Autour du problème de Lehmer relatif dans un tore

Emmanuel Delsinne

Université de Caen/Basse-Normandie
U.F.R. de Sciences
École doctorale SIMEM

T H È S E

présentée par

M. Emmanuel Delsinne

et soutenue le vendredi 14 décembre 2007

en vue de l'obtention du

Doctorat de l'Université de Caen

Spécialité : Mathématiques et leurs applications
(Arrêté du 7 août 2006)

Autour du problème de Lehmer relatif dans un tore

Membres du Jury

M. Francesco Amoroso, professeur à l'Université de Caen *(directeur)*
M. Vincent Bosser, maître de conférences à l'Université de Caen
M. Sinnou David, professeur à l'Université de Paris VI
M. David Masser, professeur à l'Université de Bâle *(rapporteur)*
M. Gaël Rémond, maître de conférences à l'Université de Grenoble I *(rapporteur)*

À mes grands-parents
À mes parents

« Les mathématiques sont un jeu que l'on exerce selon des règles simples en manipulant des symboles ou des concepts qui n'ont en soi, aucune importance particulière. »

David Hilbert

REMERCIEMENTS

De nombreuses personnes ont contribué au bon déroulement de cette thèse. L'occasion m'est ici offerte de leur exprimer ma gratitude.

Tout d'abord, c'est pour moi un grand plaisir de remercier Francesco Amoroso qui m'a proposé ce sujet et m'a encadré tout au long de ces trois années. Sa disponibilité, ses conseils et ses encouragements sont autant de facteurs qui ont largement participé à la réalisation de cette thèse. C'est notamment à l'occasion de fructueuses séances de travail chez lui (où j'étais toujours chaleureusement reçu) qu'est né le deuxième chapitre de cette thèse. Il a su me guider et m'orienter aussi bien dans mes recherches que dans la visite de la Toscane !

J'adresse mes plus sincères remerciements à David Masser et Gaël Rémond pour avoir accepté de rapporter ce travail malgré les brefs délais qui leur ont été imposés. Ils ont effectué cette tâche avec diligence. Leurs remarques pertinentes et leurs idées ont permis d'améliorer la qualité de ce manuscrit et d'envisager de futurs travaux. Par ailleurs, j'ai particulièrement apprécié les discussions amicales que j'ai pu avoir avec Gaël Rémond, que ce soit à Vienne, dans les calanques de Luminy ou lors de promenades dans la forêt d'Oberwolfach.

Je remercie vivement Sinnou David pour l'intérêt qu'il porte à mon travail. C'est un honneur pour moi qu'il participe à ce jury.

Depuis qu'il est à Caen, j'ai pu faire plus ample connaissance avec Vincent Bosser (notamment lors de passionnantes réunions IUFM !) et je lui suis reconnaissant d'avoir accepté de faire partie du jury.

Je tiens à souligner que cette thèse a largement bénéficié des excellentes conditions de travail qu'offre le laboratoire de mathématiques Nicolas Oresme ; j'en remercie tous les membres, chercheurs et personnels administratifs. Je remercie également tous les organisateurs de colloques ou de conférences qui m'ont invité, me permettant ainsi de faire de nombreuses rencontres, d'exposer mes résultats et souvent de découvrir de très beaux sites.

L'ambiance au sein des doctorants du laboratoire a toujours été chaleureuse. Je souhaite remercier tous les thésards avec qui j'ai partagé des moments mathématiques ou RU-culinaires et en particulier...

Corentin, mon cobureau et « frère de hauteur ». Grâce à lui, il régnait toujours une agréable atmosphère de travail dans le bureau 108. C'était un réel plaisir d'échanger nos connaissances en mathématiques ou nos idées sur tout autre sujet.

Marc, son Mac et ses remarques. C'est toujours enrichissant de discuter avec la réincarnation de M. Grévisse. Je garderai d'excellents souvenirs des innombrables et interminables soirées passées chez lui.

Ion et sa 205 qui m'ont souvent conduit (en retard) à la fac. J'ai découvert en lui un véritable ami (qui possède la même montre que moi...).

Erwan, son humour grinçant et ses commentaires acides...

Filippo, roi de la « *nocciola* ». Si notre travail n'en est qu'à l'*antipasto*, j'espère qu'il ira jusqu'au tiramisu...

Camille, Chloé et Émeline qui ont eu le bon goût d'apporter un peu de féminité dans ce milieu.
Si je les remercie, je veux aussi m'excuser de les avoir plus ou moins plumés au poker...

J'ai également une pensée pour mes amis rencontrés lors de mes études à Rennes : Genz, Laurent, Nomo et Tfab. C'est avec eux que les mathématiques devinrent pour moi un réel plaisir. Les nombreux moments inoubliables (et parfois inavouables !) que nous passons ensemble depuis cette époque sont toujours une bonne occasion de décompresser.

J'ai pu compter sur le soutien de ma famille tout au long de mes études. Je remercie du fond du coeur mes parents pour m'avoir encouragé et pour les délicates attentions qu'ils m'ont toujours réservées, ma soeur et mon frère pour les moments de complicité et les fous rires partagés et mes beaux-parents pour leur affection.

Enfin, il n'existe pas de mot à la *hauteur* pour exprimer mes remerciements à Cindy, qui m'a constamment supporté (dans tous les sens du terme) pendant cette thèse. Son intarissable bonne humeur, sa joie de vivre et l'amour qu'elle me porte me comblent de bonheur chaque jour.

TABLE DES MATIÈRES

CHAPITRE 1

INTRODUCTION

> *The following problem arises immediately. If ε is a positive quantity, to find a polynomial of the form*
>
> $$f(x) = x^r + a_1 x^{r-1} + \cdots + a_r$$
>
> *where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 and $1 + \varepsilon$.*

Cette question, posée par D. H. Lehmer en 1933 dans [**Leh33**], est encore ouverte aujourd'hui. Elle est connue sous le nom de *problème de Lehmer*.

1.1. La dimension 1

1.1.1. Mesure de Mahler

Afin de pouvoir reformuler ce problème, nous devons définir *la mesure de Mahler* d'un polynôme.

