)}^*(G)$ est de degré $\leq 2L$ et de hauteur $\leq h(G) + c_{14} L h(Q, MQ)$. En mettant ces deux inégalités ensemble et en utilisant les propriétés de la hauteur canonique, on trouve que pour $\boldsymbol{k} \in \mathbb{N}^{g_0}$, $|\boldsymbol{k}| \leq T_0$ on a

$$h(\delta_{(Q,MQ)}^{\boldsymbol{k}}(G)) \leq c_{15}(h(G) + L + LM^2\hat{h}(Q) + T_0 \log(T_0+L) + T_0 \log M).$$

Finalement, on évalue $\delta_{(Q,MQ)}^{\boldsymbol{k}}(G)$ à l'origine pour un monôme G et on obtient le résultat désiré.

Calculons maintenant le nombre d'inconnues du système. On veut que F soit non identiquement nulle sur $\iota(H)$ donc le système (6) a $I = \dim_K \Gamma(H \times H, \mathcal{M}^{\otimes L}_{|H\times H})$ inconnues. En utilisant les estimations de (Cha89), quitte à supposer que $L \geq \deg(H)$, on sait que cette quantité vérifie la relation

$$c_{16} \deg(H)(LM^2)^{g_0} \leq \quad I \quad \leq c_{17} \deg(H)(LM^2)^{g_0}. \tag{9}$$

4.3 Lemme de Siegel

On rappelle que l'exposant de Dirichlet η associé à un système linéaire est

$$\eta = \frac{r}{I-r}$$

où r est le rang du système et I le nombre d'inconnues.

Lemme 4.5. *Si $(LM^2)^{g_0-d} \geq c_{18} T_0^{g_0-d} \omega_{\mathbb{L}}(Q,H)^{g_0-d}$ et $L \geq \deg(H)$, il existe une fonction F solution du système (6) de hauteur bornée par*

$$c_{19}\Big(\eta(LM^2\hat{h}(Q) + T_0\log(T_0+L) + T_0 \log M + L) + \log(LM^2\deg(H))\Big) \tag{10}$$

où η désigne l'exposant de Dirichlet du système (6).

Puisque l'on veut construire la fonction auxiliaire à coefficients dans $\bar{K}$ on va utiliser un lemme de Siegel absolu. On définit la hauteur h_2 sur $\mathbb{P}^n(\bar{\mathbb{Q}})$ par

$$h_2(x_0:\ldots:x_n) = \frac{1}{[K:\mathbb{Q}]}\left(\sum_{v\in M_K^0} n_v \log \max_{0\leq i\leq n}|x_i|_v + \sum_{v\in M_K^\infty} n_v \log\sqrt{\sum_{0\leq i\leq n}|x_i|_v^2}\right),$$

et la hauteur h_2 d'un sous-$\bar{\mathbb{Q}}$-espace vectoriel S de dimension s de $\bar{\mathbb{Q}}^{n+1}$ par

$$h_2(S) = h_2(x_1 \wedge \ldots \wedge x_s)$$

où $x_1,\ldots,x_s$ est une base de S sur un corps de nombres quelconque sur lequel S est défini.

Lemme 4.6. *Soient n un entier et S un sous-$\bar{K}$-espace vectoriel de dimension $s \geq 1$ de $\bar{K}^s$. Il existe un vecteur $x \neq 0 \in n$ tel que*

$$h_2(x) \leq \frac{h_2(S)}{s} + \frac{\log s}{2}.$$

Proof. Voir (DP99), lemme 4.7.

On peut continuer la preuve du lemme 4.5. Soit B la matrice du système (6) et notons comme précédemment I le nombre d'inconnues. On cherche une solution de $\{Bb = 0\}$, donc un élément du noyau $\mathcal{N}$ de B. On sait que

$$\dim(\mathcal{N}) = I - \ \mathrm{rang}(B) \geq c_{16}(LM^2)^{g_0}\deg(H) - c_6 T_0^{g_0-d}\omega_{\mathbb{L}}(Q,H)^{g_0-d}(LM^2)^d \deg(H).$$

Maintenant, pour appliquer le lemme 4.6, il faut calculer $h_2(\mathcal{N})$ ou ce qui est équivalent, $h_2(\mathcal{N}^\perp)$ (voir (Sch91) lemme IV, p. 10).

Si $\tilde{B}$ est une sous-matrice de rang maximal de B alors $\mathcal{N}^\perp$ est l'espace engendré par les colonnes de $\tilde{B}$. On remarque que la hauteur de l'espace engendré par les colonnes de $\tilde{B}$ est égale à la hauteur de l'espace engendré par ses lignes. Si on note y_j une base de cet espace et on utilise les bornes pour la hauteur des équations et le rang du système on a :

$$\begin{aligned} h_2(\mathcal{N}^\perp) &\leq \sum_j h_2(y_j) \\ &\leq \mathrm{rang}\ (\tilde{B}) \max_j h_2(y_j) \\ &\leq c_{11} r(LM^2\hat{h}(Q)T_0\log(T_0+L) + T_0\log M + L). \end{aligned}$$

En appliquant le lemme 4.6 on trouve qu'il existe un polynôme F à coefficients dans $\bar{K}$ tel que

$$\begin{aligned} h_2(F) &\leq \frac{c_{11} r(LM^2\hat{h}(Q) + T_0\log(T_0+L) + T_0\log M + L)}{I-r} + c_{20}\log((LM^2)^{g_0}\deg H) \\ &\leq c_{21}\eta(LM^2\hat{h}(Q) + T_0\log(T_0+L) + T_0\log M + L) + c_{22}\log(LM^2\deg(H)) \end{aligned}$$

où η est l'exposant de Dirichlet du système. D'après une remarque de Roy-Thunder (p. 7 de (RT96)) on peut trouver F à coefficients entiers algébriques dans $\bar{K}$ tel que $h(F)$ soit bornée par la même quantité à une constante près.

5 Extrapolation

Commençons d'abord par quelques préliminaires. On rappelle que $\mathcal{P}$ est l'ensemble des premiers > 2 qui se décomposent totalement dans K et que pour chaque $p \in \mathcal{P}$ on a choisi une seule place v de M_K. On rappelle aussi qu'on a noté e_p l'indice de ramification de la place v au dessus de p dans le corps $\mathbb{L}$.

Soient N_i et E_i des entiers positifs pour $i = 1, \ldots, g_0$. Pour chaque i, on définit un ensemble $\mathcal{P}_i$ d'endomorphismes de Frobenius de la façon suivante : on note α_p un endomorphisme de Frobenius en v la place de K fixée au-dessus de p et on pose

$$\mathcal{P}_i = \{\alpha_p,\ p \in \mathcal{P},\ \frac{N_i}{2} \leq p \leq N_i\} \cup \{\mathrm{Id}\}.$$

On définit ensuite

$$\begin{aligned}\Delta_i^{(\mathrm{pr})} &= \{\alpha_p \in \mathcal{P}_i,\ e_p \leq E_i\} \cup \{\mathrm{Id}\},\\ \Delta_i^{(\mathrm{tr})} &= \{\alpha_p \in \mathcal{P}_i,\ e_p > E_i\}.\end{aligned}$$

Pour chaque ensemble $\mathcal{P}_i$, on va procéder de façon différente suivant que l'on a peu ou beaucoup de grande ramification. On quantifie ceci de la façon suivante :

Définition 5.1. *Pour un entier i tel que $1 \leq i \leq g_0$ on dit que $\mathcal{P}_i$ est peu ramifié si*

$$\left|\Delta_i^{(\mathrm{pr})}\right| \geq \frac{|\mathcal{P}_i|}{2}.$$

Da façon équivalente, on dit que $\mathcal{P}_i$ est très ramifié si

$$\left|\Delta_i^{(\mathrm{tr})}\right| > \frac{|\mathcal{P}_i|}{2}.$$

Étant donné des ensembles $\mathcal{P}_1, \ldots, \mathcal{P}_{g_0}$ on dira qu'on est dans le "cas peu ramifié" si tous les ensembles $\mathcal{P}_i$ sont peu ramifiés.

On sera dans le "cas très ramifié" s'il existe i, $1 \leq i \leq g_0$ tel que $\mathcal{P}_i$ soit très ramifié.

On fixe des paramètres qui satisfont des conditions différentes dans chaque cas. On fixe aussi une constante C_0 qui ne dépend que de A, K et $\mathcal{L}$ assez grande (on veut dire par là que toutes les inégalités qu'on écrira seront vraies et ceci est possible car il n'y a qu'un nombre fini d'inégalités qui interviendront).

Cas peu ramifié. On pose M, L, T_i pour $i = 0, \ldots, g_0$ des entiers satisfaisant les propriétés suivantes :

$$\begin{aligned}
\deg(H) &\leq L; && (11)\\
(LM^2)^{g_0-d} &\geq C_0^{\frac{1}{2}} T_0^{g_0-d} \omega_{\mathbb{L}}(Q,H)^{g_0-d}; && (12)\\
T_{i+1} &\leq \frac{T_i \log(N_{g_0-i})}{\log(C_0) E_{g_0-i} \log(T_{i+1}+L)}; && (13)\\
\frac{N_k}{\log(N_k)} &\geq C_0^{\frac{1}{2}} \log((LM^2 N_1 \cdots N_{k-1})^{g_0} \deg H) && (14)\\
L &\leq M^2 \leq 4L && (15)\\
\log(LM^2 \deg(H)) &\leq \frac{T_i \log(N_{g_0-i})}{\log(C_0) E_{g_0-i}}. && (16)
\end{aligned}$$

Cas très ramifié. On choisit une fois pour toutes le plus petit indice i tel que $\mathcal{P}_i$ est très ramifié ; on notera cet indice $r(\mathcal{P})$. On pose M, L, T_0, T_1 des entiers satisfaisant :

$$\begin{aligned}
\deg(H) &\leq L; && (17)\\
(LM^2)^{g_0-d} &\geq C_0^{\frac{1}{2}} T_0^{g_0-d} \omega_{\mathbb{L}}(Q,H)^{g_0-d}; && (18)\\
\log(L \deg H) &\leq \frac{T_0 \log N_{r(\mathcal{P})}}{C_0^{\frac{1}{2}} N_{r(\mathcal{P})}} && (19)\\
T_1 &\leq \frac{T_0 \log N_{r(\mathcal{P})}}{\log(C_0) N_{r(\mathcal{P})} \log(T_1+L)} && (20)\\
\frac{T_0 \log N_{r(\mathcal{P})}}{L N_{r(\mathcal{P})}} &\geq C_0^{\frac{1}{2}} && (21)\\
L &\leq M^2 \leq 4L. && (22)
\end{aligned}$$

On verra au cours de la démonstration pourquoi on a besoin de ces conditions. Grosso modo, les conditions (11) et (17) justifieront la minoration de la fonction de Hilbert. Ceci joint aux conditions (12) et (18) permettra de construire les fonctions auxiliaires. Ensuite (13) (dans le cas peu ramifié) et (19), (20), (21) (dans le cas très ramifié) permettent d'extrapoler. Pour simplifier les calculs, on va aussi supposer dans les deux cas que M est une puissance de 2.

Lorsqu'on est dans le premier cas, on procède à une extrapolation proche de celle de (DH00), dans l'autre cas on suivra l'argument de (Amo).

Soit $Q \in H$ comme plus haut, F la fonction construite à l'aide du lemme de Siegel pour les paramètres T_0, L et M qu'on vient de fixer, et η l'exposant de Dirichlet associé. On fait de plus les hypothèses suivantes pour tout $i = 0, \ldots, g_0 - 1$:

$$\begin{aligned} \hat{h}(Q) &\leq \frac{T_i \log N_{g_0-i}}{(\log C_0) LM^2 E_{g_0-i} N_{g_0-i} \cdots N_{g_0}}; && (23) \\ \eta &\leq \frac{T_i \log N_{g_0-i}}{C_0^{\frac{1}{2}} E_{g_0-i}[T_0 \log(T_0+L)M + L]} && (24) \end{aligned}$$

dans le cas peu ramifié. Ceci entraîne en particulier

$$\hat{h}(Q) < \frac{T_0 \log(T_0+L)M + L}{LM^2}. \tag{25}$$

Dans le cas très ramifié on impose

$$\hat{h}(Q) \leq \frac{T_0 \log N_{r(\mathcal{P})}}{(\log C_0) N_{r(\mathcal{P})} LM^2}. \tag{26}$$

On aura besoin de quelques résultats sur le degré des formes représentant les endomorphismes de Frobenius et la multiplication par M. Il s'agit des lemmes 6.1 et 6.2 de (DH00) et du lemme 2.1 de (DP98).

Lemme 5.2. *(i). Il existe une constante c telle que, pour tout $m \geq 1$, il existe des formes $\mathbf{F}^{2^m} = (F_0^{(2^m)}, \ldots, F_n^{(2^m)}) \in \mathcal{O}_K[X_0, \ldots, X_n]$, homogènes de degré 4^m représentant les formules de multiplication par 2^m et telles que pour toute place finie $v \in M_K$ vérifiant $N(v) \geq c$ et pour tout $\mathbf{x} = (x_0, \ldots, x_n) \in A(\mathbb{C}_v)$ on ait*

$$\frac{\|\mathbf{F}^{(2^m)}(\mathbf{x})\|_v}{\|\mathbf{x}\|_v^{(4^m)}} = 1.$$

(ii). Soit $v|p$ une place finie de K vérifiant $N(v) \geq c$, il existe une famille $\mathbf{F}_p$ de formes dans $\mathcal{O}_v[X_0, \ldots, X_n]$ homogènes de degré $N(v)$ représentant l'endomorphisme de Frobenius associé à v sur $A(\mathbb{C}_v)$ et telles que

$$\|\mathbf{F}_p(\mathbf{z})\|_v = \|\mathbf{z}\|_v^{N(v)}.$$

Soit $P \in A(\bar{K})$, v une place finie de K et $\mathcal{A}$ et $\mathcal{A}_v$ les anneaux des coordonnées de A sur $\mathcal{O}_K$ et $\mathcal{O}_v$ respectivement. On notera $\mathfrak{m}_P$ l'idéal de définition de P dans $\mathcal{A}$ et $\mathfrak{m}_{P,v}$ son extension à $\mathcal{A}_v$. Si T est un entier positif, alors on définit

$$\mathfrak{m}_P^{(T)} = \{F \in \mathcal{A}, \partial_{0,\mathrm{Id}}^{\boldsymbol{k}} F \in \mathfrak{m}_P, \forall \boldsymbol{k}, |\boldsymbol{k}| \leq T\}$$

et $\mathfrak{m}_{P,v}^{(T)}$ son extension à $\mathcal{A}_v$. Pour $\beta = (\beta_0, \ldots, \beta_s) \in \mathbb{P}^s(\bar{K})$, on notera de la même façon $\mathfrak{m}_{(P,\beta),v}$ (respectivement $\mathfrak{m}_{(P,\beta)}$, $\mathfrak{m}_{(P,\beta),v}$, $\mathfrak{m}_{(P,\beta),v}^{(T)}$) l'idéal de définition du point (P, β) dans l'anneau des coordonnées de $A \times \mathbb{P}^s$.

Théorème 5.3. *Soient R un point de $A(\bar{K})$, v' une place de $\mathbb{L}$ en laquelle A admet bonne réduction et w une place de $\mathbb{L}(R)$ au dessus de v'. Soit également $(\beta_1, \ldots, \beta_s) \in \mathcal{O}_w^s$ et $\beta = (1, \beta_1, \ldots, \beta_s)$ tel que :*

$$\mathcal{O}_{v'}\left[\frac{X_1(R)}{X_0(R)}, \ldots, \frac{X_n(R)}{X_0(R)}, \beta\right] = \mathcal{O}_w.$$

Alors, pour tout $T \geq 1$, on a

$$\mathfrak{m}_{(R,\beta),v'}^{(T)} = \mathfrak{m}_{(R,\beta),v'}^T$$

(quitte à renuméroter les variables, on peut supposer que $|X_0(R)|_w = \|\mathbf{X}(R)\|_w$).

Proof. C'est le théorème 6.4 de (DH00).

5.1 Cas peu ramifié

Supposons que les ensembles $\mathcal{P}_1, \dots, \mathcal{P}_{g_0}$ sont tous peu ramifiés. On définit alors $\Sigma = \{\sigma(Q),\, \sigma \in \mathrm{Gal}(\bar{K}/\mathbb{L})\}$ et pour chaque $r = 1, \dots, g_0$

$$\Sigma_r = \{\tau_r\alpha_r \circ \dots \circ \tau_{g_0}\alpha_{g_0}(R),\, R \in \Sigma,\, \alpha_r \in \Delta_r^{(\mathrm{pr})},\, \tau_r \in \mathrm{Gal}(\bar{K}/K),\, \tau_r^{-1}|_{\mathbb{L}} = \phi_p\}$$

(où ϕ_p est l'élément fixé par le lemme 2.14 et la remarque qui suit lorsque α_r est un endomorphisme de Frobenius en $v|p$). Lorsque $\alpha_r = \mathrm{Id}$, par convention $\phi_p = \mathrm{Id}$.

On va montrer que la fonction F qu'on a construite s'annule sur l'ensemble $\iota(\Sigma_{g_0-i})$ à l'ordre T_{i+1} le long de $T_{\iota(H)(\mathbb{C})}$. On notera $\Sigma_{g_0+1} := \Sigma$.

On sait par construction que F est nulle sur $\iota(\Sigma)$ à l'ordre T_0. On procède par récurrence, donc on suppose F nulle en $\iota(\Sigma_{g_0-i+1})$ à l'ordre T_i.

Proposition 5.4. *La fonction F est nulle à l'ordre $\geq T_{i+1}$ en tout point de l'ensemble $\iota(\tau \circ \alpha_p(\Sigma_{g_0-i+1}))$, pour tout $\alpha_p \in \Delta_{g_0-i}^{(\mathrm{pr})}$ et $\tau \in \mathrm{Gal}(\bar{K}/K)$ tel que $\tau_{|\mathbb{L}}^{-1} = \phi_p$.*

Soit α_p dans $\Delta_{g_0-i}^{(\mathrm{pr})}$, $\tau \in \mathrm{Gal}(\bar{K}/K)$ tel que $\tau_{|\mathbb{L}} = \phi_p^{-1}$ et $R \in \Sigma_{g_0-i+1}$. On voudrait utiliser la congruence du lemme 2.14, mais elle ne s'applique qu'à des éléments de $\mathcal{O}_{v'}$ pour $v' \in M_{\mathbb{L}}$. Soient donc $\mathbb{F}$ une extension galoisienne de $\mathbb{L}$ contenant les coefficients du polynôme F et les coordonnées du point R et $\partial^{\boldsymbol{k}}$ un opérateur différentiel d'ordre $|\boldsymbol{k}|$. Soient v' une place de $\mathbb{L}$ au-dessus de $v|p$ et w une place de $\mathbb{F}$ au-dessus de v'. On va donc considérer le polynôme

$$J = \prod_{\sigma \in D_w} (\partial^{\boldsymbol{k}} F)^{\sigma}$$

où D_w est le groupe de décomposition de $\mathrm{Gal}(\mathbb{F}/\mathbb{L})$ en w. On sait que $D_w \simeq \mathrm{Gal}(\mathbb{F}_w/\mathbb{L}_{v'})$ et donc J est à coefficients dans $\mathbb{L}_{v'}$.

On choisit des coordonnées w-entières $\mathbf{R} = (R_0, \dots, R_n)$ de R telles que $\|\mathbf{R}\|_w = 1$, on notera R_w une coordonnée de R telle que $|R_w|_w = 1$. On fixe aussi un élément $\beta = (1, \beta_1, \dots, \beta_s)$ à coordonnées dans $\mathcal{O}_w$ tel que $\mathcal{O}_{v'}\left[\frac{R_0}{R_w}, \dots, \frac{R_n}{R_w}, \beta\right] = \mathcal{O}_w$. Vu que F est nul à l'ordre T_i en $\iota(R)$ et tous ses conjugués sur $\mathbb{L}$, J est nul en $\iota(R)$ à l'ordre $(T_i - |k|)[\mathbb{F}_w : \mathbb{L}_{v'}]$. On applique le théorème 5.3 au polynôme J, qui nous dit qu'on peut écrire J comme un produit de polynômes définis sur $\mathbb{L}_{v'}$ nuls en $\iota(R)$ quitte à rajouter des "fausses" variables. On peut donc écrire

$$J(X_0, \dots, X_n, F_0^{(M)}(\mathbf{X}), \dots, F_n^{(M)}(\mathbf{X})) = \sum_l \prod_{s=1}^{t} h_{l_s}(\mathbf{X}, \mathbf{Y}), \tag{27}$$

où $t = (T_i - |k|)[\mathbb{F} : \mathbb{L}]$ et les h_{l_s} sont des polynômes à coefficients dans $\mathcal{O}_{v'}$, nuls en (R, β) (on a noté $(F_0^{(M)}(\mathbf{X}), \dots, F_n^{(M)}(\mathbf{X}))$ des formes homogènes à coefficients dans $\mathcal{O}_K$ représentant la multiplication par M). On rappelle qu'on note $F_{p,0}(\mathbf{X}), ..., F_{p,n}(\mathbf{X})$ des formes représentant l'endomorphisme de Frobenius α_p.

Lemme 5.5. *Soit v la place de M_K fixée au-dessus de $p \in \mathcal{P}$ et α_p l'endomorphisme de Frobenius associé à v. Alors*

$$\log \left|(\partial^{\boldsymbol{k}} F)^{\tau}(\mathbf{F}_p(\mathbf{R}), F^{(M)} \circ \mathbf{F}_p(\mathbf{R}))\right|_w \leq -\frac{(T_i - |k|)}{e_p} \log p,$$

pour toute valuation w de $\bar{K}$ prolongeant v, $\tau \in \mathrm{Gal}(\bar{\mathbb{K}}/\mathbb{K})$ tel que $\tau_{|\mathbb{L}} = \phi_p$ et e_p l'indice de ramification de v dans $\mathbb{L}$.