Définition 1.1. — Soit F un polynôme non nul à coefficients complexes. Notons

$$F(X) = a_d \prod_{i=1}^{d} (X - \alpha_i).$$

On appelle *mesure de Mahler* de F le nombre réel

$$M(F) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Remarquons que la mesure de Mahler est multiplicative : si F_1 et F_2 sont des polynômes non nuls à coefficients complexes, on a $M(F_1F_2) = M(F_1)M(F_2)$. Intéressons-nous aux polynômes à coefficients entiers ; si $F \in \mathbb{Z}[X] \setminus \{0\}$ alors $M(F) \geq 1$ et nous avons la proposition suivante :

Proposition 1.2 **(Kronecker)**. — *Soit F un polynôme irréductible à coefficients entiers. Alors $M(F) = 1$ si et seulement si $F(X) = \pm X$ ou F est un polynôme cyclotomique.*

Il est donc naturel de se demander si, parmi les polynômes à coefficients entiers, la mesure de Mahler peut prendre des valeurs arbitrairement proches de 1 : c'est la question de D. H. Lehmer dans [**Leh33**]. Dans cet article, il fournit le polynôme

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$$

dont la mesure de Mahler vaut environ 1,17628 ; cette valeur reste aujourd'hui la plus petite mesure de Mahler (strictement plus grande que 1) connue (parmi les polynômes à coefficients entiers). Ce fait, puis d'autres résultats que nous citerons dans la suite, suggère que la question de Lehmer admet une réponse négative. C'est pourquoi la conjecture s'énonce de la façon suivante :

Conjecture 1.3 **(Lehmer)**. — *Il existe une constante c strictement positive telle que pour tout polynôme F à coefficients entiers, irréductible, différent de $\pm X$ et non cyclotomique, on a*

$$M(F) \geq 1 + c.$$

Il peut être utile, pour traiter ce problème, d'utiliser la notion de hauteur.

1.1.2. Hauteur d'un nombre algébrique

La notion de hauteur joue un rôle essentiel en approximation diophantienne. D'une part, c'est un outil qui permet de contrôler la « taille » des nombres algébriques et qui, par suite, permet de montrer des résultats de finitude. D'autre part, les hauteurs possèdent des propriétés subtiles qui les rendent intrinsèquement intéressantes. Nous commençons par en rappeler la définition et les premières propriétés (on pourra se référer au chapitre 1 de [**BG06**] pour plus de détails).

Soit K un corps de nombres. On note $\mathcal{M}_K$ l'ensemble des *places* de K, c'est-à-dire l'ensemble des valeurs absolues sur K, à équivalence près. On note K_v (resp. $\mathbb{Q}_v$) le complété de K (resp. $\mathbb{Q}$) par rapport à v. Pour chaque place

de K, on choisit un représentant normalisé de la façon suivante : si v est archimédienne alors v prolonge la valeur absolue usuelle sur $\mathbb{Q}$ ($|a|_v = a$ pour tout a rationnel positif) ; si v est ultramétrique et v divise p, alors v prolonge la valeur absolue p-adique usuelle sur $\mathbb{Q}$ ($|p|_v = p^{-1}$). De cette façon, nous avons la *formule du produit* :

$$\forall \alpha \in K \setminus \{0\}, \quad \prod_{v \in \mathcal{M}_K} |\alpha|_v^{[K_v:\mathbb{Q}_v]} = 1$$

ou encore sous sa forme logarithmique :

$$\forall \alpha \in K \setminus \{0\}, \quad \sum_{v \in \mathcal{M}_K} [K_v : \mathbb{Q}_v] \log(|\alpha|_v) = 0.$$

Remarquons que le produit et la somme précédents sont en réalité finis, étant donné l'égalité $|\alpha|_v = 1$ pour presque toute place v. Nous pouvons maintenant donner la définition de la hauteur d'un nombre algébrique :

Définition 1.4. — Soient α un nombre algébrique et K un corps de nombres le contenant. On appelle *hauteur de Weil (logarithmique)* de α le nombre réel

$$h(\alpha) = \sum_{v \in \mathcal{M}_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |\alpha|_v\}.$$

On montre facilement que cette définition ne dépend pas du corps K. La hauteur possède les propriétés multiplicatives suivantes, pour α et β des nombres algébriques non nuls :

- $h(\alpha\beta) \leq h(\alpha) + h(\beta)$ avec égalité si α ou β est une racine de l'unité ;
- $h(\alpha^l) = |l| h(\alpha)$ pour tout $l \in \mathbb{Z}$.

Par ailleurs, la hauteur d'un nombre algébrique α est liée à la mesure de Mahler. En effet, si F_α est le polynôme minimal de α sur $\mathbb{Z}$, on a

$$h(\alpha) = \frac{\log M(F_\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

Ainsi le théorème de Kronecker se traduit en termes de hauteur : soit α un nombre algébrique non nul, alors $h(\alpha) = 0$ si et seulement si α est une racine de l'unité. Ainsi, de la même façon que pour la mesure de Mahler, il est naturel de s'intéresser à minorer les valeurs prises par la hauteur. Remarquons néanmoins qu'obtenir une minoration absolue strictement positive pour tous les nombres algébriques non nuls qui ne sont pas racine de l'unité est impossible. En effet, il suffit de considérer pour tout entier naturel d le nombre algébrique $\alpha = 2^{1/d}$ dont la hauteur vaut

$$h(2^{1/d}) = \frac{\log 2}{d};$$

elle est donc arbitrairement petite si d est suffisamment grand. Cependant, on peut traduire la conjecture de Lehmer de la façon suivante :

***Conjecture 1.5* (Lehmer).** — *Il existe une constante c strictement positive telle que pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité, on a*

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

1.1.3. Les résultats

Dans la direction de la conjecture de Lehmer, le meilleur résultat inconditionnel à ce jour est un théorème dû à Dobrowolski [**Dob79**], qui affirme que la conjecture de Lehmer est vraie « à un ε près » :

***Théorème 1.6* (Dobrowolski).** — *Il existe une constante c strictement positive telle que pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité,*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \left(\frac{\log\log(3[\mathbb{Q}(\alpha) : \mathbb{Q}])}{\log(3[\mathbb{Q}(\alpha) : \mathbb{Q}])} \right)^3.$$