Proof. On note $(X_0, \dots, X_n)$ des coordonnées d'un point $\mathbf{X} \in \mathbb{P}^n(\bar{K})$ quelconque. On obtient par définition du Frobenius

$$X_j^{N(v)} F_{p,i}(\mathbf{X}) - F_{p,j}(\mathbf{X}) X_i^{N(v)} \in \pi_v \mathcal{O}_K[\mathbf{X}].$$

On rappelle que, d'après la remarque 2.1, $N(v) = p$. On peut donc écrire

$$X_j^p F_{p,i}(\mathbf{X}) - F_{p,j}(\mathbf{X}) X_i^p \in \pi_v \mathcal{O}_K[\mathbf{X}].$$

Soit d le degré de h en X où h est l'un des h_{l_s} dans la décomposition de J. Par homogénéité on peut écrire

$$X_j^{pd} h^{\tau}(\mathbf{F}_p(\mathbf{X}), \mathbf{Y}^p) - F_{p,j}(\mathbf{X})^d h^{\tau}(\mathbf{X}^p, \mathbf{Y}^p) \in \pi_{v'} \mathcal{O}_{v'}[\mathbf{X}, \mathbf{Y}].$$

En utilisant la congruence 2.14 sur les coefficients des polynômes h_{l_s} et le petit théorème de Fermat pour les polynômes on obtient

$$X_j^{pd} h^{\tau}(\mathbf{F}_p(\mathbf{X}), \mathbf{Y}^p) - F_{p,j}(\mathbf{X})^d (h(\mathbf{X}, \mathbf{Y}))^p \in \pi_{v'} \mathcal{O}_{v'}[\mathbf{X}, \mathbf{Y}].$$

En évaluant cette dernière relation en (R,β), on obtient l'inégalité

$$\left|R_j^{pd} h^\tau(\mathbf{F}_p(\mathbf{R}),\beta^p)\right|_w \leq |p^{1/e_{v'/p}}|_w.$$

Si pour un w donné on choisit des coordonnées w-entières de R et on utilise l'équation (27) on obtient

$$|J^\tau(\mathbf{F}_p(\mathbf{R}),\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R}))|_w \leq |p^{1/e_p}|_w^{[\mathbb{F}_w:\mathbb{L}_{v'}](T_i-|k|)}.$$

Finalement, vu la normalisation choisie et d'après la remarque 2.1, on a $|p^{1/e_p}|w = p^{-1/e_p}$. D'autre part, par définition du groupe de décomposition, tous les facteurs de la forme $(\partial^{\boldsymbol{k}} F)^\sigma$ apparaissant dans J on la même valeur absolue par rapport à w. On en déduit immédiatement le résultat désiré.

Maintenant, on veut faire la somme sur toutes les places w au-dessus de v, mais vu que l'on a besoin de coordonnées w-entières du point $(\mathbf{F}_p(\mathbf{R}),\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R}))$ pour chaque w, on utilise l'astuce suivante de (DH00) : on note $\mathcal{S}$, $\mathcal{S}_M$, $\mathcal{S}_p$, $\mathcal{S}_{M,p}$ des coordonnées non nulles de $\mathbf{R},\mathbf{F}^{(M)}(\mathbf{R}),\mathbf{F}_p(\mathbf{R})$ et $\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})$ respectivement. Pour une place w donnée on note $\mathcal{S}_w$, $\mathcal{S}_{w,M}$, $\mathcal{S}_{w,p}$, $\mathcal{S}_{w,M,p}$ des coordonnées de ces points de valeur absolue maximale pour la place w. On peut maintenant continuer la preuve de la proposition 5.4.

Supposons $(\partial^k F)^\tau(\mathbf{F}_p(\mathbf{R}),\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R}))\neq 0$ et $|k|$ minimal avec cette propriété. On peut supposer $|k|<T_{i+1}$ sinon il n'y a rien à démontrer. On note d'abord qu'on peut écrire

$$\begin{aligned}(\partial^k F)^\tau\left(\frac{\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_p},\frac{\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{M,p}}\right) &= \frac{J^\tau\left(\mathbf{F}_p(\mathbf{R}),\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})\right)}{\mathcal{S}_p^L\mathcal{S}_{M,p}^L}\\ &= (\partial^k F)^\tau\left(\frac{\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{w,p}},\frac{\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{w,M,p}}\right)\times\frac{(\mathcal{S}_{w,p}\mathcal{S}_{w,M,p})^L}{(\mathcal{S}_p\mathcal{S}_{M,p})^L},\end{aligned}$$

et en utilisant le lemme 5.5 on a

$$\left|(\partial^k F)^\tau\left(\frac{\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_p},\frac{\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{M,p}}\right)\right|_w \leq \frac{|\mathcal{S}_{w,p}\mathcal{S}_{w,M,p}|_w^L}{|\mathcal{S}_p\mathcal{S}_{M,p}|_w^L}p^{\frac{-(T_i-|k|)}{e_p}}.$$

On est dans le cas $e_p\leq E_{g_0-i}$ donc on peut remplacer dans cette inégalité e_p par E_{g_0-i}. On fait la somme sur toutes les places de $\mathbb{F}$ au dessus de v et on obtient

$$\sum_{w|v} n_w\log\left(\left|(\partial^k F)^\tau\left(\frac{\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_p},\frac{\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{M,p}}\right)\right|_w\right)$$

où $n_w=[\mathbb{F}_w:\mathbb{Q}_w]=[\mathbb{F}_w:K_v]$. En utilisant le lemme 5.2 (on remarque qu'on a choisi pour M une puissance de 2 pour faciliter les calculs et pouvoir utiliser ce lemme) cette quantité est majorée par

$$\begin{aligned}&\leq \frac{-(T_i-|k|)\log p}{E_{g_0-i}}\left(\sum_{w|v} n_w\right)+L\sum_{w|v} n_w\log\left(\frac{|\mathcal{S}_{w,p}\mathcal{S}_{w,M,p}|_w}{|\mathcal{S}_p\mathcal{S}_{M,p}|_w}\right)\\ &\leq \frac{-(T_i-|k|)(\log p)}{E_{g_0-i}}[\mathbb{F}:K]+L[\mathbb{F}:K]h(\alpha_p(R),M(\alpha_p(R)))\\ &\leq \frac{-(T_i-|k|)(\log p)}{E_{g_0-i}}[\mathbb{F}:K]+L[\mathbb{F}:K]\left(\hat{h}(\alpha_p(R),M(\alpha_p(R)))+c_9\right)\\ &\leq \frac{-(T_i-|k|)(\log p)}{E_{g_0-i}}[\mathbb{F}:K]+L[\mathbb{F}:K]\left((M^2+1)N(\alpha_p)\hat{h}(R)+c_9\right).\end{aligned}$$

Puisque $R\in\Sigma_{g_0-i+1}$, il est de la forme $\tau_{g_0-i+1}\alpha_{g_0-i+1}\circ\ldots\circ\tau_{g_0}\alpha_{g_0}(\sigma(Q))$, donc

$$\hat{h}(R)\leq N_{g_0-i+1}\ldots N_{g_0}\hat{h}(Q).$$

On utilise le fait que $|k|<T_{i+1}\leq\frac{T_i}{2}$ (hypothèse (13)), l'hypothèse (16) et la borne pour $\hat{h}(Q)$ (hypothèse (23)) et on trouve

$$\sum_{w|v} n_w\log\left(\left|(\partial^k F)^\tau\left(\frac{\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_p},\frac{\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{M,p}}\right)\right|_w\right)\leq\frac{-c_{23}[\mathbb{F}:K]T_i\log N_{g_0-i}}{E_{g_0-i}}.$$

Notons $\zeta = (\partial^k F)^\tau \left(\frac{\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_p}, \frac{\mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R})}{\mathcal{S}_{M,p}}\right)$. Puisqu'on a supposé $\zeta \neq 0$, par les propriétés des hauteurs on a $h(\zeta) = h(\zeta^{-1})$, donc

$$\begin{aligned} h(\zeta) = h(\zeta^{-1}) &= \frac{1}{[\mathbb{F}:\mathbb{Q}]}\sum_{w\in M_{\mathbb{F}}} n_w \log\max\{1, |\zeta|_w^{-1}\} \\ &\geq \frac{1}{[\mathbb{F}:\mathbb{Q}]}\sum_{w\mid v} n_w \log\max\{1, |\zeta^{-1}|_w\} \\ &\geq \frac{c_{24}T_i \log N_{g_0-i}}{E_{g_0-i}}. \end{aligned}$$

Maintenant, par un lemme classique de hauteurs de polynômes (voir 5.4, éq. (18) (DH00)) on a

$$h\left((\partial^k F)^\tau(\mathbf{F}_p(\mathbf{R}), \mathbf{F}^{(M)}\circ\mathbf{F}_p(\mathbf{R}))\right) \quad \leq \quad c_{25}(T_{i+1}\log(T_{i+1}+L) + LM^2 N_{g_0-i}\hat{h}(R) + h(F)).$$

En mettant ensemble ces deux résultats et la borne (10) on obtient l'équation

$$\begin{aligned} \frac{c_{23}T_i \log N_{g_0-i}}{E_{g_0-i}} &\leq c_{25}(T_{i+1}\log(T_{i+1}+L) + LM^2 N_{g_0-i}\cdots N_{g_0}\hat{h}(Q)) \\ &\quad + c_{19}\left(\eta(LM^2\hat{h}(Q) + T_0\log(T_0+L) + T_0\log M + L) + \log(LM^2\deg(H))\right), \end{aligned}$$

et d'après (25)

$$\begin{aligned} \frac{c_{23}T_i \log N_{g_0-i}}{E_{g_0-i}} &\leq c_{25}(T_{i+1}\log(T_{i+1}+L) + LM^2 N_{g_0-i}\cdots N_{g_0}\hat{h}(Q)) \\ &\quad + c_{26}\left(\eta(T_0\log(T_0+L)M + L) + \log(LM^2\deg(H))\right). \end{aligned}$$

D'autre part, (13) et (23) impliquent pour C_0 assez grand

$$c_{25}(T_{i+1}\log(T_{i+1}+L) + LM^2 N_{g_0-i}\cdots N_{g_0}\hat{h}(Q)) < \frac{1}{4}\frac{c_{23}T_i\log N_{g_0-i}}{E_{g_0-i}}.$$

Finalement (24), (15) et (16) impliquent pour C_0 assez grand

$$c_{27}\left(\eta(T_0\log(T_0+L)M + L) + \log(LM^2\deg(H))\right) < \frac{1}{2}\frac{c_{23}T_i\log N_{g_0-i}}{E_{g_0-i}}$$

et en combinant ces inégalités on a bien une contradiction.

5.2 Cas très ramifié

On appliquera le raisonnement suivant lorsque parmi les ensembles $\mathcal{P}_1, \ldots, \mathcal{P}_{g_0}$ il en existe au moins un avec beaucoup de grande ramification (dans le sens de la définition 5.1).

On va suivre la preuve de la prop. 2.1 de (Amo) qui permet de simplifier, entre autres, l'application du lemme de zéros.

On rappelle que $\mathcal{H}'$ désigne l'anneau des coordonnées de $H\times H$, plongé dans un espace projectif *via* le fibré $\mathcal{M}_{|H\times H}$ et on notera pour $S \subseteq H\times H$ un sous-ensemble quelconque et pour T et L des entiers positifs,

$$H(S,T,L) := \dim_{\bar{K}}(\mathcal{H}'/\mathcal{D}^{(T)})_L,$$

où $\mathcal{D}$ est l'idéal de définition de $\bar{S}^{\mathrm{Zar}}$ et $\mathcal{D}^{(T)} = \{F\in\mathcal{H}',\ \partial^{\boldsymbol{k}}_{0,\mathrm{Id}}F \in \mathcal{D},\ \forall \boldsymbol{k},\ |\boldsymbol{k}|\leq T\}$. Voici le résultat dont on aura besoin :

Proposition 5.6. *Soit A une variété abélienne définie sur K, et $\phi_{\mathcal{L}} : A \to \mathbb{P}_n$ un plongement projectivement normal associé au fibré en droites $\mathcal{L} = \mathcal{L}_0^{\otimes 4}$. Soient $h\in\mathbb{R}_+$, $p\in\mathcal{P}$ et T, L des entiers positifs. Soit $\Sigma\subseteq A$ tel que pour tout $Q\in\Sigma$, on ait $\hat{h}(Q)\leq h$ et α_p l'endomorphisme de Frobenius associé à la place v de K ramifiée* *dans $\mathbb{L}$ telle que $v|p$. On rappelle que ι est l'application $\iota : A \to A \times A$, définie par $Q \mapsto (Q, MQ)$. On définit les ensembles*

$$S = \{\iota(Q), Q \in \Sigma\} \quad \textit{et}$$
$$S' = \bigcup_{\substack{\tau \in \mathrm{Gal}(\bar{K}/K) \\ \tau|\mathbb{L} \in G_p}} \tau(\iota(\ker(\alpha_p) + \Sigma)).$$

Soit T' un entier positif tel que $T' < T$. Alors,

$$\begin{aligned} h \quad \geq \quad & c_{28}\left(1 - \frac{H(S,T,L)}{H(S',T',L)}\right)\frac{(T-T')\log p}{pLM^2} - c_{29}\frac{\log H(S',T',L)}{2LM^2} \\ & -c_{30}\frac{T'H(S,T,L)\log(T'+L)}{H(S',T',L)LM^2} - \frac{c_{31}}{M^2}. \end{aligned}$$

Proof. Soit $\mathcal{D}$ l'idéal de définition de $\bar{S}^{\mathrm{Zar}}$ dans $\mathcal{H}'$ et $\mathcal{D}'$ l'idéal de définition de $\bar{S'}^{\mathrm{Zar}}$. Posons $l = H(S', T', L)$, $l_0 = \dim_{\bar{K}}(\mathcal{D}^{(T)})/((\mathcal{D}')^{(T')} \cap \mathcal{D}^{(T)})$. Avec les notations données, $l_0 = H(S', T', L) - H(S, T, L)$.

Considérons une base de monômes $s_1, \ldots, s_m$ de degré L du $\bar{K}$-espace vectoriel $[\mathcal{H}'/\mathcal{D}']_L$ (elle existe car le plongement projectif induit par $\mathcal{M}_{|H\times H}$ où $\mathcal{M} = \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L}$ est projectivement normal). On considère les opérateurs $\partial^{\boldsymbol{k}}_{0,\mathrm{Id}}$ définis auparavant que l'on notera $\partial^{\boldsymbol{k}}$, avec $|\boldsymbol{k}| \leq T'$. Pour un point quelconque $R \in S'$ on notera $\mathbf{R}$ des coordonnées projectives. Considérons maintenant l'application

$$\phi : F \mapsto (\partial^{\boldsymbol{k}} F(\mathbf{R}))_{|\boldsymbol{k}|\leq T', R \in S'},$$

où $F \in \mathcal{H}'$ de degré L. Le noyau de cette application est justement l'idéal $[\mathcal{D}'^{(T')}]_L$ et donc

$$\mathrm{rang}(\phi) = \dim_K \Gamma(H \times H, \mathcal{M}^{\otimes L}_{|H\times H}) - \dim_{\bar{K}}[\mathcal{D}'^{(T')}]_L = H(S', T', L).$$

On considère la matrice $\left(\partial^{\boldsymbol{k}} s_j(\mathbf{R})\right)_{\left(\substack{|\boldsymbol{k}|\leq T', R\in S' \\ j=1,\ldots,m}\right)}$; on a vu que son rang est l donc, quitte à renuméroter les indices, on peut choisir $\boldsymbol{k}_i, R_i$ et s_j avec $i, j = 1, \ldots, l$ tels que la sous-matrice

$$B = (\partial^{\boldsymbol{k}_i} s_j(\mathbf{R}_i))_{\left(\substack{1\leq i\leq l \\ 1\leq j\leq l}\right)}$$

soit de déterminant non nul. D'après les définitions, il y a l_0 polynômes $G_1, \ldots, G_{l_0}$ linéairement indépendants, non identiquement nuls sur S' à l'ordre T', nuls sur S à l'ordre T. On considère maintenant les polynômes $\partial^{\boldsymbol{k}_i} G_r$, pour $r = 1, \ldots, l_0$. D'après les choix faits, $\partial^{\boldsymbol{k}_i} G_r$ est non identiquement nul sur S' à l'ordre $T' - |\boldsymbol{k}_i|$ et nul sur S à l'ordre $T - |\boldsymbol{k}_i|$ pour tout r et on peut supposer qu'il s'écrit sous la forme

$$\partial^{\boldsymbol{k}_i} G_r = \sum_{j=1}^{l} g_{rj} \partial^{\boldsymbol{k}_i} s_j$$

pour $g_{rj} \in \bar{K}$. De plus, on peut choisir une extension de K assez grande, une place $w|v$, renuméroter les indices et faire des combinaisons linéaires de façon qu'on puisse écrire

$$\partial^{\boldsymbol{k}_i} G_r = \textstyle\sum_{j=1}^{l-r+1} g_{rj} \partial^{\boldsymbol{k}_i} s_j \qquad \text{où} \qquad \begin{cases} |g_{rj}|_w = 1, \ j = l-r+1; \\ |g_{rj}|_w \leq 1, \ j = 1\ldots, l-r. \end{cases}$$

D'après les remarques antérieures, on peut remplacer les dernières l_0 colonnes de B par

$$\begin{pmatrix} \partial^{\boldsymbol{k}_1} G_{l_0}(\mathbf{R}_1) & \ldots & \partial^{\boldsymbol{k}_1} G_1(\mathbf{R}_1) \\ \vdots & & \vdots \\ \partial^{\boldsymbol{k}_l} G_{l_0}(\mathbf{R}_l) & \ldots & \partial^{\boldsymbol{k}_l} G_1(\mathbf{R}_l) \end{pmatrix}$$

pour obtenir une nouvelle matrice $B(w)$. On vérifie facilement qu'on peut écrire

$$B(w) = B \times \begin{pmatrix} 1 & 0 & \cdots & 0 & g_{l_0,1} & & g_{11} \\ 0 & 1 & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \ddots & 1 & g_{l_0,l-l_0} & & \vdots \\ 0 & & & 0 & \boxed{g_{l_0,l-l_0+1}} & & \\ \vdots & & & & \vdots & \ddots & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \boxed{g_{1,l}} \end{pmatrix}$$

et donc
$$|\det(B(w))|_w = |g_{l_0,l-l_0+1}\cdots g_{1,l}|_w|\det(B)|_w = |\det(B)|_w.$$
Maintenant, on va calculer $|\det(B(w))|_w$ et pour cela on va d'abord borner $|\partial^{\boldsymbol{k}} G_r(\mathbf{R})|_w$. On rappelle que R_i est de la forme $\tau_i((\xi_i+Q_i), M(\xi_i+Q_i))$ où $\xi_i \in \ker(\alpha_p)$, $Q_i \in \Sigma$ et G_k est un polynôme à coefficients dans $\bar{K}$ nul en (Q_i, MQ_i) et ses conjugués sur $\mathbb{L}$ à l'ordre T. On se place sur une carte affine et on note $T_{\xi,0},\ldots,T_{\xi,n}$ des formes représentant la translation par ξ.

Comme dans le cas peu ramifié, pour utiliser les propriétés du groupe G_p il faudra travailler avec des polynômes à coefficients entiers dans $\mathbb{L}$. Plus précisement, on va travailler sur $\mathbb{L}_{v'}$ où v' est une place de $\mathbb{L}$ au-dessus de $v|p$ puisque la congruence du lemme 2.16 est encore vraie pour les entiers de $\mathbb{L}_{v'}$. On utilise la même astuce que précédemment : soit $\mathbb{F}$ une extension de K contenant les coefficients de $\partial^{\boldsymbol{k}} G_r$, w une place de $\mathbb{F}$ au-dessus de $v' \in M_{\mathbb{L}}$, telle que $w|v'$. On définit le polynôme
$$J = \prod_{\sigma\in D_w} (\partial^{\boldsymbol{k}} G_r)^\sigma$$
où D_w est le groupe de décomposition de $\mathrm{Gal}(\mathbb{F}/\mathbb{L})$ en w. Puisque $D_w \simeq \mathrm{Gal}(\mathbb{F}_w/\mathbb{L}_{v'})$, J est un polynôme à coefficients dans $\mathbb{L}_{v'}$, nul sur S à l'ordre $(T-|\boldsymbol{k}|)[\mathbb{F}_w:\mathbb{L}_{v'}]$.

Lemme 5.7. *Soit $Q\in S$. Si on choisit des coordonnées w-entières de $(\xi+Q, M(\xi+Q))$, alors*
$$|J^\tau(\mathbf{T}_\xi(\mathbf{Q}), \mathbf{F}^{(M)}\circ\mathbf{T}_\xi(\mathbf{Q})|_w \le p^{\frac{-(T-|k|)[\mathbb{F}_w:\mathbb{L}_{v'}]}{p}}$$
pour tout $\tau\in\mathrm{Gal}(\bar{K}/K)$ tel que $\tau_{|\mathbb{L}}\in G_p$.