De plus, dans certains cas, cette conjecture est vraie. Sous certaines hypothèses, il existe même des résultats bien plus forts que celui prédit par la conjecture de Lehmer. Remarquons tout d'abord que si α n'est pas un entier algébrique, alors

$$h(\alpha) \geq \frac{\log 2}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

Citons ensuite le résultat de C. Smyth [**Smy71**]. Un nombre algébrique non nul est dit *réciproque* si l'ensemble de ses conjugués (sur $\mathbb{Q}$) est stable par l'application $x \mapsto x^{-1}$. En d'autres termes, cela signifie que son polynôme minimal sur $\mathbb{Z}$ est réciproque, c'est-à-dire invariant par l'application $F(X) \mapsto X^{\deg(F)} F(X^{-1})$. C. Smyth montre alors

***Théorème 1.7* (Smyth).** — *Soit α un nombre algébrique non nul non réciproque. Alors*

$$h(\alpha) \geq \frac{\log \theta}{[\mathbb{Q}(\alpha) : \mathbb{Q}]},$$

où θ désigne la racine réelle du polynôme $X^3 - X - 1$.

Remarquons que cette minoration est optimale car on a égalité lorsque $\alpha = \theta$. Pour montrer la conjecture de Lehmer, il suffit donc de s'intéresser aux entiers algébriques réciproques.

De plus, sous certaines propriétés arithmétiques, il existe des minorations bien plus fortes, indépendantes du degré de α. Par exemple, A. Schinzel montre dans [**Sch73**] le résultat suivant.

Théorème 1.8 **(Schinzel)**. — *Soit K un corps totalement réel ou une extension quadratique imaginaire d'un tel corps. Soit $\alpha \in K^*$ tel que $|\alpha| \neq 1$. Alors*

$$h(\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2}.$$

Dans [**AmNu07**], F. Amoroso et F. A. E. Nuccio montrent que l'on ne peut faire l'économie de l'hypothèse $|\alpha| \neq 1$. Néanmoins, dans le cas des extensions abéliennes de $\mathbb{Q}$ (qui entrent dans le cadre de ce théorème) nous avons le théorème suivant, issu de [**AmDv00**].

Théorème 1.9 **(Amoroso-Dvornicich)**. — *Soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Soit $\alpha \in \mathbb{L}^*$ et supposons que α n'est pas une racine de l'unité. Alors*

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

Cette minoration admet une généralisation non triviale aux extensions abéliennes d'un corps de nombres K quelconque, la hauteur n'étant plus minorée par une constante (absolue) mais par un réel ne dépendant que du corps de base K : c'est un résultat de F. Amoroso et U. Zannier. Il s'agit en fait d'un cas particulier du théorème suivant.

Théorème 1.10 **(Amoroso-Zannier)**. — *Soit K un corps de nombres. Il existe un nombre réel strictement positif $c(K)$ ne dépendant que de K tel que pour toute extension abélienne $\mathbb{L}$ de K et pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité, on a*

$$h(\alpha) \geq \frac{c(K)}{[\mathbb{L}(\alpha) : \mathbb{L}]} \left(\frac{\log\log(5[\mathbb{L}(\alpha) : \mathbb{L}])}{\log(2[\mathbb{L}(\alpha) : \mathbb{L}])} \right)^{13}.$$

Dans le cas où $K = \mathbb{Q}$, ce théorème est un analogue du théorème d'E. Dobrowolski où le corps $\mathbb{Q}$ est remplacé par une extension abélienne. Il conduit ainsi à faire la conjecture suivante.

Conjecture 1.11. — *Il existe une constante c strictement positive telle que pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité,*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}]},$$

où $\mathbb{Q}^{\mathrm{ab}}$ désigne l'extension abélienne maximale de $\mathbb{Q}$.

C'est la conjecture de Lehmer dite « relative ». Plus généralement, le problème qui consiste à minorer la hauteur d'un nombre algébrique en fonction de son degré sur une extension abélienne est appelé ***problème de Lehmer relatif***.

À propos du théorème 1.10, il est naturel de se demander comment varie le réel $c(K)$ en fonction de K. Une conjecture optimiste consisterait à suggérer que $c(K)$ est inversement proportionnel au degré $[K:\mathbb{Q}]$, ce qui conduirait à la généralisation suivante de la conjecture de Lehmer :

$$h(\alpha) \geq \frac{c}{[K^{\mathrm{ab}}(\alpha):K^{\mathrm{ab}}][K:\mathbb{Q}]},$$

avec c une constante (absolue) et K^{ab} l'extension abélienne maximale de K. Malheureusement, cette inégalité est fausse comme le montre l'exemple suivant. Soient m un entier naturel non nul et n le produit des m premiers nombres premiers. Soit K le corps engendré par les racines n-ièmes de l'unité. Alors $[K:\mathbb{Q}] = \phi(n)$ et par le choix de n, on a

$$n \geq c_1 [K:\mathbb{Q}] \log\log[K:\mathbb{Q}],$$

où c_1 est un réel strictement positif. Considérons maintenant $\alpha = 2^{1/n}$. Alors $\alpha \in K^{\mathrm{ab}}$ donc $[K^{\mathrm{ab}}(\alpha):K^{\mathrm{ab}}] = 1$ et

$$h(\alpha) = \frac{\log 2}{n} \leq \frac{c_1^{-1}\log 2}{[K^{\mathrm{ab}}(\alpha):K^{\mathrm{ab}}][K:\mathbb{Q}]\log\log[K:\mathbb{Q}]}.$$

Ceci implique donc que $c(K)$ est au moins en $([K:\mathbb{Q}]\log\log[K:\mathbb{Q}])^{-1}$. Avec F. Amoroso, nous montrons dans [**AmDe07**] qu'en supposant l'hypothèse de Riemann généralisée (GRH), nous pouvons prendre

$$c(K) = \frac{c}{([K:\mathbb{Q}](\log(3|\Delta_K|)))^3},$$

où Δ_K est le discriminant de K. Plus exactement nous obtenons les théorèmes suivants.

Théorème 1.12. — *On suppose GRH. Soient K un corps de nombres, d son degré et Δ_K son discriminant. Soit α un nombre algébrique non nul qui n'est pas une racine de l'unité. Alors pour toute extension abélienne $\mathbb{L}$ de K, on a*

$$h(\alpha) \geq \frac{c}{D}\min\left(\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2}, \frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right),$$

où c est une constante (absolue) strictement positive, $D = [\mathbb{L}(\alpha) : \mathbb{L}]$ et $\lambda = (\log(3|\Delta_K|))^2 \max((\log\log(16|\Delta_K|))^2, (\log(3d))^4)$. En particulier, on a

$$h(\alpha) \geq \frac{c}{D} \frac{\log\log(5D)^4}{d^3\delta^2 \log(2\delta D)^2 \log(2D)^2},$$

où $\delta = \log(3|\Delta_K|)$.

Nous avons besoin, dans la démonstration de ce théorème, d'une estimation du terme reste dans le théorème des idéaux premiers de K. Sous GRH, un résultat de J. C. Lagarias et A. M. Odlyzko (voir le théorème 1.1 de [**LO77**]) fournit une très bonne estimation de ce reste. Sans GRH, les estimations de ce reste sont nettement moins bonnes (voir les théorèmes 1.3 et 1.4 de [**LO77**]) et ne permettent pas de trouver une dépendance polynomiale en Δ_K. Nous utilisons alors une estimation due à Friedlander (voir [**Fri80**]), qui donne une version moins précise du théorème des idéaux premiers, avec en contrepartie une meilleure dépendance en Δ_K.

Théorème 1.13. — *Soient K un corps de nombres, d son degré et Δ_K son discriminant. Soit α un nombre algébrique non nul qui n'est pas une racine de l'unité. Alors pour toute extension abélienne $\mathbb{L}$ de K, on a*

$$h(\alpha) \geq \frac{(2g(d)\Delta_K)^{-c}}{D} \frac{\log\log(5D)^3}{\log(2D)^4}$$

où c est une constante (absolue) strictement positive, $D = [\mathbb{L}(\alpha) : \mathbb{L}]$ et $g(d) = 1$ s'il existe une tour d'extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m = K,$$

avec K_i/K_{i-1} galoisienne pour $i = 1, \ldots, m$, et $g(d) = d!$ sinon.

Remarquons que nous améliorons nettement (avec ou sans GRH) l'exposant dans le terme en « log » par rapport au théorème 1.10. Par ailleurs, comme dans [**AmZa00**], les constantes qui interviennent dans les énoncés sont effectivement calculables. Ces deux théorèmes font l'objet du chapitre 2 de la thèse. Nous soulevons alors la question suivante : peut-on se passer de la dépendance en le discriminant de K dans $c(K)$? En d'autres termes : la hauteur d'un nombre algébrique non nul qui n'est pas une racine de l'unité et qui appartient à une extension abélienne de K peut-elle être minorée en fonction uniquement du degré de K sur $\mathbb{Q}$?

1.2. La dimension supérieure

1.2.1. Le tore

À cause des propriétés multiplicatives de la hauteur, il est souvent utile de considérer l'ensemble des nombres algébriques non nuls en tant que groupe multiplicatif $\mathbb{G}_{\mathrm{m}}(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}}^{\times}$. Le paragraphe précédent traitait de la minoration de la hauteur dans $\mathbb{G}_{\mathrm{m}} = \mathbb{G}_{\mathrm{m}}^1$. Ce type de problème possède une généralisation en dimension supérieure, c'est-à-dire dans $\mathbb{G}_{\mathrm{m}}^n$ ($n \in \mathbb{N}^*$), le *groupe multiplicatif* (ou *tore*) *de dimension* n.

Définition 1.14. — Soit n un entier naturel non nul. Le *tore* $\mathbb{G}_{\mathrm{m}}^n$ est l'ouvert de Zariski de l'espace affine $\mathbb{A}^n$ défini par

$$x_1 \cdots x_n \neq 0$$

muni de la structure de groupe multiplicatif

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in (\mathbb{G}_{\mathrm{m}}^n)^2, \quad \boldsymbol{xy} = (x_1 y_1, \cdots, x_n y_n)$$

dont l'élément neutre est $(1, \ldots, 1)$.

Soit $m \in \mathbb{N}^*$. Nous noterons $[m]$ le morphisme de multiplication par m donné par

$$\forall \boldsymbol{x} \in \mathbb{G}_{\mathrm{m}}^n, \quad [m]\boldsymbol{x} = (x_1^m, \cdots, x_n^m).$$

Le noyau de ce morphisme, que nous noterons $\ker[m]$, est constitué des *points de m-torsion*. Dans le cas de $\mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$, il s'agit de l'ensemble des points dont les coordonnées sont des racines m-ièmes de l'unité. Un *sous-groupe algébrique* de $\mathbb{G}_{\mathrm{m}}^n$ est un sous-groupe qui est fermé (dans $\mathbb{G}_{\mathrm{m}}^n$) pour la topologie de Zariski et un *sous-tore* de $\mathbb{G}_{\mathrm{m}}^n$ est un sous-groupe algébrique qui est géométriquement irréductible. Un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ est isomorphe (en tant que groupe algébrique) à $\mathbb{G}_{\mathrm{m}}^r$ pour un certain entier $r \leq n$ (voir le corollaire 3.2.8 de [**BG06**]). Si V est un sous-ensemble algébrique de $\mathbb{G}_{\mathrm{m}}^n$ et $\boldsymbol{\alpha}$ un point de $\mathbb{G}_{\mathrm{m}}^n$, nous noterons $\boldsymbol{\alpha}V$ le *translaté* de V par $\boldsymbol{\alpha}$:

$$\boldsymbol{\alpha}V = \{\boldsymbol{\alpha}\boldsymbol{x}, \boldsymbol{x} \in V\},$$

et si $m \in \mathbb{N}^*$, nous noterons $[m]V$ l'image de V par le morphisme de multiplication par m :

$$[m]V = \{\boldsymbol{x}^m, \boldsymbol{x} \in V\}.$$

Nous appellerons *variété de torsion* une réunion de translatés de sous-tores propres[1] par des points de torsion.