Proof. D'après le théorème 5.3, il existe $\beta=(1,\beta_1,\ldots,\beta_s)$ où les β_i sont des éléments de $\mathcal{O}_w$ tels que J s'écrit sous la forme
$$J(X_0,\ldots,X_n,F_0^{(M)}(\mathbf{X}),\ldots,F_n^{(M)}(\mathbf{X})) = \sum_l \prod_{j=1}^{(T-|\boldsymbol{k}|)[\mathbb{F}_w:\mathbb{L}_{v'}]} h_{l_j}(\mathbf{X},\mathbf{Y}) \tag{28}$$
avec h_{l_j} des polynômes à coefficients dans $\mathcal{O}_{v'}$ l'anneau des entiers du complété $\mathbb{L}_{v'}$ nuls en $(Q+\xi,\beta)$. Notons $h=h_{l_j}$ un de ces polynômes. On va montrer dans un premier temps
$$\left|h^\tau(\mathbf{T}_\xi(\mathbf{Q}), \mathbf{F}^{(M)}\circ\mathbf{T}_\xi(\mathbf{Q}))\right|_w \le p^{1/p}.$$
Puisque $h[\mathbf{X},\mathbf{Y}]\in\mathcal{O}_{v'}[\mathbf{X},\mathbf{Y}]$ on peut appliquer la congruence du lemme 2.16 et on obtient
$$|h(\mathbf{X},\mathbf{Y}) - h^\tau(\mathbf{X},\mathbf{Y})|_w \le p^{-1/p}$$
(on prolonge de façon canonique w dans le corps $\bar{K}(\mathbf{X},\mathbf{Y})$ en posant $|X_i|_w = |Y_j|_w = 1$ pour tout i,j). On a donc
$$|h^\tau(\mathbf{T}_\xi(\mathbf{Q}),\beta) - h(\mathbf{T}_\xi(\mathbf{Q}),\beta)|_w \le p^{-1/p}. \tag{29}$$
On note comme précédemment $F_{p,0}(\mathbf{X}),\ldots,F_{p,n}(\mathbf{X})$ des coordonnées de $\mathbf{F}_p(\mathbf{X})$. Par définition du Frobenius, on sait que pour tout $\mathbf{X}$ on a
$$X_j^pF_{p,i}(\mathbf{X}) - F_{p,j}(\mathbf{X})X_i^p \in \pi_v\mathcal{O}_K[\mathbf{X}],\ \ \forall i,j \quad 0\le i,j\le n$$
et puisque $\xi\in\ker(\alpha_p)$, on a $\mathbf{F}_p\circ\mathbf{T}_\xi(\mathbf{X}) = \mathbf{F}_p(\mathbf{X})$. Donc au niveau des coordonnées on a
$$T_{\xi,i}(\mathbf{X})^pX_j^p - X_i^pT_{\xi,j}(\mathbf{X})^p \ \in\ \pi_v\mathcal{O}_K[\mathbf{X}]$$
et en utilisant le petit théorème de Fermat on a
$$(T_{\xi,i}(\mathbf{X})X_j - X_iT_{\xi,j}(\mathbf{X}))^p \ \in\ \pi_v\mathcal{O}_K[\mathbf{X}].$$
On note d le degré de $h:=h_{l_j}$ par rapport au premier groupe de variables et par homogénéité on a
$$\left(X_j^dh(\mathbf{T}_\xi(\mathbf{X}),\mathbf{Y}) - T_{\xi,j}(\mathbf{X})^dh(\mathbf{X},\mathbf{Y})\right)^p \in\ \pi_{v'}\mathcal{O}_{v'}[\mathbf{X},\mathbf{Y}].$$
On évalue en $(Q+\xi,\beta)$ et on a $|h(\mathbf{T}_\xi(\mathbf{Q}),\beta)|_w \le p^{-1/p}$ puis en utilisant (29) on trouve
$$|h^\tau(\mathbf{T}_\xi(\mathbf{Q}),\beta)|_w \le p^{-1/p}.$$
En reportant cette inégalité dans (28) et en évaluant en $(Q+\xi,\beta)$ on a
$$\left|J^\tau(\mathbf{T}_\xi(\mathbf{Q}), \mathbf{F}^{(M)}\circ\mathbf{T}_\xi(\mathbf{Q}))\right|_w \le p^{\frac{-(T-|\boldsymbol{k}|)[\mathbb{F}_w:\mathbb{L}_{v'}]}{p}}.$$

Corollaire 5.8. *Avec les mêmes notations que ci-dessus, pour tout point $R \in S'$ on a*

$$|\partial^{\boldsymbol{k}} G_r(\mathbf{R})|_w \le p^{\frac{-(T-|\boldsymbol{k}|)}{p}}.$$

Proof. Puisque $|J|_w = |\prod_{\sigma\in D_w}(\partial^{\boldsymbol{k}} G_r)^\sigma|_w$, par définition de D_w la norme de tous les conjugués dans ce produit est la même et il y en a $[\mathbb{F}_w : \mathbb{L}_{v'}]$. En utilisant le lemme précédant on a le résultat désiré.

Continuons la preuve de 5.6. Comme on a l'a fait dans le cas peu ramifié, pour pouvoir mettre toutes les places w ensemble, on va choisir des coordonnées w-entières : on note $\mathcal{S}_i$ et $\mathcal{S}_{i,M}$ des coordonnées non nulles de $\mathbf{T}_{\xi_i}(\mathbf{Q}_i)$ et $\mathbf{F}^{(M)} \circ \mathbf{T}_{\xi_i}(\mathbf{Q}_i)$ respectivement. Pour une place w donnée on note $\mathcal{S}_{i,w}, \mathcal{S}_{i,w,M}$ des coordonnées de ces points de valeur absolue maximale pour la place w. Alors

$$\begin{aligned}\left|(\partial^{\boldsymbol{k}} G_r)^\tau\left(\frac{\mathbf{T}_{\xi_i}(\mathbf{Q}_i)}{\mathcal{S}_i}, \frac{\mathbf{F}^{(M)} \circ \mathbf{T}_{\xi_i}(\mathbf{Q}_i)}{\mathcal{S}_{i,M}}\right)\right|_w &= \left|(\partial^{\boldsymbol{k}} G_r)^\tau\left(\frac{\mathbf{T}_{\xi_i}(\mathbf{Q}_i)}{\mathcal{S}_{i,w}}, \frac{\mathbf{F}^{(M)} \circ \mathbf{T}_{\xi}(\mathbf{Q}_i)}{\mathcal{S}_{i,M,w}}\right)\left(\frac{\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}}{\mathcal{S}_i\mathcal{S}_{i,M}}\right)^{L[\mathbb{F}:\mathbb{L}]}\right|_w \\ &\le p^{\frac{-(T-T')[\mathbb{F}:\mathbb{L}]}{p}} \frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{L[\mathbb{F}:\mathbb{L}]}}{|\mathcal{S}_i\, \mathcal{S}_{i,M}|_w^{L[\mathbb{F}:\mathbb{L}]}}.\end{aligned}$$

Maintenant, on calcule le déterminant de $B(w)$ en développant à partir de la dernière colonne. On obtient

$$\begin{aligned}|\det(B(w))|_w &\le \max_{1\le i_1,\dots i_{l_0}\le l}\left|\partial^{k_{i_1}} G_1(\mathbf{R}_{i_1})\cdots\partial^{k_{i_{l_0}}} G_{l_0}(\mathbf{R}_{i_{l_0}})\right| \\ &\quad\times \max_{1\le i_1,\dots,i_{l-l_0}\le l}\left|\partial^{k_{i_1}} s_{l-l_0}(\mathbf{R}_{i_1})\cdots\partial^{k_{i_{l-l_0}}} s_1(\mathbf{R}_{i_{l-l_0}})\right|_w \\ &\le \max_{\substack{1\le i\le l\\1\le j\le l_0}}\left|\partial^{k_i} G_j(\mathbf{R}_i)\right|_w^{l_0} \max_{\substack{1\le i\le l\\1\le j\le l_0}}\left|\partial^{k_i} s_j(\mathbf{R}_i)\right|_w^{l-l_0} \\ &\le p^{-(T-T')l_0/p}\max_{1\le i\le l}\frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{Ll_0}}{|\mathcal{S}_i\mathcal{S}_{i,M}|_w^{Ll_0}}\max_{1\le i\le l}\frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{L(l-l_0)}}{|\mathcal{S}_i\mathcal{S}_{i,M}|_w^{L(l-l_0)}} \\ &\le p^{-(T-T')l_0/p}\max_{1\le i\le l}\frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{Ll}}{|\mathcal{S}_i\mathcal{S}_{i,M}|_w^{Ll}}.\end{aligned}$$

Soit maintenant w une place finie qui ne divise pas v. En utilisant l'inégalité ultramétrique on a la majoration

$$\begin{aligned}|\det(B)|_w &\le \max_{1\le i,j\le l}|\partial^{k_i} s_j(\mathbf{R}_i)|_w^l \\ &\le \max_{1\le i\le l}\frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{Ll}}{|\mathcal{S}_i\mathcal{S}_{i,M}|_w^{Ll}}.\end{aligned}$$

Finalement, pour une place w archimédienne, l'inégalité de Hadamard nous dit que

$$\begin{aligned}|\det(B)|_w &\le \prod_{j=1}^{l}\left(\sum_{j=1}^{l}|\partial^{k_i} s_j(\mathbf{R}_i)|_w^2\right)^{\frac{1}{2}} \\ &\le \max_{1\le i\le l}\frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{Ll}}{|\mathcal{S}_i\mathcal{S}_{i,M}|_w^{Ll}}\left(l\max_{1\le i,j\le l}|\partial^{k_i} s_j(\mathbf{R}_i)|_w^2\right)^{\frac{l}{2}} \\ &\le \max_{1\le i\le l}\frac{|\mathcal{S}_{i,w}\mathcal{S}_{i,M,w}|_w^{Ll}}{|\mathcal{S}_i\mathcal{S}_{i,M}|_w^{Ll}} l^{\frac{l}{2}}\max_{1\le i,j\le l}|\partial^{k_i} s_j(\mathbf{R}_i)|_w^l\end{aligned}$$

Vu que $\det B \ne 0$, on applique la formule du produit ($\frac{1}{[\mathbb{F}:\mathbb{Q}]}\sum_w n_w \log|\det(B)|_w = 0$) et on a

$$\begin{aligned}0 &\le -c_{32}\frac{(T-T')l_0\log p}{p} + \frac{l}{2}\log l + Llh(R) + c_{33}l(T'\log(T'+L)+T') \\ &\le -c_{32}\frac{(T-T')l_0\log p}{p} + \frac{l}{2}\log l + c_{34}lT'\log(T'+L) + c_{35}LM^2lh + c_{36}Ll\end{aligned}$$

d'où

$$h \ge c_{37}\frac{(T-T')l_0\log p}{LM^2lp} - c_{38}\frac{T'\log(T'+L)}{LM^2} - c_{39}\frac{\log l}{LM^2} - \frac{c_{40}}{M^2}.$$

Lemme 5.9. *Soit $r(\mathcal{P})$ l'indice fixé auparavant tel que l'ensemble $\mathcal{P}_{r(\mathcal{P})}$ est très ramifié. Alors si on utilise les paramètres $T_0, T_1, L, N_{r(\mathcal{P})}$ et $E_{r(\mathcal{P})}$ fixés pour le cas très ramifié et $\Sigma = \{\sigma(Q), \sigma \in \mathrm{Gal}(\bar{K}/\mathbb{L})\}$, alors $H(S', T_1, L) < 2H(S, T_0, L)$.*

Proof. On applique la proposition 5.6 à l'ensemble Σ avec $T = T_0$, $T' = T_1$ et $L = L$. Pour tout $Q \in \Sigma$ l'hypothèse (26) nous dit que $\hat{h}(Q) \leq h$ avec

$$h = \frac{T_0 \log(N_{r(\mathcal{P})})}{\log(C_0) N_{r(\mathcal{P})} L M^2}.$$

On obtient l'inégalité

$$\begin{aligned} h \quad \geq \quad & c_{41} \left(1 - \frac{H(S, T_0, L)}{H(S', T_1, L)}\right) \frac{(T_0 - T_1) \log(N_{r(\mathcal{P})})}{N_{r(\mathcal{P})} L M^2} - c_{42} \frac{\log H(S', T_1, L)}{L M^2} \\ & - c_{43} \frac{T_1 \log(T_1 + L)}{L M^2} - \frac{c_{44}}{M^2}. \end{aligned}$$

Si $H(S', T_1, L) \geq 2H(S, T_0, L)$, en utilisant le fait que $T_1 \leq \frac{T_0}{2}$ (hypothèse (20)) et une borne très générale pour $H(S', T_1, L)$ (par exemple on prend $H(S', T_1, L) \leq H(H \times H, L) \leq L^{2g_0} \deg(H)^2$) on a

$$h \geq c_{45} \frac{T_0 \log(N_{r(\mathcal{P})})}{N_{r(\mathcal{P})} L M^2} - c_{46} \frac{\log(L \deg H)}{L M^2} - c_{47} \frac{T_1 \log(T_1 + L)}{L M^2} - \frac{c_{48}}{M^2}.$$

Finalement en utilisant les hypothèses (19), (20) et (21) pour C_0 assez grand on a

$$h \geq \frac{c_{49} T_0 \log(N_{r(\mathcal{P})})}{N_{r(\mathcal{P})} L M^2}.$$

On remplace h par sa valeur et on trouve

$$\frac{T_0 \log(N_{r(\mathcal{P})})}{\log(C_0) N_{r(\mathcal{P})} L M^2} \geq c_{49} \frac{T_0 \log(N_{r(\mathcal{P})})}{N_{r(\mathcal{P})} L M^2},$$

ce qui est contradictoire pour C_0 assez grand.

Voyons maintenant que $H(S, T_0, L) \leq \frac{1}{2} \dim_{\bar{K}} \Gamma(\iota(H), \mathcal{M}^{\otimes L})$. Soit Z la sous-variété fixée satisfaisant $\omega_{\mathbb{L}}(Q, H) = \left(\frac{\deg Z}{\deg H}\right)^{1/\mathrm{codim}_H Z}$. Par définition, $\Sigma \subseteq Z$ et donc $S \subseteq \iota(Z)$. Si on note comme avant $\mathcal{D}$ l'idéal de définition de $\iota(Z)$, on voit facilement que

$$\begin{aligned} H(S, T_0, L) \quad & \leq \quad \dim_{\mathbb{C}}(\mathcal{H}' / t^*_{\iota(v)}(\mathcal{D})^{(T_0)})_L \\ & \leq \quad c_{50} T_0^{g_0 - d} (L M^2)^d \deg(Z) \\ & \leq \quad c_{50} T_0^{g_0 - d} (L M^2)^d \omega_{\mathbb{L}}(Q, H)^{g_0 - d} \deg H. \end{aligned}$$

D'autre part on sait que $\dim_{\bar{K}} \Gamma(\iota(H), \mathcal{M}^{\otimes L}) \geq c_{51} (L M^2)^{g_0} \deg(H)$ quitte à ce que (17) soit vérifiée. On a finalement

$$\begin{aligned} H(S, T_0, L) \quad & \leq \quad c_{50} T_0^{g_0 - d} (L M^2)^d \omega_{\mathbb{L}}(Q, H)^{g_0 - d} \deg H \\ & \leq \quad \frac{c_{51}}{2} (L M^2)^{g_0} \deg(H) \quad \text{grâce à l'hypothèse (18) pour } C_0 \text{ assez grand} \\ & \leq \quad \frac{1}{2} \dim_{\bar{K}} \Gamma(\iota(H), \mathcal{M}^{\otimes L}). \end{aligned}$$

Il existe donc un polynôme F de degré L non identiquement nul sur $\iota(H)$, nul sur S' à l'ordre T_0'.

On recapitule dans la proposition qui suit le résultat démontré dont on aura besoin :

Proposition 5.10. *Soit i un indice tel que $1 \leq i \leq g_0$, N_i, L, M, T_0, T_1 des entiers vérifiant les conditions (17) à (22) (début du paragraphe 5) et $Q \in H(\bar{K})$ d'ordre infini modulo toute sous-variété abélienne propre de H vérifiant (26). Soit $v \in M_K$ une place ramifiée dans $\mathbb{L}$ au-dessus de $p \in \mathcal{P}_i$. Soit α_p un endomorphisme de Frobenius en v (on rappelle que $\frac{N_i}{2} \leq N(v) \leq N_i$) et Σ l'ensemble de conjugués du point Q sur $\mathbb{L}$. Alors il existe un polynôme F bihomogène à coefficients dans $\bar{K}$ de bidegré (L, L) nul sur l'ensemble*

$$\bigcup_{\substack{\tau \in \mathrm{Gal}(\bar{K}/K) \\ \tau | \mathbb{L} \in G_p}} \tau(\iota(\ker(\alpha_p) + \Sigma))$$

à l'ordre T_1 le long de $T_{\iota(H)(\mathbb{C})}$.

6 Lemme de zéros

Dans cette partie on applique un lemme de zéros aux fonctions construites auparavant. Il s'agit d'une variante du lemme de zéros de (DH00) théo. 4.1. Comme dans la preuve du problème de Lehmer classique "à ϵ-près", le lemme de zéros ne suffit pas pour conclure et il faut faire une descente. Celle-ci est encore proche de celle de (DH00) mais en plus de tenir compte des deux cas traités plus haut (peu et très ramifié) elle fait intervenir un nouvel ingrédient : une suite de corps emboîtés qui permettent de capturer plus d'information. Contrairement au cas classique déjà mentionné, ceci ne suffit pas pour démontrer le théorème principal ; il faudra en dernier lieu procéder à une récurrence sur la dimension de la variété H en question.

On commence par donner une définition.

Définition 6.1. *Soit V une sous-variété de A et $\mathcal{V}$ un sous-espace vectoriel de $T_{A(\mathbb{C})}$. Soient T et L deux entiers positifs. On dit que V est définie incomplètement dans A avec multiplicité $\geq T$ le long de $\mathcal{V}$ par des formes de degré au plus L, s'il existe des formes $q_1, \ldots, q_s$ de degré $\leq L$ telles que V soit une composante irréductible du lieu des zéros de l'idéal $(q_1, \ldots, q_s)$ et chaque forme q_i, $i = 1, \ldots, s$, s'annule à un ordre $\geq T$ sur V le long de $\mathcal{V}$.*

6.1 Cas peu ramifié

Supposons d'abord qu'on dispose de g_0 ensembles d'isogénies $\mathcal{P}_1, \ldots, \mathcal{P}_{g_0}$ avec peu de grande ramification. On utilise le lemme de zéros de (DH00), théorème 4.1 en faisant quelques modifications pour tenir compte des conjugués et avoir des résultats en fonction de $\omega_{\mathbb{L}}$ et $\deg(H)$. Pour un premier $p \in \mathcal{P}$, notons

$$S_p = \{\tau \in \mathrm{Gal}(\bar{K}/K), \tau_{|\mathbb{L}} = \phi_p\}.$$

On rappelle les notations suivantes :

$$\Sigma = \{\sigma(Q), \sigma \in \mathrm{Gal}(\bar{K}/\mathbb{L})\} \text{ et}$$
$$\Sigma_i = \{\tau_i\alpha_i \circ \ldots \circ \tau_{g_0}\alpha_{g_0}(R), R \in \Sigma\} \text{ pour } i = 1, \ldots, g_0$$

où α_i parcourt $\Delta_i^{(\mathrm{pr})}$ et τ_i parcourt S_p si $\alpha_i = \alpha_p \neq \mathrm{Id}$ ou $\tau_i \in \mathrm{Gal}(\bar{K}/K)$ tel que $\tau_{|\mathbb{L}} = \mathrm{Id}$ lorsque $\alpha_i = \mathrm{Id}$.

Théorème 6.2. *Soient A une variété abélienne plongée dans un espace projectif $\mathbb{P}^n$ de façon projectivement normale, B une sous-variété abélienne de A de dimension g_0, $Q \in B(\bar{K})$ et des ensembles Σ_i pour $i = 1, \ldots, g_0$ comme ci-dessus. Soit $F \in \mathbb{L}[X_0, \ldots, X_n]$ une forme homogène de degré ν non identiquement nulle sur B, nulle à un ordre supérieur à $T_1' + \ldots + T_{g_0}'$ pour T_i' des entiers positifs, le long de $T_{B(\mathbb{C})}$ en tous les points de Σ_1. Alors il existe un entier k, $1 \leq k \leq g_0$, une sous-variété propre V de B, géométriquement irréductible incomplètement définie dans B par des formes de degré $\leq 2N_1 \cdots N_{k-1}\nu$ avec multiplicité $\geq T_k'$ le long de $T_{B(\mathbb{C})}$, de dimension $d \geq g_0 - k$, contenant une composante irréductible de Σ_{k+1}, telle que*

$$T_k'^{g_0-d} \deg\left(\bigcup_{\alpha_p \in \Delta_k^{(\mathrm{pr})}, \tau \in S_p} \tau \circ \alpha_p(V)\right) \leq c_{52}(\deg B)(\nu N_1 \ldots N_{k-1})^{g_0-d}$$

Proof. C'est le théorème 4.1 (avec supplément galoisien) et la scolie 4.8 de (DH00) où l'on a utilisé les idéaux $\mathcal{J}_1 = (F)$, $\mathcal{J}_{i+1} = (\partial_{0,\alpha_p}^{T_i'}\tau\mathcal{J}_i \,; \alpha_p \in \Delta_i^{(\mathrm{pr})}, \tau \in S_p)$.

On applique le théorème 6.2 à la trace sur $\mathbb{L}$ de la fonction F construite dans le lemme 4.5 tirée en arrière par la fonction $\iota : A \hookrightarrow A \times A$. Par construction, F n'est pas identiquement nulle sur $\iota(H)$ de bidegré (L, L). On sait de plus que F est nulle en tous les points de $\iota(\Sigma_1)$ à l'ordre T_{g_0} le long de $T_{\iota(H)(\mathbb{C})}$, donc la fonction $G = \mathrm{Tr}_{\bar{K}/\mathbb{L}}(F \circ \iota)$, de degré $L(M^2+1)[\mathbb{F} : \mathbb{L}]$ (où $\mathbb{F}$ est le corps de défintion de F) vérifie les hypothèses du lemme de zéros avec $T_i' = \left[\frac{T_{g_0}}{g_0+1}\right][\mathbb{F} : \mathbb{L}]$ et $\nu = L(M^2+1)[\mathbb{F} : \mathbb{L}]$. On obtient donc un entier k, $1 \leq k \leq g_0$, une sous-variété V de H, géométriquement irréductible, incomplètement définie avec multiplicité $\geq T_k$ le long de $T_{H(\mathbb{C})}$ par des formes de degré au plus $2[\mathbb{F} : \mathbb{L}]LM^2N_1 \cdots N_k$, de dimension $d \geq g_0 - k$ contenant un point Q_1 de la forme $\tau_{k+1}\alpha_{k+1} \circ \ldots \circ \tau_{g_0}\alpha_{g_0}(\sigma(Q))$ telle que

$$(T_{g_0}[\mathbb{F} : \mathbb{L}])^{g_0-d} \deg\left(\bigcup_{\alpha_p \in \Delta_k^{(\mathrm{pr})}, \tau \in S_p} \tau \circ \alpha_p(V)\right) \leq c_{53} \deg(H)([\mathbb{F} : \mathbb{L}]LM^2N_1 \ldots N_{k-1})^{g_0-d}$$

et donc

$$T_{g_0}^{g_0-d}\deg\left(\bigcup_{\alpha_p\in\Delta_k^{(\mathrm{pr})},\tau\in S_p}\tau\circ\alpha_p(V)\right) \leq c_{53}\deg(H)(LM^2N_1\ldots N_{k-1})^{g_0-d} \tag{30}$$

On veut estimer le mieux possible le degré de la partie gauche de cette inéquation et, pour cela, compter combien de conjugués différents des $\alpha_p(V)$ on a. Par le point (i) du lemme 2.18, on sait que si α_1,α_2 sont deux isogénies distinctes de $\mathcal{P}_k$, alors on ne peut pas avoir $\alpha_1(\tau_1(V))=\alpha_2(\tau_2(V))$ pour n'importe quels $\tau_1,\tau_2\in\mathrm{Gal}(\bar{K}/K)$ à moins que V soit une sous-variété de torsion. Mais $V\subsetneq H$, elle contient Q_1 et par définition la plus petite sous-variété de torsion contenant ce point-là est bien entendu H.

D'autre part, si on note $V_{\mathbb{L}}=\bigcup_{\tau\in\mathrm{Gal}(\bar{K}/\mathbb{L})}\tau(V)$, on a

$$\deg\left(\bigcup_{\tau\in S_p}\tau(V)\right)=\deg(\phi_p(V_{\mathbb{L}}))=\deg(V_{\mathbb{L}}).$$

En utilisant 2.12.*(iii)* et puisque $\alpha_j(\phi_{p_j}V_{\mathbb{L}})\neq\alpha_l(\phi_{p_l}V_{\mathbb{L}})$ pour tout $j\neq l$, alors on peut écrire

$$\deg\left(\bigcup_{\alpha_p\in\Delta_k^{(\mathrm{pr})},\tau\in S_p}\alpha_p(\tau(V))\right)=\deg(V_{\mathbb{L}})\sum_{\alpha_p\in\Delta_k^{(\mathrm{pr})}}\frac{N(\alpha_p)^d}{|\ker(\alpha_p)\cap G_{V_{\mathbb{L}}}|},$$

et en utilisant l'inégalité arithmético-géométrique on a

$$\begin{aligned}\deg\left(\bigcup_{\alpha_p\in\Delta_k^{(\mathrm{pr})},\tau\in S_p}\alpha_p(\tau(V))\right) &\geq \frac{c_{54}\deg(V_{\mathbb{L}})N_k^d|\Delta_k^{(\mathrm{pr})}|}{\sqrt[|\Delta_k^{(\mathrm{pr})}|]{\prod_{\alpha_p}|\ker(\alpha_p)\cap G_{V_{\mathbb{L}}}|}}\\ &\geq \frac{c_{55}\deg(V_{\mathbb{L}})N_k^d|\Delta_k^{(\mathrm{pr})}|}{\sqrt[|\Delta_k^{(\mathrm{pr})}|]{\left|\ker\left(\prod_{\alpha_p\in\Delta_k^{(\mathrm{pr})}}\alpha_p\right)\cap G_{V_{\mathbb{L}}}\right|}},\end{aligned}$$

puisque les α_p sont tous premiers entre eux. Voyons maintenant que

$$|\Delta_k^{(\mathrm{pr})}|\geq\frac{c_{56}N_k}{\log N_k}.$$

D'après la proposition 2.9 A possède un endomorphisme de Frobenius en presque toute place finie de K. On rappelle qu'on a choisi une seule place v au-dessus de chaque premier p et donc tous les α_p sont premiers entre eux. En utilisant le théorème de Čebotarev on a que $|\mathcal{P}_k|\geq c_{57}\frac{N_k}{\log N_k}$ et donc pour C_0 assez grand

$$|\Delta_k^{(\mathrm{pr})}|\geq\frac{|\mathcal{P}_k|}{2}\geq c_{58}\frac{N_k}{\log N_k}.$$

Notons $s=\dim(G_{V_{\mathbb{L}}})$ et rappelons que V est définie incomplètement par des équations de degré $\leq c_{59}LM^2N_1\cdots N_{k-1}$. En utilisant le lemme 2.3, le lemme 2.13 et une borne très générale obtenue par le lemme de zéros pour $\deg(V_{\mathbb{L}})$ (on prend ici $\deg(V_{\mathbb{L}})\leq c_{60}\deg(H)(LM^2)^{g_0-d}N_1\cdots N_{k-1}$ en prenant $\alpha_p=\mathrm{Id}$), on obtient pour une isogénie admissible quelconque β de poids $q(\beta)$

$$\begin{aligned}\mathrm{Card}(\ker(\beta)\cap G_{V_{\mathbb{L}}}) &\leq |G_{V_{\mathbb{L}}}:G_{V_{\mathbb{L}}}^{\circ}|q(\beta)^s\\ &\leq q(\beta)^s\deg(G_{V_{\mathbb{L}}})\\ &\leq q(\beta)^s\deg(V_{\mathbb{L}})(4LM^2N_1\cdots N_{k-1})^{d-s}\\ &\leq c_{61}q(\beta)^s(LM^2N_1\cdots N_{k-1})^{g_0-s}\deg(H).\end{aligned}$$

En mettant ensemble ces inégalités et la borne pour $|\Delta_k^{(\mathrm{pr})}|$, on a

$$\deg\left(\bigcup_{\alpha_p\in\Delta_k^{(\mathrm{pr})},\tau\in S_p}\alpha_p(\tau(V))\right)\geq c_{62}\frac{\deg(V_{\mathbb{L}})N_k^{d-s+1}}{\log(N_k)\sqrt[\mathrm{Card}\Delta_k^{(\mathrm{pr})}]{(LM^2N_1\cdots N_{k-1})^{g_0-s}\deg H}}.$$

D'après (30), l'hypothèse (14), la minoration de $|\Delta_k^{(\mathrm{pr})}|$ ci-dessus et puisque $d \geq s$ on a

$$\deg(H)(LM^2N_1 \ldots N_{k-1})^{g_0-d} \geq \frac{c_{63}N_k \deg(V_{\mathbb{L}})T_{g_0}^{g_0-d}}{\log(N_k)}$$

et alors

$$\deg(V_{\mathbb{L}}) \quad \leq \quad c_{64}\frac{(LM^2N_1 \ldots N_{k-1})^{g_0-d} \deg(H) \log(N_k)}{(T_{g_0})^{g_0-d}N_k}. \tag{31}$$

Remarque 6.3. *Dans l'application du lemme de zéros on aurait pu considérer des ensembles Σ_i plus petits en remplaçant dans leur définition l'ensemble $\Delta_i^{(\mathrm{pr})}$ par un sous-ensemble de celui-ci. Pour obtenir le même résultat final (borne (31)) il suffit d'assurer qu'il s'agit d'un ensemble de cardinal $\geq c_{65}\frac{N_i}{\log N_i}$.*

On peut résumer ces résultats dans le corollaire suivant :

Corollaire 6.4. *Soit Q un point de $H(\bar{K})$ satisfaisant l'hypothèse (23), d'ordre infini modulo toute sous-variété de torsion de H. Alors il existe un entier k, $1 \leq k \leq g_0$, un point $Q_1 = \tau_{k+1}\alpha_{k+1} \circ \ldots \circ \tau_{g_0}\alpha_{g_0}(Q)$ pour certains $\alpha_i \in \mathcal{P}_i$, $\tau_i \in S_p$ où p est tel que $\alpha_i = \alpha_p$ et une sous-variété propre de H, V définie sur $\mathbb{L}$ contenant le point Q_1, de dimension d, où $d \geq g_0 - k$ et dont le degré satisfait l'inégalité :*

$$\deg V \leq c_{64}\frac{(LM^2N_1 \ldots N_{k-1})^{g_0-d} \deg(H) \log(N_k)}{T_{g_0}^{g_0-d}N_k}.$$

De plus, V est définie incomplètement par des formes de degré $\leq c_{66}LM^2N_1 \cdots N_{k-1}$ le long de $T_{H(\mathbb{C})}$ avec multiplicité au moins $\frac{T_{g_0}}{g_0+1}$.

6.2 Cas très ramifié

On se replace dans le cas où il existe un ensemble $\mathcal{P}_{r(i)}$ avec beaucoup de grande ramification et soit $\alpha_p \in \Delta_{r(i)}^{(\mathrm{tr})}$. On choisit des paramètres T_0, T_1, L, M satisfaisant les conditions (17) à (22) et on suppose de plus que la condition (26) est satisfaite. D'après la proposition 5.10 il existe un polynôme $F \in \bar{K}[\mathbf{X}]$ nul en $\iota(\tau(R+U))$ à l'ordre T_1 pour tout $U \in \ker(\alpha_p)$, $\tau \in \mathrm{Gal}(\bar{K}/K)$ tel que $\tau_{|\mathbb{L}} \in G_p$, et pour tout R conjugué de Q sur $\mathbb{L}$.

On rappelle qu'il existe m minimal tel que $\mathbb{L} \subseteq \mathbb{Q}_p(\zeta_m)$ (voir paragraphe 2.5). On définit le sous-corps $\mathbb{L}_1$ de $\mathbb{L}$ comme l'intersection

$$\mathbb{L} \cap \mathbb{Q}_p(\zeta_{m/p}).$$

Avec cette notation on remarque que $G_p = \mathrm{Gal}(\mathbb{L}/\mathbb{L}_1)$.

Lemme 6.5. *Il existe une variété $V_{\mathbb{L}_1}$ de dimension d_1 définie sur $\mathbb{L}_1$ définie incomplètement par des formes de degré $\leq c_{67}LM^2$ avec multiplicité $\geq T_1$ passant par Q, telle que*

$$\deg(\alpha_p(V_{\mathbb{L}_1})) \leq c_{69}\left(\frac{LM^2}{T_1N_{r(i)}}\right)^{g_0-d_1} \deg(H).$$

Proof. Posons $\Gamma_p = \mathrm{Gal}(\bar{K}/\mathbb{L}_1) = \{\tau \in \mathrm{Gal}(\bar{K}/K),\ \tau_{|\mathbb{L}} \in G_p\}$. On suit le lemme de zéros de (Phi86). On pose

$$\mathcal{J} = (\partial_{0,\mathrm{Id}}^{T_1}\tau(F \circ \iota) \circ t_U,\ U \in \ker(\alpha_p), \tau^{-1} \in \Gamma_p)$$

et $W = \mathcal{Z}(\mathcal{J})$. Alors il existe une composante V de W, géométriquement irréductible, passant par Q. Puisque W est stable par translation par des points de α_p-torsion et par l'action des $\tau \in \Gamma_p$, alors $\tau(V) + U$ est aussi une composante de W lorsque $U \in \ker(\alpha_p)$. On peut donc écrire

$$T_1^{g_0-d_1} \deg\left(\bigcup_{\substack{U\in\ker(\alpha_p)\\ \tau\in\Gamma_p}} \tau(V) + U\right) \leq c_{68}(LM^2)^{g_0-d_1} \deg(H),$$

d'après le lemme 5 de (Phi96). En notant $V_{\mathbb{L}_1} = \bigcup_{\tau\in\Gamma_p} \tau(V)$ alors

$$\deg(\alpha_p^{-1}\alpha_pV_{\mathbb{L}_1}) \leq c_{68}\left(\frac{LM^2}{T_1}\right)^{g_0-d_1} \deg(H).$$

En utilisant la proposition 2.12 on a

$$\deg(\alpha_pV_{\mathbb{L}_1}) \quad \leq \quad c_{69}\left(\frac{LM^2}{T_1N(v)}\right)^{g_0-d_1} \deg(H).$$

7 Paramètres

Considérons P, $\mathbb{L}$ et H comme dans le théorème 1.15 et supposons que l'on a

$$\hat{h}(P) < \frac{1}{\omega_{\mathbb{L}}(P,H)} \left(\frac{\log\log \omega_{\mathbb{L}} \deg(H)^2}{C_0 \log \omega_{\mathbb{L}} \deg(H)^2} \right)^{(2g_0^2(g_0+1)!)^{2g_0}}. \tag{32}$$

L'idée de la descente est de construire une suite de variétés "emboîtées" de degré contrôlé et dont on contrôle aussi les stabilisateurs, à l'aide d'une utilisation répétée des lemmes de zéros 6.5 et 6.2. Ces lemmes s'appliquent à des ensembles $\mathcal{P}_1, \ldots, \mathcal{P}_{g_0}$ et des paramètres $L, M, T_0, \ldots, T_{g_0}, E_1, \ldots, E_{g_0}, N_1, \ldots, N_{g_0}$ satisfaisant les conditions (11) à (16) et (24) ou bien (17) à (22) et un point Q satisfaisant (23) ou bien (26) respectivement. Par la suite on va définir des ensembles de paramètres et des points satisfaisant ces conditions.

On pose $\delta = g_0^2(g_0+1)! + 2$ et on définit pour tout $i, j = 1, \ldots, g_0$,

$$\rho_j = \delta^{2g_0 - 2j}(g_0+1), \qquad a_i^{(j)} = i.i!\delta\rho_j,$$
$$b_i^{(j)} = i.i!\rho_j \quad \text{et} \quad b^{(j)} = \textstyle\sum_{i=1}^{g_0} b_i^{(j)}.$$

On remarque que $\sum_{i=1}^{k} i.i! = (k+1)! - 1$. Par la suite on notera $\omega_{\mathbb{L}} = \omega_{\mathbb{L}}(P,H)$ où P est le point de départ pour lequel on veut montrer le théorème principal. On rappelle qu'on a supposé plus haut que P satisfait (32).

Pour simplifier les calculs, on notera aussi

$$\Delta = \log(\omega_{\mathbb{L}} \deg(H)^2).$$

Du fait que $\mathcal{L} = \mathcal{L}_0^{\otimes 4}$ et la définition de $\omega_{\mathbb{L}}$ on a

$$\Delta \geq \log\deg(H) \geq \log 4 > 1.$$

On pose maintenant pour tout $1 \leq i, j \leq g_0$ les paramètres suivants :

$$N_i^{(j)} = \left[\left(\frac{C_0 \Delta}{\log \Delta} \right)^{a_i^{(j)}} \right] \quad \text{et} \quad E_i^{(j)} = \left[\left(\frac{C_0 \Delta}{\log \Delta} \right)^{b_i^{(j)}} \right].$$

On définit ensuite des ensembles d'isogénies $\mathcal{P}_1^{(j)}, \ldots \mathcal{P}_{g_0}^{(j)}$ pour $1 \leq j \leq g_0$ par

$$\mathcal{P}_i^{(j)} = \{\alpha_p,\ p \in \mathcal{P},\ \frac{N_i^{(j)}}{2} \leq p \leq N_i^{(j)}\} \cup \{\mathrm{Id}\}.$$

Pour chaque groupe d'isogénies $\mathcal{P}_i^{(j)}, \ldots, \mathcal{P}_{g_0}^{(j)}$ on disposera comme auparavant de deux cas : tous les ensembles sont "peu ramifiés" ou bien il existe au moins un ensemble très ramifié (par rapport aux indices de ramification $E_1^{(j)}, \ldots, E_{g_0}^{(j)}$). Lorsque le deuxième cas se présente, on rappelle qu'on a choisi le plus petit indice i tel que $\mathcal{P}_i^{(j)}$ est très ramifié et on l'a noté $r(\mathcal{P}^{(j)})$. Pour simplifier les notations on le notera dorénavant $r(j)$. On définit aussi comme auparavant pour tous $1 \leq i, j \leq g_0$ des ensembles $\Delta_i^{(j,\mathrm{pr})}$ et $\Delta_i^{(j,\mathrm{tr})}$.

Pour j donné on pose

$$\mathfrak{B}_j = \{\beta_j = \tau_1^{(j)}\alpha_1^{(j)} \circ \cdots \circ \tau_{g_0}^{(j)}\alpha_{g_0}^{(j)}\}$$

pour $\alpha_i^{(j)} \in \mathcal{P}_i^{(j)}$ et $\tau_i^{(j)}$ un élément de $\mathrm{Gal}(\bar{K}/K)$ qui prolonge ou bien ϕ_p si $\alpha_i^{(j)} = \alpha_p \in \Delta_i^{(j,\mathrm{pr})}$ ou bien un élément de G_p si $\alpha_i^{(j)} = \alpha_p \in \Delta_i^{(j,\mathrm{tr})}$ et $\tau_i^{(j)} = \mathrm{Id}$ si $\alpha_i^{(j)} = \mathrm{Id}$. On définit

$$\mathfrak{R}_i = \{F_i = \beta_i \circ \cdots \circ \beta_1,\ \beta_\ell \in \mathfrak{B}_\ell\}.$$

D'après le choix des paramètres on trouve

$$\begin{aligned} N(\beta_j) &\leq N_1^{(j)} \cdots N_{g_0}^{(j)} \\ &\leq \left(\frac{C_0 \Delta}{\log \Delta} \right)^{\sum_{i=1}^{g_0} \delta\rho_j i.i!} \\ &\leq \left(\frac{C_0 \Delta}{\log \Delta} \right)^{\delta\rho_j[(g_0+1)!-1]}. \end{aligned} \tag{33}$$

Par la suite on va travailler avec une suite de sous-corps de $\mathbb{L}$ qu'on construira inductivement à l'aide des isogénies qu'on va obtenir grâce aux lemmes de zéros. Ils sont définis de la façon suivante :

Définition 7.1. *Soient $\beta_1, \dots, \beta_{g_0}$ avec $\beta_j \in \mathfrak{B}_j$ tels que si pour j donné il existe $\mathcal{P}_{r(j)}^{(j)}$ très ramifié alors $\beta_j \in \Delta_{r(j)}^{(j,\mathrm{tr})}$. On associe une suite d'extensions abéliennes $\mathbb{L}_j$ pour $j = 0, \dots, g_0$ de la façon suivante :*
- *$\mathbb{L}_0 = \mathbb{L}$;*
- *si $\mathcal{P}_1^{(j+1)}, \dots, \mathcal{P}_{g_0}^{(j+1)}$ ont tous peu de grande ramification (au sens de la définition 5.1) on pose $\mathbb{L}_{j+1} = \mathbb{L}_j$;*
- *si on est dans le cas très ramifié, β_j est un endomorphisme de Frobenius associé à $v|p$ pour un certain p. Il existe un entier $m = m(p, \mathbb{L}_j)$ minimal tel que $\mathbb{L}_j \subseteq \mathbb{Q}_p(\zeta_m)$ et on pose $\mathbb{L}_{j+1} = \mathbb{L}_j \cap \mathbb{Q}_p(\xi_{m/p})$).*

Pour effectuer la descente on commencera par appliquer le lemme 6.5 ou le lemme 6.2 à un point P satisfaisant l'inégalité (32) (on verra plus loin que cette dernière implique les conditions (23) et (26)), aux entiers $E_1^{(1)}, \dots, E_{g_0}^{(1)}, N_1^{(1)}, \dots, N_{g_0}^{(1)}$ et à des paramètres $L^{(1)}, M^{(1)}, T_0^{(1)}, \dots, T_{g_0}^{(1)}$ qu'on va fixer plus bas. L'application des lemmes 6.5 ou 6.2 donne entre autres un élément $\beta_1 \in \mathfrak{B}_1$ et on notera $P_1 = \beta_1(P)$. On recomencera le même procédé avec le point P_1 et de nouveaux paramètres $L^{(2)}, M^{(2)}, T_0^{(2)}, \dots, T_{g_0}^{(2)}$ et ainsi de suite. De cette façon on construira au fur et à mesure une suite de points $P = P_0, P_1, \dots, P_{g_0}$.