Afin de définir la hauteur d'un point de $\mathbb{G}_{\mathrm{m}}^n$, il est nécessaire de considérer un plongement dans un certain espace projectif. La hauteur d'un point de $\mathbb{G}_{\mathrm{m}}^n$ sera alors la hauteur projective de son image par ce plongement. Dans toute la suite, nous considérerons le plongement naturel

$$\begin{array}{rccc} \iota : & \mathbb{G}_{\mathrm{m}}^n & \hookrightarrow & \mathbb{P}_n \\ & \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) & \mapsto & (1 : \alpha_1 : \ldots : \alpha_n). \end{array}$$

La hauteur correspondante est alors donnée par

Définition 1.15. — Soient $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ et K un corps de nombres contenant $\alpha_1, \ldots, \alpha_n$. On appelle *hauteur de Weil (logarithmique)* de $\boldsymbol{\alpha}$ le nombre réel

$$h(\boldsymbol{\alpha}) = \sum_{v \in \mathcal{M}_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |\alpha_1|_v, \ldots |\alpha_n|_v\}.$$

Comme en dimension 1, la hauteur possède des propriétés intéressantes, compatibles avec la structure de groupe du tore. Citons tout d'abord la généralisation du théorème de Kronecker : un point α est de hauteur nulle si et seulement si c'est un point de torsion, c'est-à-dire si ses coordonnées sont des racines de l'unité. De plus, si m un entier naturel, alors $h(\boldsymbol{\alpha}^m) = mh(\boldsymbol{\alpha})$. Si m est un entier négatif, nous n'avons plus l'égalité mais simplement $h(\boldsymbol{\alpha}^m) \leq n|m|h(\boldsymbol{\alpha})$. Enfin, pour tout $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in (\mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}}))^2$,

$$h(\boldsymbol{\alpha}\boldsymbol{\beta}) \leq h(\boldsymbol{\alpha}) + h(\boldsymbol{\beta}),$$

ce qui implique en particulier que pour tout point de torsion $\boldsymbol{\zeta}$, on a

$$h(\boldsymbol{\zeta}\boldsymbol{\alpha}) = h(\boldsymbol{\alpha}).$$

1.2.2. Le problème de Lehmer pour les points

Pour minorer la hauteur d'un point en dimension supérieure, le degré n'est pas le bon invariant à considérer. Il en existe un plus fin, qui tient compte de l'aspect géométrique du problème : l'*indice d'obstruction*.

[1] Nous dirons qu'un sous-ensemble algébrique de $\mathbb{G}_{\mathrm{m}}^n$ est « propre » s'il est strictement inclus dans $\mathbb{G}_{\mathrm{m}}^n$.

Définition 1.16. — Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ et K un sous-corps de $\bar{\mathbb{Q}}$. On appelle *indice d'obstruction* de $\boldsymbol{\alpha}$ relativement à K (ou sur K) et on note $\omega_K(\boldsymbol{\alpha})$ le plus petit degré[(2)] d'une hypersurface de $\mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ définie sur K contenant $\boldsymbol{\alpha}$.

Remarquons tout d'abord que l'indice d'obstruction est bien une généralisation du degré, dans la mesure où $\omega_K(\alpha) = [K(\alpha) : K]$ pour tout $\alpha \in \mathbb{G}_{\mathrm{m}}(\bar{\mathbb{Q}})$. Plus généralement, en dimension supérieure, un argument d'algèbre linéaire fournit la majoration

$$\forall \boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}}), \quad \omega_K(\boldsymbol{\alpha}) \leq n[K(\boldsymbol{\alpha}) : K]^{1/n}.$$

Dans [**AmDa99**], F. Amoroso et S. David proposent une conjecture généralisant la conjecture de Lehmer :

Conjecture 1.17. — *Pour tout entier naturel non nul n, il existe un nombre réel strictement positif $c(n)$ tel que, pour tout $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

$$h(\boldsymbol{\alpha}) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(\boldsymbol{\alpha})}.$$

Rappelons que $\alpha_1, \ldots, \alpha_n$ sont dits multiplicativement indépendants si

$$\forall (a_1, \ldots, a_n) \in \mathbb{Z}^n, \ \prod_{i=1}^{n} \alpha_i^{a_i} = 1 \quad \Longrightarrow \quad (a_1, \ldots, a_n) = (0, \ldots, 0).$$

Cette hypothèse est absolument essentielle comme le montre l'exemple suivant. Soient d un entier naturel non nul et $\boldsymbol{\alpha}_d = (2^{1/d}, \ldots, 2^{1/d}) \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$. Alors, si $n \geq 2$, on a

$$\omega_{\mathbb{Q}}(\boldsymbol{\alpha}_d) = 1 \quad \text{et} \quad h(\boldsymbol{\alpha}_d) = \frac{\log 2}{d}.$$

de sorte qu'il est impossible de minorer la hauteur de $\boldsymbol{\alpha}_d$ en fonction uniquement de son indice d'obstruction sur $\mathbb{Q}$. Ainsi, il est impossible d'obtenir une telle minoration pour *tous* les points de $\mathbb{G}_{\mathrm{m}}^n$ qui ne sont pas de torsion. Néanmoins, l'hypothèse « $\boldsymbol{\alpha}$ est à coordonnées multiplicativement indépendante » est équivalente à « $\boldsymbol{\alpha}$ n'appartient à aucun translaté de sous-tore propre par un point de torsion » ; dans le cas où il existe un translaté de sous-tore propre par un point de torsion qui contient $\boldsymbol{\alpha}$, le problème peut alors se ramener, par paramétrage du sous-tore, au problème de Lehmer dans $\mathbb{G}_{\mathrm{m}}^r$ où r est la dimension du sous-tore.

[(2)] Le plongement $\mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}_n$ ayant été fixé, on entend par degré d'une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ le degré de son adhérence de Zariski dans $\mathbb{P}_n$.

F. Amoroso et S. David montrent dans [**AmDa99**] que cette conjecture est vraie « à un ε près ».

Théorème 1.18 **(Amoroso-David)**. — *Pour tout entier naturel non nul n, il existe un nombre réel strictement positif $c(n)$ tel que, pour tout $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

$$h(\boldsymbol{\alpha}) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(\boldsymbol{\alpha})} \log(3\omega_{\mathbb{Q}}(\boldsymbol{\alpha}))^{-\kappa(n)},$$

avec $\kappa(n) = 2n(n+1)!^n - 1$.

Par analogie avec la dimension 1, on peut également énoncer le problème de Lehmer relatif en dimension supérieure pour les points :

Conjecture 1.19. — *Pour tout entier naturel non nul n, il existe un nombre réel strictement positif $c(n)$ tel que, pour tout $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

$$h(\boldsymbol{\alpha}) \geq \frac{c(n)}{\omega_{\mathbb{Q}^{\mathrm{ab}}}(\boldsymbol{\alpha})}.$$

F. Amoroso et S. David obtiennent dans [**AmDa04**] un résultat « semi-relatif ».

Théorème 1.20 **(Amoroso-David)**. — *Soit n un entier naturel non nul. Posons*

$$\kappa(n) = 2n(n+1)!^n - 1 \quad \text{et} \quad \mu(n) = 2n(n+1)!^n + (n+1)!^{n-1} - 2.$$

Il existe un nombre réel strictement positif $c(n)$ tel que la propriété suivante soit vraie.

Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ et K une extension cyclotomique de $\mathbb{Q}$. Si

$$h(\boldsymbol{\alpha}) < c(n)^{-1}\omega_K(\boldsymbol{\alpha})^{-1} \left(\log(3[K:\mathbb{Q}]\omega_K(\boldsymbol{\alpha}))\right)^{-\kappa(n)},$$

alors il existe une sous-variété de torsion B définie sur K et contenant $\boldsymbol{\alpha}$ telle que

$$(\deg B)^{1/\mathrm{codim}(B)} \leq c(n)\omega_K(\boldsymbol{\alpha}) \left(\log(3[K:\mathbb{Q}]\omega_K(\boldsymbol{\alpha}))\right)^{\mu(n)}.$$

Remarquons que ce théorème est un peu plus précis que le précédent dans la mesure où il fournit une borne sur le degré de la variété de torsion contenant $\boldsymbol{\alpha}$ dans le cas où la hauteur de $\boldsymbol{\alpha}$ est petite. Cependant, une telle minoration n'est pas satisfaisante si le degré $[K:\mathbb{Q}]$ est pathologiquement grand par rapport à $\omega_K(\boldsymbol{\alpha})$ (plus précisément si $[K:\mathbb{Q}] \gg \exp(\omega_K(\boldsymbol{\alpha}))$). Il est donc souhaitable d'avoir un énoncé ne faisant pas intervenir ce degré. Pour obtenir

un tel théorème, nous sommes contraint de faire une hypothèse technique sur $\boldsymbol{\alpha}$:

Hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$ **:** *Soient* $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ *et* $\mathbb{L}$ *une extension abélienne de* $\mathbb{Q}$*. Alors pour tout sous-tore* H *de* $\mathbb{G}_{\mathrm{m}}^n$*, pour tout entier naturel* l*, pour tout nombre premier* p *ramifié dans* $\mathbb{L}$ *et pour tout conjugué*[3] $\tilde{\boldsymbol{\alpha}}$ *de* $\boldsymbol{\alpha}$*, on a*

$$(\tilde{\boldsymbol{\alpha}}\boldsymbol{\alpha}^{-1})^l \notin H \Longrightarrow (\tilde{\boldsymbol{\alpha}}\boldsymbol{\alpha}^{-1})^{lp} \notin H. \tag{1.1}$$

En d'autres termes, cette hypothèse affirme que si $\boldsymbol{\alpha}^l$ et $\tilde{\boldsymbol{\alpha}}^l$ sont indépendants modulo H alors il en est de même pour leurs puissances p-ièmes. En réalité, nous utilisons une version plus faible de cette hypothèse. En particulier, l'assertion (1.1) n'est supposée que pour des sous-tores H, des entiers l et des premiers p dont nous contrôlons degrés et valeurs (en fonction de $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$). De plus, ceci ne vaut que pour certains conjugués $\tilde{\boldsymbol{\alpha}}$ de $\boldsymbol{\alpha}$. Nous pouvons maintenant énoncer notre résultat.

Théorème 1.21. — *Soit* n *un entier naturel non nul. Posons*

$$\kappa(n) = \big(2(n+1)^2(n+1)!\big)^n \quad \textit{et} \quad \mu(n) = 2\kappa(n).$$

Il existe un nombre réel strictement positif $c(n)$ *ne dépendant que de* n *et effectivement calculable tel que la propriété suivante soit vraie.*

Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ *et soit* $\mathbb{L}$ *une extension abélienne de* $\mathbb{Q}$*. Supposons que l'hypothèse* $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$ *soit satisfaite. Si*

$$h(\boldsymbol{\alpha}) \leq c(n)^{-1}\omega_{\mathbb{L}}(\boldsymbol{\alpha})^{-1}(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{-\kappa(n)},$$

alors il existe une sous-variété de torsion B *définie sur* $\mathbb{L}$ *et contenant* $\boldsymbol{\alpha}$ *telle que*

$$(\deg B)^{1/\mathrm{codim}(B)} \leq c(n)\omega_{\mathbb{L}}(\boldsymbol{\alpha})(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{\mu(n)}.$$

La démonstration de ce théorème sera effectuée au chapitre 4. Bien entendu, il serait souhaitable par la suite d'obtenir un énoncé du même type en se passant de l'hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$.

[3] On dit que $\tilde{\boldsymbol{\alpha}} = (\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$ est un conjugué de $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ s'il existe $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que pour tout $i \in [\![1, n]\!]$ de $\boldsymbol{\alpha}$, on a $\tau\alpha_i = \alpha_i$.

1.2.3. Le problème de Lehmer pour les variétés

Il est également possible de définir la hauteur d'une sous-variété d'un tore. Dans [**Phi91**], P. Philippon définit, *via* les formes de Chow, la notion de *hauteur normalisée* pour les sous-variétés d'un tore. L'idée est de fixer, dans un premier temps, une hauteur locale (*via* une norme) puis globale pour les polynômes, et de définir la hauteur h d'une variété projective comme la hauteur d'une de ses formes de Chow. On obtient alors, *via* le plongement de $\mathbb{G}_{\mathrm{m}}^n$ dans un espace projectif, la hauteur normalisée $\hat{h}$ par un procédé limite à la Néron-Tate :

$$\hat{h}(V) = \lim_{m\to\infty} \frac{h([m]V)\deg(V)}{m\deg([m]V)}.$$

Dans le cas où V est un point de $\mathbb{G}_{\mathrm{m}}^n$, on peut montrer que sa hauteur normalisée coïncide avec la hauteur de Weil définie précédemment.