On peut maintenant préciser les paramètres. Dans le cas peu ramifié on pose pour $j = 1, \dots, g_0$

$$\begin{aligned}
T_0^{(j)} &= \left[(\deg H)^4 \omega_{\mathbb{L}_{j-1}}(P_{j-1}, H) \frac{C_0^{b^{(j)}+2} \Delta^{b^{(j)}+g_0}}{(\log \Delta)^{b^{(j)}}}\right] \\
T_{i+1}^{(j)} &= \left[\frac{T_i^{(j)}}{(\log C_0)^2 \Delta} \left(\frac{\log \Delta}{C_0 \Delta}\right)^{b_{g_0-i}^{(j)}}\right] \qquad \forall i = 0, \dots, g_0 - 1 \\
L^{(j)} &= \left[\deg(H)^2 \omega_{\mathbb{L}_{j-1}}(P_{j-1}, H) \frac{C_0^{b^{(j)}+2} \Delta^{b^{(j)}+g_0}}{(\log \Delta)^{b^{(j)}}}\right] \\
M^{(j)} &= 2^{q+1} \text{ où } q = \left[\frac{\log L^{(j)}}{2 \log 2}\right].
\end{aligned}$$

On remarque facilement que pour C_0 assez grand

$$T_i^{(j)} \geq (\deg H)^4 \omega_{\mathbb{L}_{j-1}}(P_{j-1}, H) \frac{C_0^2 \Delta^{g_0-i}}{(\log C_0)^{2i+1}} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{b_1^{(j)}+\ldots+b_{g_0-i}^{(j)}}. \tag{34}$$

Avant de vérifier que ces paramètres satisfont les conditions imposées dans le paragraphe 5, on donne un corollaire qui facilitera les calculs.

Corollaire 7.2. *Si les ensembles $\mathcal{P}_1^{(j)}, \dots, \mathcal{P}_{g_0}^{(j)}$ ont tous peu de grande ramification et si les paramètres $T_i^{(j)}, L^{(j)}, M^{(j)}$ satisfont les conditions (11) à (16), (24) et (23) avec $Q = P_{j-1}$ et $\mathbb{L} = \mathbb{L}_{j-1}$ alors il existe une variété V définie sur $\mathbb{L}_j = \mathbb{L}_{j-1}$, définie incomplètement par des formes de degré $\leq c_{70} L^{(j)} (M^{(j)})^2 N_1^{(j)} \cdots N_{g_0-1}^{(j)}$ avec multiplicité $\geq c_{71} T_{g_0}$ le long de $T_{H(\mathbb{C})}$ de dimension d et une isogénie $\beta_j \in \mathfrak{B}_j$ telle que $P_j = \beta_j(P_{j-1}) \in V$ et*

$$\deg V \leq \frac{\deg(H) \omega_{\mathbb{L}_{j-1}}(P_{j-1}, H)^{g_0-d}}{(N_1^{(j)})^{g_0-d}} \left(\frac{\log \Delta}{C_0 \Delta}\right)^{2(b^{(j)}+g_0+1)(g_0-d)}.$$

On a aussi $\omega_{\mathbb{L}_j}(P_j, H) \leq \omega_{\mathbb{L}_{j-1}}(P_{j-1}, H)$.

Proof. Pour la première inégalité on remplace dans la conclusion du corollaire 6.4 les paramètres par leur valeur. On sait qu'il existe $k \geq g_0 - d$ tel que

$$\deg(V) \leq c_{72} \frac{\left(L^{(j)} (M^{(j)})^2 N_1^{(j)} \dots, N_{k-1}^{(j)}\right)^{g_0-d} \deg(H) \log N_k^{(j)}}{(T_{g_0}^{(j)})^{g_0-d} N_k^{(j)}}$$

et on vérifie facilement que

$$\begin{aligned}
\frac{(N_1^{(j)} \dots, N_{k-1}^{(j)})^{g_0-d}}{N_k} &\leq 2 \left(\frac{C_0 \Delta}{\log \Delta}\right)^{(g_0-d)\left(\sum\limits_{i=1}^{k-1} a_i^{(j)}\right) - a_k^{(j)}} \\
&\leq 2 \left(\frac{C_0 \Delta}{\log \Delta}\right)^{(g_0-d)(k!-1)\delta\rho_j - k.k!\delta\rho_j} \\
&\leq \frac{2}{(N_1^{(j)})^{g_0-d}}.
\end{aligned}$$

D'autre part,

$$\frac{L^{(j)}(M^{(j)})^2}{T_{g_0}^{(j)}} \leq c_{73}\frac{\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)C_0^{2b^{(j)}+2}\Delta^{2(b^{(j)}+g_0)}(\log C_0)^{2g_0+2}}{(\log\Delta)^{2b^{(j)}}},$$

et finalement

$$\begin{aligned}\deg(V) &\leq c_{74}(\log C_0)^{(2g_0+2)g_0+1}\log(\Delta)\deg(H)\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)^{g_0-d}\\ &\quad\times\left(\frac{C_0^{2b^{(j)}+2}\Delta^{2(b^{(j)}+g_0)}}{N_1^{(j)}(\log\Delta)^{2b^{(j)}}}\right)^{g_0-d}\\ &\leq c_{75}(\log C_0)^{(2g_0+2)g_0+1}\frac{\deg(H)\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)^{g_0-d}}{(N_1^{(j)})^{g_0-d}}\left(\frac{C_0^{2b^{(j)}+2}\Delta^{2(b^{(j)}+g_0)}}{(\log\Delta)^{2b^{(j)}-1}}\right)^{g_0-d}\\ &\leq \frac{\deg(H)\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)^{g_0-d}}{(N_1^{(j)})^{g_0-d}}\left(\frac{C_0\Delta}{\log\Delta}\right)^{2(b^{(j)}+g_0+1)(g_0-d)}.\end{aligned}$$

On a utilisé le fait que $\frac{(\log\Delta)^c}{\Delta}\leq c^c$ puisque $\Delta\geq 4$.

Ensuite, puisque V est définie sur $\mathbb{L}_j$, contenue dans H et contient P_j, $\omega_{\mathbb{L}_j}(P_j,H)\leq\left(\frac{\deg V}{\deg H}\right)^{1/\mathrm{codim}_H V}$ par définition. En remplaçant $\deg V$ par la borne ci-dessus on a

$$\omega_{\mathbb{L}_j}(P_j,H)\leq\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)\left(\frac{\log\Delta}{C_0\Delta}\right)^{a_1^{(j)}-2b^{(j)}-2g_0-2}$$

et, d'après le choix de δ, $a_1^{(j)}\geq 2b^{(j)}+2g_0+2$ ce qui permet de conclure.

Dans le cas très ramifié, pour chaque j on rappelle qu'on a choisi un ensemble $\mathcal{P}_{r(j)}^{(j)}$ très ramifié et supposons donnée une suite d'extensions $\mathbb{L}_0,\ldots,\mathbb{L}_{g_0}$ comme auparavant. On pose

$$\begin{aligned}T_0^{(j)} &= \left[(\deg H)^4\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)C_0^3\left(\frac{C_0\Delta}{\log\Delta}\right)^{2a_{r(j)}^{(j)}}\right]\\ T_1^{(j)} &= \left[\frac{T_0^{(j)}}{(\log C_0)^2\Delta}\left(\frac{\log\Delta}{C_0\Delta}\right)^{a_{r(j)}^{(j)}}\right]\\ L^{(j)} &= \left[\deg(H)^2\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)C_0^2\left(\frac{C_0\Delta}{\log\Delta}\right)^{a_{r(j)}^{(j)}}\right]\\ M^{(j)} &= 2^{q+1} \text{ où } q=\left[\frac{\log L^{(j)}}{2\log 2}\right].\end{aligned}$$

On remarque que

$$T_1^{(j)}\geq\frac{\deg(H)^4\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)C_0^{a_{r(j)}^{(j)}+3}\Delta^{a_{r(j)}^{(j)}-1}}{(\log C_0)^3(\log\Delta)^{a_{r(j)}^{(j)}}}. \tag{35}$$

Dans ce cas on a le corollaire suivant du lemme de zéros :

Corollaire 7.3. *Soit $r(j)$ le plus petit indice tel que l'ensemble $\mathcal{P}_{r(j)}^{(j)}$ a "beaucoup" de grande ramification. Si les paramètres $T_0^{(j)}, L^{(j)}, M^{(j)}$ vérifient les conditions (17) à (22) et (26) avec $Q=P_{j-1}$ et $\mathbb{L}=\mathbb{L}_{j-1}$, alors il existe une isogénie $\beta_j\in\mathfrak{B}_j$ et une variété V définie sur $\mathbb{L}_j\subsetneq\mathbb{L}_{j-1}$ de dimension d passant par P_{j-1} incomplètement définie par des formes de degré $\leq c_{76}LM^2$ avec multiplicité $\geq T_1$ le long de $T_{H(\mathbb{C})}$. De plus on a l'inégalité*

$$\deg(\beta_j(V))\leq c_{77}\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)^{g_0-d}\deg(H)(C_0^2\Delta)^{g_0-d}.$$

On a aussi

$$\omega_{\mathbb{L}_j}(P_j,H)\leq c_{78}\omega_{\mathbb{L}_{j-1}}(P_{j-1},H)C_0^2\Delta$$

où $P_j=\beta_j(P_{j-1})$.

Proof. Il suffit de remplacer les paramètres par leur valeur et suivre le même raisonnement que dans le cas peu ramifié.

Remarque 7.4. *De façon triviale, on a l'inégalité suivante dans les deux cas*

$$\omega_{\mathbb{L}_j}(P_j, H) \leq c_{79}\omega_{\mathbb{L}_{j-1}}(P_{j-1}, H)C_0^2\Delta.$$

Voyons maintenant que les paramètres fixés vérifient les conditions désirées.

***Cas* $\mathbf{j = 1}$.** Dans un premier temps, vérifions les conditions pour $L^{(1)}, M^{(1)}, T_0^{(1)}, \ldots, T_{g_0}^{(1)}$ les paramètres du cas peu ramifié, le point $P_0 = P$ et l'extension $\mathbb{L}_0 = \mathbb{L}$. On va oublier l'exposant (1) pour simplifier l'écriture.

La condition (11) est satisfaite puisque $\deg(H)\omega_{\mathbb{L}}(P, H) \geq 1$. La vérification de (15) est aussi immédiate. Pour (12) on calcule

$$\frac{LM^2}{T_0\omega_{\mathbb{L}}(P, H)} \geq c_{80}\frac{C_0^{b+2}\Delta^{b+g_0}}{(\log\Delta)^b} \geq C_0$$

ce qui conclut. La condition (13) est vérifiée en calculant

$$\begin{aligned}\frac{T_i\log(N_{g_0-i})}{(\log C_0)E_{g_0-i}\log(T_{i+1}+L)} &\geq c_{81}\frac{T_i(\log\Delta)^{b_{g_0-i}}\log(C_0\Delta)}{(\log C_0)(C_0\Delta)^{b_{g_0-i}}\Delta\log(C_0\Delta)}\\ &\geq \frac{T_i}{\Delta\log(C_0)^2}\left(\frac{\log\Delta}{C_0\Delta}\right)^{b_{g_0-i}} \quad \text{pour } C_0 \text{ assez grand}\\ &\geq T_{i+1}.\end{aligned}$$

Vérifions (14) :

$$\begin{aligned}\frac{N_k}{\log N_k\log((LM^2N_1\cdots N_{k-1})^{g_0}\deg H)} &\geq c_{82}\left(\frac{C_0\Delta}{\log\Delta}\right)^{a_k}\frac{1}{\log(C_0\Delta)^2\Delta}\\ &\geq \frac{C_0^{a_k-1}\Delta^{a_k-1}}{(\log\Delta)^{a_k+2}}\\ &\geq c_{83}C_0^{a_k-1}(\log\Delta)^{a_k-4}\end{aligned}$$

où l'on a utilisé de nouveau $\frac{\Delta}{(\log\Delta)^2} \geq 1$. Puisque $a_k \geq 4$ d'après le choix de δ la condition est vérifiée. Pour (16) on calcule

$$\begin{aligned}\frac{T_i\log N_{g_0-i}}{\log(C_0)E_{g_0-i}\log(LM^2\deg H)} &\geq c_{84}\deg(H)^4\omega_{\mathbb{L}}(P, H)\frac{C_0\Delta^{g_0-i-1}}{\log C_0} \quad \text{(en utilisant (34))}\\ &\geq \deg(H)^4\omega_{\mathbb{L}}(P, H) \quad \text{pour } C_0 \text{ assez grand}\\ &\geq 1.\end{aligned}$$

Voyons maintenant que la condition (24) sur l'exposant de Dirichlet η est aussi vérifiée. On rappelle que r est le rang du système (6) au cran 1 pour le point $P_0 = P$ et I est le nombre d'inconnues de ce système. En appliquant le lemme 4.3 au point P on a

$$r \leq c_{85}T_0^{g_0-d}\omega_{\mathbb{L}}(P, H)^{g_0-d}\deg(H)(LM^2)^d$$

et d'après l'encadrement (9) on a

$$I \geq c_{86}\deg(H)(LM^2)^{g_0}.$$

En utilisant la condition (12) on a pour C_0 assez grand $I \geq 2r$ d'où

$$\begin{aligned}\eta \leq \frac{2r}{I} &\leq c_{87}\frac{T_0^{g_0-d}\omega_{\mathbb{L}}(P, H)^{g_0-d}}{(LM^2)^{g_0-d}}\\ &\leq \frac{c_{88}}{C_0^2\Delta^{g_0}}\left(\frac{\log\Delta}{C_0\Delta}\right)^b.\end{aligned}$$

D'autre part, on remarque que $L \leq T_0$ et que $T_0\log(T_0+L)M + L \leq c_{89}T_0\Delta\log(C_0\Delta)$. En utilisant (34) on a donc

$$\begin{aligned}\frac{T_i\log N_{g_0-i}}{C_0^{\frac{1}{2}}E_{g_0-i}(T_0\log(T_0+L)M+L)} &\geq c_{90}\frac{1}{C_0^{\frac{3}{4}}\Delta^{g_0}}\left(\frac{\log\Delta}{C_0\Delta}\right)^b\\ &\geq \frac{1}{C_0\Delta^{g_0}}\left(\frac{\log\Delta}{C_0\Delta}\right)^b\\ &\geq \eta.\end{aligned}$$

Voyons maintenant le cas très ramifié. La vérification de (17) et (22) est triviale. Pour (18) on voit facilement que

$$\frac{LM^2}{T_0\omega_{\mathbb{L}}(P,H)} \geq c_{91}C_0 \geq C_0^{\frac{1}{2}}.$$

La condition (19) est vérifiée puisque

$$\begin{aligned}\frac{T_{r(0)}\log N_{r(0)}}{N_{r(0)}\log(L\deg H)} &\geq c_{92}\deg(H)^4\omega_{\mathbb{L}}(P,H)\frac{C_0^{a_{r(1)}+3}\Delta^{a_{r(1)}-1}}{(\log\Delta)^{a_{r(1)}}}\\ &\geq c_{93}\deg(H)^4\omega_{\mathbb{L}}(P,H)C_0^{a_{r(1)}+3}(\log\Delta)^{a_{r(1)}-2}\\ &\geq \deg(H)^4\omega_{\mathbb{L}}(P,H)C_0^{a_{r(1)}+2}(\log\Delta)^{a_{r(1)}-2}\end{aligned}$$

et $a_{r(1)}+2>1$. Pour (20) on calcule

$$\begin{aligned}\frac{T_0\log(N_{r(1)})}{\log(C_0)N_{r(1)}\log(T_1+L)} &\geq c_{94}\frac{T_0}{\Delta(\log C_0)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{a_{r(1)}}\\ &\geq \frac{T_0}{(\log C_0)^2\Delta}\left(\frac{\log\Delta}{C_0\Delta}\right)^{a_{r(1)}}\\ &\geq T_1.\end{aligned}$$

Il ne reste qu'à vérifier (21). On a

$$\begin{aligned}\frac{T_0\log N_{r(1)}}{C_0^{\frac{1}{2}}N_{r(1)}L} &\geq c_{95}\frac{\deg(H)^2C_0\log(C_0\Delta)}{C_0^{\frac{1}{2}}}\\ &\geq \deg(H)^2\log(\Delta)\\ &\geq 1,\end{aligned}$$

ce qu'il fallait démontrer.

Cas général. On procède par récurrence. On a montré que les différentes conditions sont vérifiées dans les deux cas pour $j=1$. Supposons qu'on a montré que les paramètres vérifient les conditions imposées à chaque cran pour $j=1,\dots,i$. Ceci implique en particulier d'après la remarque 7.4

$$\omega_{\mathbb{L}_i}(P_i,H) \leq c_{96}\omega_{\mathbb{L}}(P,H)C_0^{2i}\Delta^i.$$

Il suffit de reprendre les calculs effectués dans le cas $j=1$. Les inégalités restent vraies dans le cas $j=i+1$ du fait que seules les constantes changent puisque $\log(C_0\omega_{\mathbb{L}_i}(P_i,H)(\deg H)^2) \leq c_{97}\Delta\log(C_0\Delta)$.

Remarque 7.5. *D'après la remarque 6.3 on peut appliquer les corollaires 7.2 et 7.3 à des sous-ensembles $\mathcal{P}_i^{*(j)}$ des ensembles $\mathcal{P}_i^{(j)}$, pour $1\leq i\leq g_0$, pourvu que l'on sache que $|\mathcal{P}_i^{*(j)}\cap\Delta_i^{(j,\mathrm{pr})}|$ est de cardinal $\geq c_{98}\frac{N_i^{(j)}}{\log(N_i^{(j)})}$ pour tout $1\leq i\leq g_0$ dans le cas peu ramifié, et $|\mathcal{P}_{r(j)}^{*(j)}\cap\Delta_{r(j)}^{(j,\mathrm{tr})}|\geq 1$ dans le cas très ramifié.*

8 Descente

Comme on l'a déjà dit, l'idée est de construire une suite de variétés "emboîtées". Pour conclure il faut ensuite montrer qu'on peut construire de telles variétés de façon qu'il y en ait deux de même dimension et ensuite appliquer le théorème de Bézout pour obtenir une contradiction.

C'est l'argument de (DH00) (7.3) qu'il faudra modifier puisque l'on dispose de deux lemmes de zéros différents qu'il faut traiter en même temps.

Dans cette partie on aura besoin d'un raffinement de l'inégalité de Bézout. C'est le lemme suivant (lemme 4.9 de (DH00)) :

Lemme 8.1. *Il existe une constante c vérifiant la propriété suivante. Soit V une sous-variété propre de A définie sur $\mathbb{L}$ et $\mathbb{L}$-irréductible, F une forme de degré ν sur A, définie sur $\mathbb{L}$ et V' une sous-variété de A, $\mathbb{L}$-irréductible telle que F est nulle avec multiplicité $\geq m$ sur V'. S'il existe une composante $\mathbb{L}$-irréductible commune W de $V.V'$ et $V.\mathcal{Z}(F)$ de codimension 1 dans V, alors*

$$\deg(W) \leq c\frac{\deg(V)\nu}{m}.$$

Remarque 8.2. *Par la suite, pour utiliser le lemme ci-dessus, on sera amené à calculer à plusieurs reprises les quotients* $\frac{L^{(j)}M^{(j)2}N_1^{(j)}\cdots N_{r-1}^{(j)}}{T_{g_0}^{(j)}}$ *avec* $r \le g_0$ *dans le cas peu ramifié et* $\frac{L^{(j)}M^{2(j)}}{T_1^{(j)}}$ *dans le cas très ramifié. Pour simplifier les calculs on vérifie facilement en remplaçant les paramètres par leur valeur et les inégalités (34) et (35) que ces deux quantités sont majorées par*

$$\omega_{\mathbb{L}_{j-1}}(P_{j-1}, H)\left(\frac{C_0\Delta}{\log\Delta}\right)^{g_0!\delta\rho_j}$$

dans le cas peu ramifié et

$$c_{99}(\log C_0)^2\omega_{\mathbb{L}_{j-1}}(P_{j-1}, H)C_0\Delta\left(\frac{C_0\Delta}{\log\Delta}\right)^{a^{(j)}_{r(j)}}$$

dans le cas très ramifié.

Lemme 8.3. *Soit* j *un entier compris entre 1 et* $g_0 - 1$, $F_j = \beta_j \circ \cdots \circ \beta_1 \in \mathfrak{R}_j$ *et* $\mathbb{L}_j$ *une extension associée. Si* P *vérifie les conditions (23) et (25) pour les paramètres* $L^{(1)}, M^{(1)}, T_0^{(1)}, \ldots, T_{g_0}^{(1)}$ *peu ramifiés et (26) pour les paramètres* $L^{(1)}, M^{(1)}, T_0^{(1)}, T_1^{(1)}$ *très ramifiés alors* $P_j = F_j(P)$ *vérifie les conditions (23) (avec les paramètres* $L^{(j+1)}, M^{(j+1)}, T_0^{(j+1)}, \ldots, T_{g_0}^{(j+1)}$ *peu ramifiés) et (26) (avec les paramètres* $L^{(j+1)}, M^{(j+1)}, T_0^{(j+1)}, T_1^{(j+1)}$ *très ramifiés).*

Proof. Posons $\kappa(g_0) = (2g_0^2(g_0+1)!)^{2g_0}$. On a $F_j(P) = (\beta_j \circ \cdots \circ \beta_1)(P)$ avec $\beta_l \in \mathfrak{B}_l$. D'après (33), l'hypothèse (32) et la remarque 7.4 on a

$$\begin{aligned}
\hat{h}(F_j(P)) &= N(\beta_1)\cdots N(\beta_j)\hat{h}(P)\\
&\le \left(\frac{C_0\Delta}{\log\Delta}\right)^{[(g_0+1)!-1]\delta\sum_{k=1}^{j}\rho_k}\frac{1}{\omega_{\mathbb{L}}(P,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa(g_0)}\\
&\le \frac{c_{100}(C_0^2\Delta)^j}{\omega_{\mathbb{L}_j}(P_j,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa(g_0)-(g_0+1)!j\delta\rho_1+\delta j\rho_1}\\
&\le \frac{c_{101}}{\omega_{\mathbb{L}_j}(P_j,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa(g_0)-(g_0+1)!j\delta\rho_1+\delta j\rho_1-2j}.
\end{aligned}$$

D'autre part, dans le cas peu ramifié, pour tout $i = 0, \ldots, g_0 - 1$ l'expression

$$\frac{T_i^{(j+1)}\log(N_{g_0-i}^{(j+1)})}{(\log C_0)L^{(j+1)}(M^{(j+1)})^2E_{g_0-i}^{(j+1)}N_{g_0-i}^{(j+1)}\cdots N_{g_0}^{(j+1)}}$$

est minorée par

$$\begin{aligned}
&\ge \frac{c_{102}}{(\log C_0)^{2i+1}\omega_{\mathbb{L}_j}(P_j,H)}\frac{(\log\Delta)^{2b^{(j+1)}+[(g_0+1)!-1]\delta\rho_{j+1}}}{C_0^{2b^{(j+1)}+2+[(g_0+1)!-1]\delta\rho_{j+1}}\Delta^{2b^{(j+1)}+2g_0+[(g_0+1)!-1]\delta\rho_{j+1}}}\\
&\ge \frac{1}{\omega_{\mathbb{L}_j}(P_j,H)}\frac{(\log\Delta)^{2b^{(j+1)}+[(g_0+1)!-1]\delta\rho_{j+1}}}{C_0^{2b^{(j+1)}+3+[(g_0+1)!-1]\delta\rho_{j+1}}\Delta^{2b^{(j+1)}+2g_0+[(g_0+1)!-1]\delta\rho_{j+1}}}\\
&\ge \frac{1}{\omega_{\mathbb{L}_j}(P_j,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{2b^{(j+1)}+2g_0+2+[(g_0+1)!-1]\delta\rho_{j+1}}.
\end{aligned}$$

On vérifie facilement d'après la définition de δ que

$$j\delta\rho_1 - 2j \ge (g_0+1)!\delta\rho_{j+1} - \delta\rho_{j+1} + 2g_0 + 2b^{(j+1)} + 2.$$

Pour conclure il faut simplement vérifier que

$$\kappa(g_0) > (g_0+1)!(g_0-1)\delta\rho_1.$$

La partie droite de cette inégalité est majorée par $(g_0+1)!g_0^2(2g_0^2(g_0+1)!)^{2g_0-1}$ et on conclut que (23) est vérifiée quitte à choisir C_0 assez grand.

Pour montrer que (26) est satisfaite, on remplace les paramètres du cas très ramifié par leur valeur et on montre que l'expression

$$\frac{T_0^{(j+1)}\log(N_{r(j+1)}^{(j+1)})}{(\log C_0)N_{r(j+1)}^{(j+1)}L^{(j+1)}(M^{(j+1)})^2}$$

est minorée par

$$\begin{aligned}
&\geq \frac{c_{103}}{C_0(\log C_0)\omega_{\mathbb{L}_j}(P_j,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{a_{r(j+1)}^{(j+1)}}\\
&\geq \frac{1}{C_0^2\omega_{\mathbb{L}_j}(P_j,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{g_0.g_0!\delta\rho_{j+1}}\\
&\geq \frac{1}{\omega_{\mathbb{L}_j}(P_j,H)}\left(\frac{\log\Delta}{C_0\Delta}\right)^{g_0.g_0!\delta\rho_{j+1}+2}.
\end{aligned}$$

Il faut donc montrer

$$g_0.g_0!\delta\rho_{j+1}+2<\kappa(g_0)-(g_0+1)!j\delta\rho_1+\delta j\rho_1-2j.$$

On vérifie facilement que $\delta j\rho_1>g_0.g_0!\delta\rho_{j+1}+2+2j$ et, comme dans le cas peu ramifié plus haut, on a $\kappa(g_0)>(g_0+1)!j\delta\rho_1$ ce qui permet de conclure.

De plus, on remarque que F_i est une isogénie et donc $F_i(P)$ n'appartient à aucune sous-variété de torsion propre de H.

Définition 8.4. *Pour $1\leq i\leq g_0$ un entier donné, on notera μ la fonction définie par :*

$$\mu(i)=\begin{cases}1 \text{ si } \mathcal{P}_1^{(i)},\dots,\mathcal{P}_{g_0}^{(i)} \text{ ont tous peu de grande ramification;}\\ 0 \text{ sinon.}\end{cases}$$

On pose $\mu(0)=0$.

On rappelle que dans la définition 7.1 on a vu comment associer à une suite d'éléments $\beta_1,\dots,\beta_k$ où $\beta_i\in\mathfrak{B}_i$, une suite d'extensions $\mathbb{L}_0,\dots,\mathbb{L}_k$.

Définition 8.5. *Soit $\mathcal{W}$ l'ensemble des triplets (k,β,W) où $k\in[0,g_0]$ est un entier, $\beta=(\beta_1,\dots,\beta_k)$ est un k-uplet d'isogénies admissibles appartenant à $\mathfrak{B}_1\times\cdots\times\mathfrak{B}_k$, $F_i=\beta_1\circ\cdots\circ\beta_i$ pour $i=1,\dots,k$, $(\mathbb{L}_0,\dots,\mathbb{L}_k)$ une suite de sous-corps de $\mathbb{L}$ associée à $(\beta_1,\dots,\beta_k)$ et $W=(W_0,\dots,W_k)$ un $(k+1)$-uplet de variétés propres de H, satisfaisant :*

(i). W_i définie sur $\mathbb{L}_i$, $\mathbb{L}_i$-irréductible et $P_i=F_i(P)\in W_i$;
(ii). $\beta_i^{-1}(W_i)\supseteq W_{i-1}$ pour tout $i=1,\dots,k$;
(iii). pour tout $i=0,\dots,k$ on a

$$\begin{aligned}\deg(W_i)\quad\leq\quad & c_{104}\frac{\omega_{\mathbb{L}_{i-1}}(P_{i-1},H)^{g_0-d_i}\deg(H)}{(N_1^{(i)})^{\mu(i)}}\\ &\times\left(\frac{C_0\Delta}{\log\Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+1}+2(g_0+1)!\rho_i\mu(i)](g_0-d_i)}\end{aligned}\tag{36}$$

où $d_i=\dim W_i$;
(iv). $N(\beta_{i+1})$ est premier avec $|G_{W_i}:G_{W_i}^\circ|$ pour tout i, $0\leq i\leq k-1$.

On pose les conventions suivantes : $\beta_0=\mathrm{Id}$, $\mathbb{L}_{-1}=\mathbb{L}_0$, $P_{-1}=P_0$, $\rho_{g_0+1}=1$.

On veut maintenant trouver un élément (k,β,W) tel que $\dim(W_{i+1})=\dim(W_i)$ pour au moins un indice i. Motivés par cet objectif, on pose

$$\mathcal{W}_{\mathbf{0}}=\{(k,\beta,W)\in\mathcal{W}\text{ tels que }\dim(W_0)<\cdots<\dim(W_k)\}.$$

On cherche donc à démontrer :

Proposition 8.6. *Soit $P\in H(\bar{K})$ vérifiant la condition (32), d'ordre infini modulo toute sous-variété abélienne propre de H. Alors $\mathcal{W}_{\mathbf{0}}\neq\mathcal{W}$.*

On va d'abord munir l'ensemble des suites finies d'entiers d'un ordre total noté $\preceq$.

Définition 8.7. *Soit* $(v) = (v_i)_{0\le i\le s}$ *et* $(u) = (u_i)_{0\le i\le s'}$ *deux suites d'entiers. On dit que* $(v) \preceq (u)$ *si*

$$(v_i)_{0\le i\le \min\{s,s'\}} < (u_i)_{0\le i\le \min\{s,s'\}}$$

pour l'ordre lexicographique ou si $(v_i)_{0\le i\le \min\{s,s'\}} = (u_i)_{0\le i\le \min\{s,s'\}}$ *et* $s \ge s'$.

On peut maintenant définir un ordre sur $\mathcal{W}$: on dira que

$$(s, \beta, W) \preceq (s', \beta', W') \text{ si et seulement si } (\dim W_i)_{0\le i\le s} \preceq (\dim W_i')_{0\le i\le s'}.$$

Le but des lemmes suivants est de montrer que pour un élément donné $(k, \beta, W) \in \mathcal{W}$ avec $k \ne g_0$ on peut construire un nouvel élément $(k', \beta', W') \in \mathcal{W}$ tel que $(k', \beta', W') \prec (k, \beta, W)$.

Lemme 8.8. *Soit* $(k, \beta^{(k)}, W^{(k)}) \in \mathcal{W}$ *où* $\beta^{(k)} = (\beta_1, \dots, \beta_k)$ *et* $W^{(k)} = (W_0^{(k)}, \dots, W_k^{(k)})$. *Il existe des éléments* $\beta_{k+1}, \dots, \beta_{g_0} \in \mathfrak{B}_{k+1} \times \cdots \times \mathfrak{B}_{g_0}$ *et des* j*-uplets de sous-variétés* $W^{(j)} = (W_0^{(j)}, \dots, W_j^{(j)})$ *pour* $j = k+1, \dots, g_0$, *tels que*

(i). Pour tout $j = k+1, \dots, g_0$, $(j, \beta^{(j)}, W^{(j)})$ *satisfait les propriétés (i) et (ii) de la définition 8.5 où* $\beta^{(j)}$ *désigne le* j*-uplet* $(\beta_1, \dots, \beta_j)$ *;*

(ii). Pour tout $j = k+1, \dots, g_0$ *et* $0 \le i \le j$ *on a*

$$\deg(W_i^{(j)}) \le c_{105} \frac{\omega_{\mathbb{L}_{i-1}}(P_{i-1}, H)^{g_0 - d_i^{(j)}} \deg(H)}{(N_1^{(i)})^{\mu(i)}} \times \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+1} + 2(g_0+1)!\rho_i \mu(i)](g_0 - d_i^{(j)})} \tag{37}$$

où $d_i^{(j)} = \dim(W_i^{(j)})$ *;*

(iii). $N(\beta_{j+1})$ *est premier avec* $|G_{W_j^{(j)}} : G^\circ_{W_j^{(j)}}|$ *pour tout* $j = k, \dots, g_0 - 1$ *;*

(iv). $W_i^{(j)} \supseteq W_i^{(j+1)}$ *pour* $k \le j \le g_0 - 1$, $0 \le i \le j$.

Proof. C'est le lemme 7.5 de (DH00) où il faudra faire quelques modifications pour tenir compte de tous les cas. Il s'agit d'une construction par récurrence. Dans un premier temps, on voit bien que si $(k, \beta^{(k)}, W^{(k)}) \in \mathcal{W}$ alors les variétés $W_i^{(k)}$ satisfont la condition (37) puisqu'elles satisfont par définition la condition (36).

On montre par la suite comment construire à partir d'un triplet $(k, \beta^{(k)}, W^{(k)})$ un triplet $(k+1, \beta^{(k+1)}, W^{(k)})$.

Premier cas. S'il existe $r(k+1)$ tel que l'ensemble $\mathcal{P}_{r(k+1)}^{(k+1)}$ ait beaucoup de grande ramification, on applique le corollaire 7.3 au point $F_k(P) = P_k$, et l'ensemble

$$\mathcal{P}_{r(k+1)}^{*(k+1)} = \mathcal{P}_{r(k+1)}^{(k+1)} \setminus \mathcal{S} \quad \text{où} \quad \mathcal{S} = \{\alpha_p \in \mathcal{P}_{r(k+1)}^{(k+1)}, (p, |G_{W_k^{(k)}} : G^\circ_{W_k^{(k)}}|) \ne 1\}.$$

Cet ensemble respecte la condition de la remarque 7.5 : en effet le lemme 2.3 assure que la partie discrète du stabilisateur de $W_k^{(k)}$ est au plus polynomiale en le degré de $W_k^{(k)}$, donc au plus polynomiale en $\omega_{\mathbb{L}_{k-1}}(P_{k-1})$ et $\deg(H)$. D'autre part le nombre de premiers divisant un entier N donné est un $O(\log(N))$ donc le cardinal de $\mathcal{S}$ est inférieur à $C_0\Delta$. D'autre part $\left|\Delta_{r(k+1)}^{(k+1,\mathrm{tr})}\right| > \frac{|\mathcal{P}_{r(k+1)}^{(k+1)}|}{2}$ et donc $|\mathcal{P}_{r(k+1)}^{*(k+1)} \cap \Delta_{r(k+1)}^{(k+1,\mathrm{tr})}| \ge 1$.

On obtient ainsi une isogénie α_p qu'on note β_{k+1} (il suffit de compléter par des identités pour avoir un élément de $\mathfrak{B}_{k+1}$), une variété $\tilde{W}_{k+1}^{(k+1)}$ propre de H définie sur $\mathbb{L}_{k+1}$, de dimension notée $d_{k+1}^{(k+1)}$ passant par P_k. On pose

$$W_{k+1}^{(k+1)} := \beta_{k+1}(\tilde{W}_{k+1}^{(k+1)})$$

et donc d'après le corollaire 7.3

$$\deg(W_{k+1}^{(k+1)}) \le c_{106}\omega_{\mathbb{L}_k}(P_k, H)^{g_0 - d_{k+1}^{(k+1)}} \deg(H)(C_0^2\Delta)^{g_0 - d_{k+1}^{(k+1)}}.$$

Dans ce cas $\mu(k+1) = 0$ et donc $W_{k+1}^{(k+1)}$ vérifie la condition (37) de façon triviale.

D'après le corollaire 7.3 il existe des formes définies sur $\mathbb{L}_{k+1}$ de degré $\leq c_{107}L^{(k+1)}(M^{(k+1)})^2$ qui définissent incomplètement $\tilde{W}_{k+1}^{(k+1)}$ avec multiplicité $\geq T_1^{(k+1)}$; soient $G_1, \ldots, G_s$ de telles formes. On construit $W_0^{(k+1)}$ de la façon suivante : parmi les composantes irréductibles sur $\mathbb{L}_0$ de $W_0^{(k)} \cap F_k^{-1}\mathcal{Z}(G_{i_1})$ on en choisit une Y_1 contenant une composante irréductible de dimension maximale de $W_0^{(k)} \cap F_k^{-1}(\tilde{W}_{k+1}^{(k+1)})$ passant par P_k. D'après le lemme 8.1 on a

$$\deg(Y_1) \leq \frac{c_{108} \deg(W_0^{(k)}) L^{(k+1)}(M^{(k+1)})^2 N(F_k)}{T_1^{(k+1)}}.$$

On recommence le même procédé avec G_{i_2} et ainsi de suite jusqu'à trouver un entier u tel que

$$W_0^{(k)} \cap F_k^{-1}\mathcal{Z}(G_{i_1}) \cap \ldots \cap F_k^{-1}\mathcal{Z}(G_{i_u})$$

ait même dimension en P que $W_0^{(k)} \cap F_k^{-1}(\tilde{W}_{k+1}^{(k+1)})$. On choisit pour $W_0^{(k+1)}$ une composante irréductible de $W_0^{(k)} \cap F_k^{-1}\mathcal{Z}(G_1) \ldots F_k^{-1}\mathcal{Z}(G_u)$ contenant une composante irréductible sur $\mathbb{L}_0$ de dimension maximale de $W_0^{(k)} \cap F_k^{-1}(\tilde{W}_{k+1}^{(k+1)})$ passant par P. On a donc

$$\deg(W_0^{(k+1)}) \leq c_{109} \deg(W_0^{(k)}) \left(\frac{L^{(k+1)}(M^{(k+1)})^2 N(\beta_1) \cdots N(\beta_k)}{T_1^{(k+1)}} \right)^u$$

et en utilisant la remarque 8.2 on obtient

$$\begin{aligned} \deg(W_0^{(k+1)}) \quad &\leq \quad c_{110} \deg(W_0^{(k)}) \omega_{\mathbb{L}_k}(P_k, H)^u (C_0\Delta)^u (\log C_0)^{2u} \\ &\quad \times \left(\frac{C_0\Delta}{\log \Delta} \right)^{g_0 . g_0! \delta \rho_{k+1} u} \big(N(\beta_k) \cdots N(\beta_1) \big)^u. \end{aligned}$$

Par définition $d_0^{(k+1)} = d_0^{(k)} - u$ et d'après la remarque 7.4 et la borne (33) on a

$$\begin{aligned} \deg(W_0^{(k+1)}) &\leq c_{111} \deg(W_0^{(k)}) \omega_{\mathbb{L}_0}(P_0, H)^{\left(d_0^{(k)} - d_0^{(k+1)}\right)} \left(\frac{C_0\Delta}{\log \Delta} \right)^{(2k+1)\left(d_0^{(k)} - d_0^{(k+1)}\right)} \\ &\quad \times \left(\frac{C_0\Delta}{\log \Delta} \right)^{\left(g_0 . g_0! \delta \rho_{k+1} + 1 + [(g_0+1)! - 1]\delta \sum_{j=1}^{k} \rho_j\right)\left(d_0^{(k)} - d_0^{(k+1)}\right)}. \end{aligned}$$

On vérifie facilement que

$$g_0 . g_0! \delta \rho_{k+1} + 2 + 2k - \delta \sum_{j=1}^{k} \rho_j \leq g_0 . g_0! \delta \rho_{k+1} + 2 + 2k - k\delta\rho_k \leq 0$$

pour $k > 0$ et donc

$$\deg(W_0^{(k+1)}) \leq c_{112} \deg(W_0^{(k)}) \omega_{\mathbb{L}_0}(P_0, H)^{d_0^{(k)} - d_0^{(k+1)}} \left(\frac{C_0\Delta}{\log \Delta} \right)^{(g_0+1)! \delta \rho_1 (g_0 - 1)(d_0^{(k)} - d_0^{(k+1)})}.$$

Si $k = 0$, $F_k = \mathrm{id}$ et la dernière inégalité est encore vraie.

En utilisant l'hypothèse de récurrence on a

$$\begin{aligned} \deg(W_0^{(k+1)}) &\leq c_{113} \omega_{\mathbb{L}_0}(P_0, H)^{g_0 - d_0^{(k+1)}} \deg(H) \left(\frac{C_0\Delta}{\log \Delta} \right)^{g_0(g_0+1)! \delta \rho_1 (g_0 - d_0^{(k)})} \\ &\quad \times \left(\frac{C_0\Delta}{\log \Delta} \right)^{(g_0 - 1)(g_0+1)! \delta \rho_1 (d_0^{(k)} - d_0^{(k+1)})} \\ &\leq c_{114} \omega_{\mathbb{L}_0}(P_0, H)^{g_0 - d_0^{(k+1)}} \deg(H) \left(\frac{C_0\Delta}{\log \Delta} \right)^{g_0(g_0+1)! \delta \rho_1 (g_0 - d_0^{(k+1)})} \end{aligned}$$

ce qu'il fallait démontrer.

Supposons les variétés $W_0^{(k+1)}, \dots, W_m^{(k+1)}$ construites pour $m \leq k-1$ et construisons $W_{m+1}^{(k+1)}$. On coupe $W_{m+1}^{(k)}$ par le nombre minimal de formes $G_1, \dots, G_u$ définissant $\tilde{W}_{k+1}^{(k+1)}$ avec multiplicité $\geq T_1^{(k+1)}$ tirées en arrière par $(\beta_k \circ \cdots \circ \beta_{m+2})^{-1}$ de sorte que

$$W_{m+1}^{(k)} \cap (\beta_k \circ \cdots \circ \beta_{m+2})^{-1} \mathcal{Z}(G_1) \cap \ldots \cap (\beta_k \circ \cdots \circ \beta_{m+2})^{-1} \mathcal{Z}(G_u)$$

ait même dimension en P_{m+1} que

$$W_{m+1}^{(k)} \cap (\beta_k \circ \cdots \circ \beta_{m+2})^{-1} (\tilde{W}_{k+1}^{(k+1)}).$$

Comme plus haut, on fait ce choix de façon inductive sur u et on trouve une composante $\mathbb{L}_{m+1}$-irréductible de dimension maximale de

$$W_{m+1}^{(k)} \cap (\beta_k \circ \cdots \circ \beta_{m+2})^{-1} \mathcal{Z}(G_1) \cap \ldots \cap (\beta_k \circ \cdots \circ \beta_{m+2})^{-1} \mathcal{Z}(G_u)$$

parmi les composantes contenant $\beta_{m+1} W_m^{(k+1)}$ (elle existe puisque $W_m^{(k)} \subseteq \beta_{m+1}^{-1}(W_{m+1}^{(k)})$ par hypothèse de récurrence et $W_m^{(k+1)} \subseteq W_m^{(k)}$). On a donc d'après le lemme 8.1 et la remarque 8.2

$$\begin{aligned} \deg(W_{m+1}^{(k+1)}) \quad &\leq \quad c_{115} \deg(W_{m+1}^{(k)}) \omega_{\mathbb{L}_k}(P_k, H)^u (C_0 \Delta)^u \left(N(\beta_k) \cdots N(\beta_{m+2})\right)^u \\ &\times \left(\frac{C_0 \Delta}{\log \Delta} \right)^{g_0 . g_0! \delta \rho_{k+1} u} (\log C_0)^{2u}. \end{aligned} \tag{38}$$

Bien entendu, si $k = m+1$ on n'a pas besoin de tirer en arrière les formes $G_1, \dots, G_u$ et le dernier terme à droite dans cette inégalité disparaît simplifiant le calcul.