L. Szpiro a également introduit le *minimum essentiel* de V, noté $\hat{\mu}^{\mathrm{ess}}(V)$, comme la borne inférieure des nombres réels $\theta > 0$ tels que l'ensemble des points $P \in V(\bar{\mathbb{Q}})$ de hauteur normalisée majorée par θ soit Zariski-dense dans V. Si V est $\bar{\mathbb{Q}}$-irréductible, on dispose alors de la relation suivante, montrée dans [**Zha95a**] et [**Zha95b**] :

$$\frac{\hat{h}(V)}{(\dim(V)+1)\deg(V)} \leq \hat{\mu}^{\mathrm{ess}}(V) \leq \frac{\hat{h}(V)}{\deg(V)} \ .$$

Le minimum essentiel et la hauteur normalisée ont la propriété remarquable suivante, montré encore par S. Zhang (voir [**Zha92**]) : $\hat{\mu}^{\mathrm{ess}}(V) = 0$ (et donc $\hat{h}(V) = 0$) si et seulement si V est une variété de torsion.

Il est donc naturel de chercher à minorer le minimum essentiel (ou la hauteur normalisée) d'une variété qui n'est pas de torsion.

Une telle minoration va dépendre des caractéristiques géométriques de la variété, par exemple son degré. Cependant, si l'on n'impose aucune condition géométrique sur la variété, il faudra également tenir compte de son corps de définition. En effet, soit H un sous-groupe de $\mathbb{G}_{\mathrm{m}}^n$ et soit $\boldsymbol{\alpha}_d$ une suite de points non de torsion dont la hauteur tend vers 0 (par exemple $\boldsymbol{\alpha}_d = (2^{1/d}, \ldots, 2^{1/d})$). Alors les variétés $V_d = \boldsymbol{\alpha}_d H$ ont toutes même degré $\deg(H)$ mais la suite de leurs minima essentiels $\hat{\mu}^{\mathrm{ess}}(V_d) \leq h(\boldsymbol{\alpha}_d)$ converge vers 0.

Comme pour les points, le bon invariant à considérer est l'indice d'obstruction :

Définition 1.22. — Soient V un sous-ensemble algébrique de $\mathbb{G}_{\mathrm{m}}^n$ et K un sous-corps de $\bar{\mathbb{Q}}$. On appelle *indice d'obstruction* de V relativement à K (ou

sur K) et on note $\omega_K(V)$ le plus petit degré d'une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie sur K contenant V.

Si V est une variété[4], nous avons, comme pour les points une relation entre $\omega_K(V)$ et son degré (voir le corollaire 2 et l'exemple 1 du chapitre 1 de [**Cha88**]) :

$$\omega_K(V) \leq n(\deg V)^{1/n}.$$

Nous pouvons alors énoncer la généralisation du problème de Lehmer en dimension supérieure.

Conjecture 1.23. — *Pour tout entier naturel non nul n, il existe un nombre réel strictement positif $c(n)$ tel que, pour toute sous-variété V de $\mathbb{G}_{\mathrm{m}}^n$ qui n'est contenue dans aucune sous-variété de torsion, on a*

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(V)}.$$

Dans [**AmDa01**], F. Amoroso et S. David montrent que le théorème 1.18 (pour les points) implique que cette conjecture est vraie « à un ε près » :

Théorème 1.24 **(Amoroso-David)**. — *Pour tout entier naturel non nul n, il existe un nombre réel strictement positif $c(n)$ tel que, pour toute sous-variété V de $\mathbb{G}_{\mathrm{m}}^n$ qui n'est contenue dans aucune sous-variété de torsion, on a*

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(V)}(\log(3\omega_{\mathbb{Q}}(V)))^{-\kappa(n)},$$

avec $\kappa(n) = 2n(n+1)!^n - 1$.

Bien entendu il est possible de faire une conjecture pour le problème de Lehmer relatif pour les sous-variétés des tores :

Conjecture 1.25. — *Pour tout entier naturel non nul n, il existe un nombre réel strictement positif $c(n)$ tel que, pour toute sous-variété V de $\mathbb{G}_{\mathrm{m}}^n$ qui n'est contenue dans aucune sous-variété de torsion, on a*

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}^{\mathrm{ab}}}(V)}.$$

[4] Nous utiliserons la terminologie « variété » pour désigner un ensemble algébrique irréductible sur son corps de définition.

À la manière de [**AmDa01**], un résultat du même type que le théorème 1.21 sans l'hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$ permettrait de démontrer que cette conjecture est vraie « à un ε près ». Néanmoins, si V est une hypersurface, nous pouvons montrer directement ce résultat.

Théorème 1.26. — *Pour tout entier naturel non nul n, il existe des nombres réels strictement positifs $c(n)$ et $\kappa(n)$ tels que, pour toute hypersurface V de $\mathbb{G}_{\mathrm{m}}^n$ qui n'est contenue dans aucune sous-variété de torsion, on a*

$$\hat{\mu}^{\mathrm{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}^{\mathrm{ab}}}(V)}(\log(3\omega_{\mathbb{Q}^{\mathrm{ab}}}(V)))^{-\kappa(n)}.$$

Nous donnons une démonstration directe de ce résultat et nous montrons qu'il peut également se déduire d'une minoration de type géométrique (problème de Bogomolov) et du théorème 1.10.

Enfin, signalons qu'il existe des conjectures et des résultats analogues dans le cadre des variétés abéliennes. Le lecteur pourra se référer à [**Rat04**] pour un panorama sur le problème de Lehmer abélien.