Lorsque $k > m+1$ on a

$$\begin{aligned} \deg(W_{m+1}^{(k+1)}) \quad &\leq \quad c_{116} \deg(W_{m+1}^{(k)}) \omega_{\mathbb{L}_m}(P_m, H)^u \\ \times \quad &\left(\frac{C_0 \Delta}{\log \Delta} \right)^{\left(2 + 2(k-m) + g_0 . g_0! \delta \rho_{k+1} + [(g_0+1)! - 1] \delta \sum_{j=m+2}^{k} \rho_j \right) u} \end{aligned}$$

et en regardant l'exposant de plus près on a

$$\begin{aligned} &2(k-m) + 2 + g_0 . g_0! \delta \rho_{k+1} + [(g_0+1)! - 1] \delta \sum_{j=m+2}^{k} \rho_j \\ &\leq 2(k-m) + 2 + g_0 . g_0! \delta \rho_{m+3} + (g_0+1)!(k-m-1) \delta \rho_{m+2} - \delta (k-m-1) \rho_{m+2} \\ &\leq (g_0+1)!(k-m-1) \delta \rho_{m+2} + 2(k-m+1) + g_0 g_0! \delta \rho_{m+3} - \delta^3 \rho_{m+3} \\ &\leq (g_0+1)!(g_0-1) \delta \rho_{m+2} \end{aligned}$$

et alors

$$\begin{aligned} \deg(W_{m+1}^{(k+1)}) &\leq c_{117} \deg(W_{m+1}^{(k)}) \omega_{\mathbb{L}_m}(P_m, H)^{d_{m+1}^{(k)} - d_{m+1}^{(k+1)}} \left(\frac{C_0 \Delta}{\log \Delta} \right)^{(g_0-1)(g_0+1)! \delta \rho_{m+2} (d_{m+1}^{(k)} - d_{m+1}^{(k+1)})} \\ &\leq c_{118} \frac{\omega_{\mathbb{L}_m}(P_m, H)^{g_0 - d_{m+1}^{(k+1)}} \deg(H)}{(N_1^{(m+1)})^{\mu(m+1)}} \\ &\qquad \times \left(\frac{C_0 \Delta}{\log \Delta} \right)^{[g_0(g_0+1)! \delta \rho_{m+2} + 2(g_0+1)! \rho_{m+1} \mu(m+1)](g_0 - d_{m+1}^{(k)})}. \end{aligned}$$

Dans le cas $k = m+1$ on vérifie facilement que cette borne est aussi valable.

De cette façon on a construit un triplet $(k+1, \beta^{(k+1)}, W^{(k+1)})$ satisfaisant les conditions demandées.

Deuxième cas. Puisqu'on a utilisé des inégalités très larges dans le premier cas, les calculs dans ce cas sont presque les mêmes. Pour convaincre le lecteur, on expliquera en détail seulement la construction de $W_0^{(k+1)}$. On applique le lemme 6.4 au point P_k et aux ensembles $\mathcal{P}_i^{*(k+1)} = \mathcal{P}_i^{(k+1)} \setminus \mathcal{S}_i$ où

$$\mathcal{S}_i = \{\alpha_p \in \mathcal{P}_i^{(k+1)}, (p, |G_{W_k^{(k)}} : G^{\circ}_{W_k^{(k)}}|) \neq 1\}$$

pour tout $i = 1, \ldots, g_0$. Ces ensembles respectent la condition de la remarque 7.5, puisque le cardinal de $\mathcal{S}_i$ est inférieur à $C_0\Delta$ (comme on vient de le voir dans le cas très ramifié) et donc $|\mathcal{P}_i^{*(k+1)} \cap \Delta_i^{(k+1,\mathrm{pr})}| \geq c_{119} \frac{N_i^{(k+1)}}{\log(N_i^{(k+1)})}$.

Ce lemme nous donne un élément β_{k+1} et une variété W définie sur $\mathbb{L}_k = \mathbb{L}_{k+1}$ passant par le point $\beta_{k+1}(P_k) = P_{k+1}$. On pose alors

$$W_{k+1}^{(k+1)} = W.$$

Cette variété vérifie bien la condition (37) d'après le corollaire 7.2 puisque $\mu(k+1) = 1$ et $2(b^{(k+1)} + g_0 + 1) \leq 2(g_0+1)!\rho_{k+1}$.

On construit $W_0^{(k+1)}$ de la même façon que dans le premier cas, mais cette fois-ci en coupant $W_0^{(k)}$ par le nombre minimal de formes $G_1, \ldots, G_u$ définissant $W_{k+1}^{(k+1)}$ avec multiplicité $\geq c_{120} T_{g_0}^{(k+1)}$ tirées en arrière par F_{k+1}^{-1}. Ensuite, on utilise de nouveau le lemme 8.1 et la remarque 8.2 et on obtient

$$\deg(W_0^{(k+1)}) \leq c_{121} \deg(W_0^{(k)}) \omega_{\mathbb{L}_k}(P_k, H)^u \left(\frac{C_0\Delta}{\log\Delta}\right)^{g_0!\delta\rho_{k+1}u} (N(\beta_{k+1})\cdots N(\beta_1))^u.$$

D'après la remarque 7.4 et la borne (33) on a

$$\begin{aligned}
\deg(W_0^{(k+1)}) &\leq c_{122} \deg(W_0^{(k)}) \omega_{\mathbb{L}_0}(P_0, H)^{(d_0^{(k)} - d_0^{(k+1)})} \\
&\quad \times \left(\frac{C_0\Delta}{\log\Delta}\right)^{\left[2k + g_0!\delta\rho_{k+1} + [(g_0+1)! - 1]\delta \sum_{i=1}^{k+1} \rho_i\right](d_0^{(k)} - d_0^{(k+1)})} \\
&\leq c_{123} \deg(W_0^{(k)}) \omega_{\mathbb{L}_0}(P_0, H)^{(d_0^{(k)} - d_0^{(k+1)})} \left(\frac{C_0\Delta}{\log\Delta}\right)^{[g_0(g_0+1)!\delta\rho_1](d_0^{(k)} - d_0^{(k+1)})} \\
&\leq c_{124} \omega_{\mathbb{L}_0}(P_0, H)^{g_0 - d_0^{(k+1)}} \deg(H) \left(\frac{C_0\Delta}{\log\Delta}\right)^{[g_0(g_0+1)!\delta\rho_1](g_0 - d_0^{(k)})}.
\end{aligned}$$

Pour continuer la construction, on recommence ce procédé cette fois-ci en partant de $(k+1, \beta^{(k+1)}, W^{(k+1)})$ et des ensembles $\mathcal{P}_1^{(k+2)}, \ldots, \mathcal{P}_{g_0}^{(k+2)}$ et ainsi de suite.

Avant de continuer la preuve de la proposition 8.6, on donne un lemme qui utilise la construction qu'on vient de faire et donne en plus une information sur l'ordre $\preceq$.

Lemme 8.9. *Si $k < g_0$ et $(k, \beta^{(k)}, W^{(k)}) \in \mathcal{W}$, alors il existe un triplet $(\tilde{k}, \tilde{\beta}, V) \in \mathcal{W}$ tel que*

$$(\tilde{k}, \tilde{\beta}, V) \prec (k, \beta^{(k)}, W^{(k)}).$$

Proof. On applique le lemme 8.8 à $(k, \beta^{(k)}, W^{(k)})$. Soit $\tilde{k}$ le plus grand entier $\leq g_0$ tel que

$$\forall i < \tilde{k}, \quad W_i^{(g_0)} = W_i^{(\max\{k,i\})}.$$

On pose maintenant $V_i = W_i^{(g_0)}$ pour $0 \leq i \leq \tilde{k}$ et $\tilde{\beta} = (\beta_1, \ldots, \beta_{\tilde{k}})$. On a vu que ce triplet vérifie les conditions $(i), (ii)$ et (iii) de la définition 8.5.

Si $\tilde{k} \leq k$, alors $V_i = W_i^{(k)}$ pour $i \leq \tilde{k} - 1$ et puisque $(k, \beta^{(k)}, W^{(k)}) \in \mathcal{W}$, la condition (iv) de la définition 8.5 est encore vraie pour le uplet $(\tilde{k}, \tilde{\beta}, V)$.

Si $\tilde{k} > k$, la condition (iii) du lemme 8.8 nous dit que $N(\beta_{i+1})$ est premier avec $|G_{W_i^{(i)}} : G^\circ_{W_i^{(i)}}|$ et vu que $V_i = W_i^{(i)}$ pour tout $k \leq i \leq \tilde{k} - 1$ on a donc $N(\beta_{i+1})$ premier avec $|G_{V_i} : G^\circ_{V_i}|$ pour tout i tel que $k \leq i < \tilde{k}$. On a donc $(\tilde{k}, \tilde{\beta}, V) \in \mathcal{W}$.

Voyons maintenant la condition sur l'ordre : deux cas se présentent. Si $\tilde{k} \leq k$ on a

$$\begin{array}{ccccccccc}
W_0^{(k)} & \cdots & W_{\tilde{k}-1}^{(k)} & W_{\tilde{k}}^{(k)} & \cdots & W_k^{(k)} & & & \\
\| & & \| & \cup\!\!\not\parallel & & & & & \\
W_0^{(g_0)} & \cdots & W_{\tilde{k}-1}^{(g_0)} & W_{\tilde{k}}^{(g_0)} & \cdots & \cdots & \cdots & W_{g_0}^{(g_0)} &
\end{array}$$

et on voit clairement que $(\tilde{k}, \tilde{\beta}, V) \prec (k, \beta^{(k)}, W^{(k)})$. D'autre part, si $\tilde{k} > k$ on a le diagramme

$$\begin{array}{cccccccc}
W_0^{(k)} & \cdots & W_k^{(k)} & & & & & \\
\| & & \| & & & & & \\
W_0^{(\tilde{k}-1)} & \cdots & W_k^{(\tilde{k}-1)} & \cdots & W_{\tilde{k}-1}^{(\tilde{k}-1)} & & & \\
\| & & \| & & \| & \cup\!\!\!\not\shortparallel & & \\
W_0^{(g_0)} & \cdots & W_k^{(g_0)} & \cdots & W_{\tilde{k}-1}^{(g_0)} & W_{\tilde{k}}^{(g_0)} & \cdots & W_{g_0}^{(g_0)}
\end{array}$$

et encore une fois il est évident que $(\tilde{k}, \tilde{\beta}, V) \prec (k, \beta^{(k)}, W^{(k)})$.

On peut maintenant démontrer la proposition 8.6.

Proof. (Proposition 8.6) Voyons d'abord que $\mathcal{W}_{\mathbf{0}} \neq \emptyset$; en effet, soit W_0 une variété de H définie sur $\mathbb{L}_0$ passant par P telle que $\omega_{\mathbb{L}}(P, H) = \left(\frac{\deg(W_0)}{\deg H}\right)^{1/\mathrm{codim}_H W_0}$; alors $(0, \emptyset, W_0) \in \mathcal{W}_{\mathbf{0}}$.
Puisque l'ensemble des suites finies d'entiers compris entre 0 et $g_0 - 1$ de longueur au plus g_0 strictement croissantes est fini, il existe alors un élément de $\mathcal{W}_{\mathbf{0}}$ minimal pour $\preceq$. Soit (s, β, W) un tel triplet (on remarque que $s \leq g_0 - 1$ sinon, par le principe des tiroirs, il y aurait un indice i pour lequel $\dim(W_{i-1}) = \dim(W_i)$). On applique le lemme 8.9 à ce triplet et on obtient un nouveau triplet $(\tilde{s}, \tilde{\beta}, V)$ qui appartient à $\mathcal{W}$ et tel que $(\tilde{s}, \tilde{\beta}, V) \prec (s, \beta, W)$, mais (s, β, W) est minimal pour $\preceq$ d'où $(\tilde{s}, \tilde{\beta}, V) \notin \mathcal{W}_{\mathbf{0}}$.

9 Preuve du théorème principal

On donne une proposition qui regroupe les résultats obtenus jusqu'à présent et résout le théorème dans la plupart des cas.

Proposition 9.1. *Soient A une variété abélienne définie sur un corps de nombres K admettant des multiplications complexes, munie d'un fibré $\mathcal{L}_0$ ample et symétrique, $\mathcal{L} = \mathcal{L}_0^{\otimes 4}$ et P un point de $A(\bar{K}) \setminus A(\bar{K})_{\mathrm{tors}}$. Soit H une sous-variété abélienne de A telle que $P \in H$ et P est d'ordre infini modulo toute sous-variété abélienne propre de H. Alors une des deux assertions suivantes est vraie :*

(i). si $\mathbb{L} \subseteq K_{\mathrm{tors}}$ on a

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{1}{\omega_{\mathbb{L}}(P, H)} \left(\frac{\log\log \omega_{\mathbb{L}} \deg_{\mathcal{L}}(H)^2}{C_0 \log \omega_{\mathbb{L}} \deg_{\mathcal{L}}(H)^2}\right)^{\kappa(g_0)}, \tag{39}$$

où $\kappa(g_0) = (2g_0^2(g_0+1)!)^{2g_0}$ et $g_0 = \dim H$;

(ii). $\hat{h}_{\mathcal{L}}(P)$ contredit l'inégalité ci-dessus pour un certain $\mathbb{L}$ et il existe une sous-variété abélienne propre B/K de H, des éléments $\beta_j \in \mathfrak{B}_j$ pour $j = 1, \ldots, g_0$ satisfaisant les hypothèses de la définition 7.1, une suite de sous-corps $\mathbb{L}_j$ associée et un entier i, $0 \leq i \leq g_0 - 1$, tel que $\mathcal{P}_{r(i+1)}^{(i+1)}$ est très ramifié et

$$\tau\beta_{i+1}(P_i) - \beta_{i+1}(P_i) \in B$$

pour un certain $\tau \in \mathrm{Gal}(\bar{K}/\mathbb{L}_{i+1})$ tel que $\tau_{|\mathbb{L}_i} \neq \{\mathrm{Id}\}$ et $P_i = (\beta_i \circ \ldots \circ \beta_1)(P)$. De plus on a l'inégalité

$$\begin{aligned}\deg_{\mathcal{L}}\left(\bigcup_{\substack{\xi \in \ker(\beta_{i+1}) \cap H \\ \tau \in \mathrm{Gal}(\bar{K}/\mathbb{L}_{i+1})}} \tau(P_i + \xi) + B\right) \quad &\leq \quad c_{125} N(\beta_{i+1})^{g_0 - d_i} \omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \\ &\times \deg_{\mathcal{L}}(H) \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2}](g_0 - d_i)}\end{aligned} \tag{40}$$

où $d_i = \dim B$ et $i \leq d_i$.

Proof. Soit $P \in A(\bar{K})$ contredisant (39) (vérifiant (32)). On applique la proposition 8.6 qui nous donne un élément $(s, \beta, W) \in \mathcal{W} \setminus \mathcal{W}_{\mathbf{0}}$. Soit i le plus petit indice tel que

$$d_i := \dim(W_i) = \dim(W_{i+1}).$$

Par minimalité on a donc $i \leq d_i$.

Premier cas. Les ensembles $\mathcal{P}_1^{(i+1)}, \ldots, \mathcal{P}_{g_0}^{(i+1)}$ ont tous peu de grande ramification d'où $\mathbb{L}_i = \mathbb{L}_{i+1}$ et $\mu(i+1) = 1$. Puisque $W_i \subseteq \beta_{i+1}^{-1}(W_{i+1}) \cap H$, on a

$$\bigcup_{\xi \in \ker(\beta_{i+1}) \cap H} W_i + \xi \subseteq \beta_{i+1}^{-1}(W_{i+1}) \cap H.$$

Pour calculer le nombre de translatés différents dans cette union on remarque que deux tels translatés $\xi + W_i$ et $\xi' + W_i$ sont égaux si $\xi - \xi' \in \ker(\beta_{i+1}) \cap G_{W_i} \cap H$. Vu que $N(\beta_{i+1})$ est premier avec $|G_{W_i} : G_{W_i}^{\circ}|$ on sait que le nombre de translatés est $N(\beta_{i+1})^{g_0 - \dim(G_{W_i})}$. D'autre part, $\deg(\beta_{i+1}^{-1}(W_{i+1}) \cap H) = N(\beta_{i+1})^{\operatorname{codim}_H(W_{i+1})} \deg(W_{i+1})$ par la proposition 2.12, d'où

$$N(\beta_{i+1})^{g_0 - \dim(G_{W_i})} \deg(W_i) \leq N(\beta_{i+1})^{g_0 - \dim(W_{i+1})} \deg(W_{i+1})$$

et alors

$$N(\beta_{i+1})^{d_i - s_i} \deg(W_i) \leq \deg(W_{i+1})$$

où $s_i = \dim(G_{W_i})$. Vu que $P_i \in W_i \subseteq H$, par définition on a

$$\omega_{\mathbb{L}_i}(P_i, H) \leq \left(\frac{\deg(W_i)}{\deg H}\right)^{1/\operatorname{codim}_H(W_i)}$$

et donc

$$N(\beta_{i+1})^{d_i - s_i} \omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \deg(H) \leq \deg(W_{i+1}).$$

En utilisant la borne pour le degré de W_{i+1} donnée dans la définition 8.5, cette quantité est majorée par

$$\begin{aligned}
\deg(W_{i+1}) &\leq c_{126} \frac{\omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \deg(H)}{(N_1^{(i+1)})^{\mu(i+1)}} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2} + 2(g_0+1)!\rho_{i+1}\mu(i+1)](g_0 - d_i)} \\
&\leq c_{127} \frac{\omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \deg(H)}{N_1^{(i+1)}} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2} + 2(g_0+1)!\rho_{i+1}](g_0 - d_i)}
\end{aligned}$$

et puisque $d_i \geq s_i$ on a en particulier

$$N_1^{(i+1)} \leq c_{128} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2} + 2(g_0+1)!\rho_{i+1}](g_0 - d_i)}.$$

En remplaçant les paramètres par leur valeur on trouve

$$\begin{aligned}
\left(\frac{C_0 \Delta}{\log \Delta}\right)^{\delta\rho_{i+1}} &\leq c_{129} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2} + 2(g_0+1)!\delta^2\rho_{i+2}](g_0 - d_i)} \\
\left(\frac{C_0 \Delta}{\log \Delta}\right)^{\delta^3\rho_{i+2}} &\leq \left(\frac{C_0 \Delta}{\log \Delta}\right)^{g_0(g_0+1)!\delta\rho_{i+2}(g_0+2\delta)+1}.
\end{aligned}$$

D'après le choix de δ on vérifie facilement que

$$\delta^2 \quad > \quad g_0(g_0+1)!(g_0 + 2\delta)$$

ce qui est absurde.

Deuxième cas. Il existe $r(i+1)$ tel que $\mathcal{P}_{r(i+1)}^{(i+1)}$ a beaucoup de grande ramification. Comme dans le premier cas on a

$$\bigcup_{\xi \in \ker(\beta_{i+1}) \cap H} W_i + \xi \subseteq \beta_{i+1}^{-1}(W_{i+1}) \cap H$$

et on obtient à nouveau

$$N(\beta_{i+1})^{d_i - s_i} \omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \deg(H) \leq \deg(W_{i+1}).$$

Premier sous-cas. Si $s_i < d_i$, on remplace $\deg(W_{i+1})$ par sa valeur et on trouve

$$\begin{aligned}
N(\beta_{i+1}) \omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} &\leq c_{130} \frac{\omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i}}{(N_1^{(i+1)})^{\mu(i+1)}} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2} + 2(g_0+1)!\rho_{i+1}\mu(i+1)](g_0 - d_i)} \\
&\leq c_{131} \omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \left(\frac{C_0 \Delta}{\log \Delta}\right)^{g_0(g_0+1)!\delta\rho_{i+2}(g_0 - d_i)}.
\end{aligned}$$

D'après le lemme de zéros 6.5, β_{i+1} est une isogénie de $\mathcal{P}_{r(i+1)}^{(i+1)}$ et elle est différente de l'identité, d'où $N(\beta_{i+1}) \geq \dfrac{N_1^{(i+1)}}{2}$. On a donc

$$N_1^{(i+1)} \leq c_{132} \left(\frac{C_0\Delta}{\log\Delta}\right)^{g_0^2(g_0+1)!\delta\rho_{i+2}}$$

et en remplaçant

$$\left(\frac{C_0\Delta}{\log\Delta}\right)^{\delta\rho_{i+1}} \leq \left(\frac{C_0\Delta}{\log\Delta}\right)^{g_0^2(g_0+1)!\delta\rho_{i+2}+1}.$$

Ceci implique

$$\delta\rho_{i+2}(\delta^2 - g_0^2(g_0+1)!) \leq 1.$$

D'après le choix de δ et ρ_{i+2} on a

$$\delta\rho_{i+2}(\delta^2 - g_0^2(g_0+1)!) \geq \delta(\delta^2 - \delta + 2) > 1$$

ce qui est contradictoire.

Deuxième sous-cas. Si en revanche $s_i = d_i$, puisque

$$\bigcup_{x\in W_i} G_{W_i} + x \subseteq W_i,$$

on peut écrire

$$W_i = \bigcup_{y\in W_i} G^\circ_{W_i} + y.$$

De plus, $G^\circ_{W_i} \subset H$ et $W_i \subsetneq H$ et donc par minimalité de H, $P_i \notin G^\circ_{W_i}$. La composante connexe de W_i passant par P_i est $G^\circ_{W_i} + P_i$. Puisque W_i est défini sur $\mathbb{L}_i$ alors

$$\bigcup_{\sigma\in\mathrm{Gal}(\bar{K}/\mathbb{L}_i)} G^\circ_{W_i} + \sigma(P_i) \subseteq W_i.$$

De plus, $\beta_{i+1}^{-1}(W_{i+1})$ est stable par action de $\mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i+1})$. On a donc

$$\bigcup_{\substack{\xi\in\ker(\beta_{i+1})\cap H\\ \tau\in\mathrm{Gal}(\bar{K}/K)\\ \tau_{|\mathbb{L}_i}\in\mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i+1})}} G^\circ_{W_i} + \tau(P_i+\xi) \subseteq \beta_{i+1}^{-1}(W_{i+1}) \cap H.$$

Si toutes les composantes $G^\circ_{W_i} + \tau(P_i+\xi)$ sont différentes, on a l'inégalité

$$N(\beta_{i+1})^{g_0-s_i}[\mathbb{L}_i:\mathbb{L}_{i+1}]\deg\left(\bigcup_{\sigma\in\mathrm{Gal}(\bar{K}/\mathbb{L}_i)} G^\circ_{W_i} + \sigma(P_i)\right) \leq N(\beta_{i+1})^{g_0-d_i}\deg(W_{i+1}).$$

D'après le lemme 2.16,

$$[\mathbb{L}_i:\mathbb{L}_{i+1}] \geq \min\left(E_{r(i+1)}^{(i+1)}, \frac{N_{r(i+1)}^{(i+1)}}{2}\right) = E_{r(i+1)}^{(i+1)},$$

alors on a toujours $[\mathbb{L}_i:\mathbb{L}_{i+1}] \geq E_1^{(i+1)} = \left[\left(\frac{C_0\Delta}{\log\Delta}\right)^{\rho_{i+1}}\right]$. En remplaçant $\deg(W_{i+1})$ et $[\mathbb{L}_i:\mathbb{L}_{i+1}]$ on a

$$E_1^{(i+1)}\omega_{\mathbb{L}_i}(P_i,H)^{g_0-d_i} \leq c_{133}\omega_{\mathbb{L}_i}(P_i,H)^{g_0-d_i}\left(\frac{C_0\Delta}{\log\Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2}](g_0-d_i)}$$

d'où

$$\left(\frac{C_0\Delta}{\log\Delta}\right)^{\rho_{i+1}} \leq \left(\frac{C_0\Delta}{\log\Delta}\right)^{[g_0^2(g_0+1)!\delta\rho_{i+2}]+1}.$$

On a donc

$$\rho_{i+1} \leq g_0^2(g_0+1)!\delta\rho_{i+2} + 1$$

et alors

$$\begin{aligned}\delta\rho_{i+2}(\delta-\delta+2) &\leq 1\\ 2\delta\rho_{i+2} &\leq 1,\end{aligned}$$

mais $2\delta\rho_{i+2} \geq 2\delta \geq 8$ ce qui est contradictoire.

Si au contraire il y a des composantes identiques parmi cette union, on est dans le deuxième cas de la proposition avec $B = G^{\circ}_{W_i}$, β_{i+1} et P_i comme ci-dessus.

Avant de terminer la preuve du théorème 2.5, on donne un énoncé qui nous aidera à conclure quand le deuxième cas de la proposition 9.1 se présente.

Théorème 9.2. *Soient P et H comme dans l'énoncé du théorème 2.5 et $\mathbb{L} \subseteq K_{\mathrm{tors}}$. Alors il existe une constante c ne dépendant que de A, K et $\mathcal{L}$ telle que*

$$\hat{h}(P) \geq c\left(\frac{\deg H}{D_{\mathbb{L}}(P)}\right)^{\frac{1}{g_0}}\left(\frac{\log\log D_{\mathbb{L}}(P)\deg(H)^2}{\log D_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa(g_0)},$$

où $\kappa(g_0) = (2g_0^2(g_0+1)!)^{2g_0}$ et $D_{\mathbb{L}}(P) = [\mathbb{L}(P) : \mathbb{L}]$.

Proof. On procède par récurrence sur la dimension de H. Plus précisément, on montre que si le théorème est vrai pour toute sous-variété abélienne C de H telle que $0 \neq C \subsetneq H$ et tout point $y \in C$ d'ordre infini modulo toute sous-variété de torsion de C, alors il est vrai pour H et P comme dans l'énoncé.

- Si H est simple, la condition ci-dessus est vide donc le théorème est vrai.
- Supposons P et $\mathbb{L}$ qui contredisent le théorème avec $\dim H = g_0$. Dans ce cas on reconnaît la condition (5) et on peut appliquer ce que l'on a fait dans le paragraphe 3 et choisir P et $\mathbb{L}$ minimaux. D'après la proposition 9.1, ou bien

$$\begin{aligned}\hat{h}(P) &\geq \frac{1}{\omega_{\mathbb{L}}(P,H)}\left(\frac{\log\log\omega_{\mathbb{L}}\deg(H)^2}{C_0\log\omega_{\mathbb{L}}\deg(H)^2}\right)^{\kappa(g_0)}\\ &\geq c_{134}\left(\frac{\deg H}{D_{\mathbb{L}}(P)}\right)^{\frac{1}{g_0}}\left(\frac{\log\log D_{\mathbb{L}}\deg(H)^2}{\log D_{\mathbb{L}}\deg(H)^2}\right)^{\kappa(g_0)}\end{aligned}$$

  et on a une contradiction (on rappelle que $\omega_{\mathbb{L}}(P,H) \leq \frac{D_{\mathbb{L}}(P)}{\deg(H)}$ par définition), ou bien il existe P_i, β_{i+1} et B satisfaisant (40). Dans ce qui suit par abus de notation on notera $\mathcal{L}$ le fibré donnant la polarisation sur H (qui provient de la restriction à H du fibré $\mathcal{L}$ sur A). Si $\dim B > 0$, il existe une sous-variété abélienne C de H de dimension $g_0 - d_i$ telle que l'application μ soit une isogénie de variétés abéliennes polarisées

$$\begin{aligned}\mu : (B, \mathcal{L}_{|B}) \times (C, \mathcal{L}_{|C}) &\to (H, \mathcal{L})\\ (x,y) &\mapsto x+y,\end{aligned}$$

voir (BL04), 5.3.13, p. 128. Soit $(x,y) \in B \times C$ tel que $\mu(x,y) = P_i$. Par fonctorialité de la hauteur canonique, on sait que

$$\hat{h}_{\mathcal{L}}(P_i) = \hat{h}_{\mu^*\mathcal{L}}(x,y) = \hat{h}_{\mathcal{L}}(x) + \hat{h}_{\mathcal{L}}(y).$$

Puisque C est une sous-variété abélienne de A et y est d'ordre infini modulo toute sous-variété abélienne propre de C, le théorème est vrai pour y. D'autre part,

$$\deg_{\mathcal{L}}\left(\bigcup_{\tau\in\mathrm{Gal}(\bar{K}/\mathbb{L}_{i+1})}\tau(P_i) + B\right) \geq \frac{\deg_{\mathcal{L}} B[\mathbb{L}_{i+1}(y) : \mathbb{L}_{i+1}]}{|\ker\mu|}$$

donc en remplaçant dans (40) on obtient

$$[\mathbb{L}_{i+1}(y) : \mathbb{L}_{i+1}] \leq c_{135}\frac{|\ker\mu|\omega_{\mathbb{L}_i}(P_i,H)^{g_0-d_i}\deg_{\mathcal{L}} H}{\deg_{\mathcal{L}} B}\left(\frac{C_0\Delta}{\log\Delta}\right)^{[g_0(g_0+1)!\delta\rho_{i+2}+g_0!g_0\delta\rho_{i+1}](g_0-d_i)}.$$

On remarque que dans cette inégalité on a utilisé une borne plus précise pour $N(\beta_{i+1})$ que (33) puisqu'il s'agit du cas très ramifié et donc β_{i+1} est un endomorphisme de Frobenius dans un certain $\mathcal{P}_j^{(i+1)}$ et non une composition de plusieurs isogénies. L'hypothèse de récurrence appliquée à y et l'extension $\mathbb{L}_{i+1}$ donne

$$\hat{h}_{\mathcal{L}}(y) \geq c \left(\frac{\deg_{\mathcal{L}} C}{D_{\mathbb{L}_{i+1}}(y)} \right)^{\frac{1}{g_0 - d_i}} \left(\frac{\log\log D_{\mathbb{L}_{i+1}}(y) \deg_{\mathcal{L}}(C)^2}{\log D_{\mathbb{L}_{i+1}}(y) \deg_{\mathcal{L}}(C)^2} \right)^{\kappa(g_0 - d_i)},$$

et donc

$$\begin{aligned} \hat{h}_{\mathcal{L}}(y) &\geq c_{136} \left(\frac{\deg_{\mathcal{L}} C \deg_{\mathcal{L}} B}{|\ker \mu| \omega_{\mathbb{L}_i}(P_i, H)^{g_0 - d_i} \deg_{\mathcal{L}} H} \right)^{1/g_0 - d_i} \\ &\quad \times \left(\frac{\log\log D_{\mathbb{L}_{i+1}}(y) \deg_{\mathcal{L}}(C)^2}{\log D_{\mathbb{L}_{i+1}}(y) \deg_{\mathcal{L}}(C)^2} \right)^{\kappa(g_0 - d_i)} \left(\frac{\log \Delta}{C_0 \Delta} \right)^{g_0(g_0+1)!\delta\rho_{i+2} + g_0! g_0 \delta \rho_{i+1}} \\ &\geq \frac{1}{\omega_{\mathbb{L}_i}(P_i, H)} \left(\frac{\log \Delta}{C_0 \Delta} \right)^{\kappa(g_0 - d_i) + g_0(g_0+1)!\delta\rho_{i+2} + g_0! g_0 \delta\rho_{i+1}}. \end{aligned}$$

D'après les propriétés du degré et la décomposition de $\mu^* \mathcal{L}$ dans $B \times C$, on sait que

$$\deg_{\mathcal{L}} B \times \deg_{\mathcal{L}} C = c_{137} \deg_{\mu^* \mathcal{L}}(B \times C) = c_{137} \deg_{\mathcal{L}}(\mu(B \times C)) |\ker \mu|.$$

On rappelle que P contredit l'inégalité (39) et donc en reprenant les calculs du lemme 8.3 on a

$$\hat{h}(P_i) < \frac{1}{\omega_{\mathbb{L}_i}(P_i, H)} \left(\frac{\log \Delta}{C_0 \Delta} \right)^{\kappa(g_0) - (g_0+1)! i \delta \rho_1 + i \delta \rho_1 - 2i}.$$

De plus, $\hat{h}_{\mathcal{L}}(P_i) \geq \hat{h}_{\mathcal{L}}(y)$. En mettant ces inégalités ensemble on obtient l'inégalité

$$\left(\frac{\log \Delta}{C_0 \Delta} \right)^{\kappa(g_0) - (g_0+1)! i \delta \rho_1 + i \delta \rho_1 - 2i} > \left(\frac{\log \Delta}{C_0 \Delta} \right)^{\kappa(g_0 - d_i) + g_0(g_0+1)!\delta\rho_{i+2} + g_0! g_0 \delta\rho_{i+1}}. \tag{41}$$

On remarque d'après la construction des variétés W_i que $d_i > 0$. De plus la fonction $\kappa(x)$ est croissante, donc

$$\kappa(g_0 - d_i) \leq \kappa(g_0 - 1).$$

En remplaçant $\kappa(x)$ par sa valeur on voit bien que l'equation (41) est absurde.

Si $\dim B = d_i = 0$, puisque $i \leq d_i$, on a $i = 0$. D'après la remarque 6.3 on peut enlever des ensembles $\mathcal{P}_j^{(1)}$ les éléments α_p qui ne vérifient pas $\mathbb{L}(\alpha_p(P)) = \mathbb{L}(P)$ puisque d'après le lemme 3.10 ils sont en nombre inférieur à $c_{138}\Delta$. De plus d'après le lemme 5.2 de (BS04) on peut supposer que A a bonne réduction ordinaire en toutes les places v qui interviennent dans les ensembles $\mathcal{P}_j^{(1)}$. On peut donc appliquer le lemme 3.9 qui nous dit que $\tau(\alpha_p(P)) \neq \alpha_p(P)$ pour tout $\alpha_p \in \mathcal{P}_j^{(1)}$, $j = 1, \ldots, g_0$. D'après la proposition 9.1, on a $\tau(\beta_1(P)) = \beta_1(P)$ et de plus β_1 est un endomorphisme de Frobenius ce qui fournit la contradiction désirée.

On peut maintenant terminer la preuve du théorème 2.5. Soit $P, \mathbb{L}$ et H comme auparavant avec $\dim H = g_0$. D'après la proposition 9.1 deux cas se présentent. Si

$$\hat{h}(P) \geq \frac{c}{\omega_{\mathbb{L}}(P, H)} \left(\frac{\log\log \omega_{\mathbb{L}} \deg(H)^2}{C_0 \log \omega_{\mathbb{L}} \deg(H)^2} \right)^{\kappa(g_0)}$$

le théorème est vrai puisque $\kappa(g_0) \leq \kappa_1(g_0)$.

Sinon, il existe P_i, β_{i+1} et B satisfaisant (40). Voyons d'abord que dans ce cas on a de nouveau $B = \{0\}$. Si ce n'est pas le cas, on peut reprendre la fin de la preuve du théorème 9.2 et on a encore une variété abélienne C et un point $y \in C$ tels que $\mu(x, y) = P_i$. D'après le théorème 9.2

$$\hat{h}(P_i) \geq \hat{h}(y) \geq c_{139} \left(\frac{\deg_{\mathcal{L}} C}{D_{\mathbb{L}_{i+1}}(y)} \right)^{\frac{1}{g_0 - d_i}} \left(\frac{\log\log D_{\mathbb{L}_{i+1}}(y) \deg_{\mathcal{L}}(C)^2}{\log D_{\mathbb{L}_{i+1}}(y) \deg_{\mathcal{L}}(C)^2} \right)^{\kappa(g_0 - d_i)}.$$

De plus, P contredit le théorème 2.5 (sinon il n'y a rien à démontrer) et donc

$$\hat{h}(P) < \frac{1}{\omega_{\mathbb{L}}(P,H)} \left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa_1(g_0)}.$$

Reprenant les calculs du lemme 8.3 on a

$$\hat{h}(P_i) < \frac{1}{\omega_{\mathbb{L}_i}(P_i,H)} \left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa_1(g_0)-(g_0+1)!i\delta\rho_1+i\delta\rho_1-2i}.$$

On en déduit comme auparavant

$$\left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa_1(g_0)-(g_0+1)!i\delta\rho_1+i\delta\rho_1-2i} \geq \left(\frac{\log\Delta}{C_0\Delta}\right)^{\kappa(g_0-1)+g_0(g_0+1)!\delta\rho_{i+2}+g_0!g_0\delta\rho_{i+1}}.$$

Comme on l'a vu plus haut, ceci est impossible.

On a donc $B=0$ et donc $d_i=0$. Puisque $i \leq d_i$, on a $i=0$. En remplaçant dans l'inégalité (40) on a

$$\deg\left(\bigcup_{\substack{\xi\in\ker(\beta_1)\cap H\\ \tau\in\mathrm{Gal}(\bar{K}/K)\\ \tau_{|\mathbb{L}}\in\mathrm{Gal}(\mathbb{L}/\mathbb{L}_1)}} \tau(P+\xi)\right) \leq c_{140}N(\beta_1)^{g_0}\omega_{\mathbb{L}}(P,H)^{g_0}\deg(H)\left(\frac{C_0\Delta}{\log\Delta}\right)^{g_0^2(g_0+1)!\delta\rho_2}$$

et alors en particulier

$$\begin{aligned}[\mathbb{L}(P):\mathbb{L}] &\leq c_{141}\omega_{\mathbb{L}}(P,H)^{g_0}\deg(H)\left(\frac{C_0\Delta}{\log\Delta}\right)^{g_0^2(g_0+1)!\delta\rho_2+\delta\rho_1[(g_0+1)!-1]}\\ &\leq c_{142}\omega_{\mathbb{L}}(P,H)^{g_0}\deg H\left(\frac{C_0\Delta}{\log\Delta}\right)^{(g_0+1)!\delta\rho_1}.\end{aligned}$$

D'après le théorème 9.2 on a

$$\begin{aligned}\hat{h}(P) &\geq c_{143}\left(\frac{\deg(H)}{D_{\mathbb{L}}(P)}\right)^{\frac{1}{g_0}}\left(\frac{\log\log D_{\mathbb{L}}(P)\deg(H)^2}{\log D_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa(g_0)}\\ &\geq c_{144}\left(\frac{\deg(H)}{\omega_{\mathbb{L}}(P,H)^{g_0}\deg H}\right)^{\frac{1}{g_0}}\left(\frac{\log\log\omega_{\mathbb{L}}(P,H)\deg(H)^2}{\log\omega_{\mathbb{L}}(P,H)\deg(H)^2}\right)^{\frac{(g_0+1)!\delta\rho_1}{g_0}}\\ &\qquad\times\left(\frac{\log\log D_{\mathbb{L}}(P)\deg(H)^2}{\log D_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa(g_0)}\\ &\geq \frac{c_{145}}{\omega_{\mathbb{L}}(P,H)}\left(\frac{\log\log\omega_{\mathbb{L}}(P,H)\deg(H)^2}{\log\omega_{\mathbb{L}}(P,H)\deg(H)^2}\right)^{(g_0+1)!\delta\rho_1+\kappa(g_0)}\\ &\geq \frac{c_{145}}{\omega_{\mathbb{L}}(P,H)}\left(\frac{\log\log\omega_{\mathbb{L}}(P)\deg(H)^2}{\log\omega_{\mathbb{L}}(P)\deg(H)^2}\right)^{\kappa_1(g_0)}\end{aligned}$$

ce qu'il fallait démontrer.

Références

[AD99] Francesco Amoroso and Sinnou David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. **513** (1999), 145–179.

[AD00] Francesco Amoroso and Roberto Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272.

[Amo] Francesco Amoroso, *Bogomolov on tori revisited*, prépublication, `http ://hal.archives-ouvertes.fr/hal-00132119`.

[Art86] M. Artin, *Néron models*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 213–230.

[AZ00] Francesco Amoroso and Umberto Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), no. 3, 711–727.

[Bak03] Matthew H. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Not. (2003), no. 29, 1571–1589.

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, seconde ed., vol. 302, Springer-Verlag, Berlin, 2004.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, vol. 21, Springer-Verlag, Berlin, 1990.

[BMZ99] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Internat. Math. Res. Notices (1999), no. 20, 1119–1140.

[BS04] Matthew H. Baker and Joseph H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett. **11** (2004), 377–396.

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986.

[Cha89] Marc Chardin, *Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique*, Bull. Soc. Math. France **117** (1989), no. 3, 305–318.

[Dav91] Sinnou David, *Fonctions thêta et points de torsion des variétés abéliennes*, Compositio Math. **78** (1991), no. 2, 121–160.

[Del07] E. Delsinne, *Autour du problème de Lehmer relatif dans un tore*, Ph.D. thesis, Université de Caen/Basse Normandie, 2007.

[DH00] Sinnou David and Marc Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M*, J. Reine Angew. Math. **529** (2000), 1–74.

[Dob79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401.

[DP98] Sinnou David and Patrice Philippon, *Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes*, Number theory (Tiruchirapalli, 1996), Contemp. Math., vol. 210, Amer. Math. Soc., Providence, RI, 1998, pp. 333–364.

[DP99] ______, *Minorations des hauteurs normalisées des sous-variétés des tores*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 3, 489–543.

[Elk87] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567.

[FM96] Etienne Fouvry and M. Ram Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), no. 1, 81–104.

[Ful84] William Fulton, *Intersection theory*, vol. 2, Springer-Verlag, Berlin, 1984.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Lan83] Serge Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 255, Springer-Verlag, New York, 1983.

[Lau83] Michel Laurent, *Minoration de la hauteur de Néron-Tate*, Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Progr. Math., vol. 38, Birkhäuser Boston, Boston, MA, 1983, pp. 137–151.

[LR85] H. Lange and W. Ruppert, *Complete systems of addition laws on abelian varieties*, Invent. Math. **79** (1985), no. 3, 603–610.

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Springer-Verlag, Berlin, 1976.

[Nér64] André Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Études Sci. Publ.Math. No. **21** (1964), 128.

[Phi86] Patrice Philippon, *Lemmes de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France **114** (1986), no. 3, 355–383.

[Phi95] ______, *Sur des hauteurs alternatives. III*, J. Math. Pures Appl. (9) **74** (1995), no. 4, 345–365.

[Phi96] ______, *Nouveaux lemmes de zéros dans les groupes algébriques commutatifs*, Rocky Mountain J. Math. **26** (1996), no. 3, 1069–1088, Symposium on Diophantine Problems (Boulder, CO, 1994).

[Rat04] Nicolas Ratazzi, *Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe*, Int. Math. Res. Not. (2004), no. 58, 3121–3152.

[Rat08] ______, *Intersection de courbes et de sous-groupes et problèmes de minoration de dernière hauteur dans les variétés abéliennes C.M*, Ann. Inst. Fourier (Grenoble) **58** (2008), no. 5, 1575–1633.

[Rém05] Gaël Rémond, *Intersection de sous-groupes et de sous-variétés I*, Math. Ann. **333** (2005), no. 3, 525–548.

[Rém07] ______, *Intersection de sous-groupes et de sous-variétés II*, J. Inst. Math. Jussieu **6** (2007), no. 2, 317–348.

[RT96] Damien Roy and Jeffrey Lin Thunder, *An absolute Siegel's lemma*, J. Reine Angew. Math. **476** (1996), 1–26.

[Rup] W.M Ruppert, *Torsion points of abelian varieties in abelian extensions*, prépublication, `http ://www.math.uiuc.edu/Algebraic-Number-Theory/0101/tpavae.dvi`.

[Sch91] Wolfgang M. Schmidt, *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, vol. 1467, Springer-Verlag, Berlin, 1991.

[Sil92] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262.

[ST61] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.