1.3. Contenu de la thèse

1.3.1. Plan de la thèse

La thèse se divise en deux parties. La première partie est consacrée au problème de Lehmer relatif en dimension 1. Elle ne contient qu'un seul chapitre consacré à la démonstration des théorèmes 1.12 et 1.13 ; il s'agit de la reproduction, à quelques modifications près, de l'article [**AmDe07**]. La deuxième partie, qui concerne le problème de Lehmer relatif en dimension supérieure, est constituée de deux chapitres. Le premier est consacré aux hypersurfaces et à la démonstration du théorème 1.26 ; il s'agit, là aussi, à peu de chose près de [**Del05**]. Enfin, dans le dernier chapitre, nous démontrons le théorème 1.21.

Les chapitres 2, 3 et 4 sont ainsi logiquement indépendants les uns des autres. De plus chaque chapitre possède ses propres introduction et rappel de notations, ce qui le rend lisible hors de son contexte.

1.3.2. Techniques utilisées et schémas des preuves

Les démonstrations dans le cadre du problème de Lehmer relatif s'inspirent de la preuve du théorème d'E. Dobrowolski. Celle-ci suit le schéma classique d'une preuve de transcendance. Il s'agit en premier lieu de construire, à l'aide

d'un lemme de Siegel, une *fonction auxiliaire*, c'est-à-dire un polynôme dont nous contrôlons degré et hauteur et qui s'annule avec forte multiplicité en α. Puis à l'aide de propriétés métriques, on montre que si la hauteur de α est « petite », cette fonction auxiliaire s'annule en de nombreuses puissances de α. Un choix judicieux de paramètres permet alors d'aboutir à une contradiction.

Dans le cadre du problème de Lehmer classique, la propriété métrique utilisée est le petit théorème de Fermat, c'est-à-dire le fait qu'un entier et sa puissance p-ième, pour un nombre premier p, sont p-adiquement proches. Dans le cadre du problème de Lehmer relatif, nous ne travaillons plus sur $\mathbb{Q}$ mais sur une extension abélienne $\mathbb{L}$. Afin de ne pas faire intervenir le degré de $\mathbb{L}$, il est nécessaire d'utiliser des propriétés métriques non plus sur $\mathbb{Z}$ mais sur l'anneau des entiers de $\mathbb{L}$. Si p est un nombre premier et ϕ_p le morphisme de Frobenius associé à p, on utilise le fait que pour toute place v divisant p, l'entier $\phi_p(a)$ est v-adiquement proche de a^p pour tout $a \in \mathcal{O}_{\mathbb{L}}$. Cependant, plus la ramification de p est grande, plus cette propriété métrique est « faible ». Dans [**AmZa00**], les auteurs proposent alors une approche différente : ils construisent une fonction auxiliaire s'annulant avec forte multiplicité sur l'ensemble des conjugués de α^p au-dessus de $\mathbb{L}$, puis ils montrent que si la hauteur de α est « petite », cette fonction s'annule sur les conjugués de α^p au-dessus d'un certain sous-corps $\mathbb{E}$ de $\mathbb{L}$. Ce corps $\mathbb{E}$ est en fait le corps fixé par un sous-groupe de ramification de p dans $\mathbb{L}$ dont le cardinal est d'autant plus grand que l'indice de ramification de p dans $\mathbb{L}$ est grand ; les propriétés métriques utilisées sont données par des congruences du groupe de ramification. Ainsi, si le degré de $[\mathbb{L} : \mathbb{E}]$ est assez grand (donc si l'indice de ramification de p dans $\mathbb{L}$ est assez grand), on montre que la fonction auxiliaire possède « trop » de zéros et on aboutit à une contradiction. Avec un bon choix de paramètres, on effectue alors une dichotomie. Si l'ensemble des premiers considérés sont majoritairement « peu » ramifiés, la démonstration est semblable à celle du théorème d'E. Dobrowolski (avec le morphisme de Frobenius) ; sinon, on conclut avec l'argument alternatif.

Dans le chapitre 2, nous raffinons ce raisonnement en séparant la preuve en trois cas. Nous traitons le cas de « grande ramification » à part, en montrant qu'il ne peut y avoir de premier « très » ramifié si la hauteur de α est « petite ». Puis nous séparons le cas « petite ramification » en deux parties, suivant qu'une majorité de premiers est ramifiée ou pas. Par ailleurs, bien qu'il eût été possible d'utiliser le schéma précédent avec construction de fonctions auxiliaires nécessitant des lemmes de Siegel, nous donnons une preuve plus

élémentaire, à l'aide de déterminants de type Vandermonde. Le principe reste toutefois le même, à savoir utiliser des propriétés métriques adéquates.

Dans le chapitre 3, nous adaptons la preuve de [**AmZa00**] au cas des hypersurfaces. Mises à part les difficultés inhérentes à la dimension supérieure, le schéma de la preuve est identique.

Enfin, dans le dernier chapitre, nous adaptons ce raisonnement au cas des points en dimension supérieure. Nous effectuons une dichotomie et traitons le cas de « petite ramification » en nous inspirant de l'article [**AmDa99**] qui généralise le théorème d'E. Dobrowolski à la dimension supérieure. Pour le cas de « grande ramification », nous utilisons un argument de déterminant qui a l'avantage de se passer d'un lemme de Siegel. Nous combinons alors ces deux résultats pour montrer que si la hauteur de $\boldsymbol{\alpha}$ est « petite », il existe soit un multiple $\boldsymbol{\alpha}^l$ de $\boldsymbol{\alpha}$ pour lequel l'indice d'obstruction $\omega_{\mathbb{L}}(\boldsymbol{\alpha}^l)$ sur $\mathbb{L}$ est pathologiquement petit, soit un multiple $\boldsymbol{\alpha}^{l'}$ de $\boldsymbol{\alpha}$ pour lequel l'indice d'obstruction $\omega_{\mathbb{E}}(\boldsymbol{\alpha}^{l'})$ sur un sous-corps strict $\mathbb{E}$ de $\mathbb{L}$ est du même ordre de grandeur que $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$. Comme dans [**AmDa99**] et [**AmDa04**], cette proposition ne suffit pas pour conclure : il faut utiliser un argument de descente.

PARTIE I

LE PROBLÈME DE LEHMER RELATIF EN DIMENSION 1

CHAPITRE 2

UNE MINORATION RELATIVE EXPLICITE

Ce chapitre est la reproduction fidèle de l'article [**AmDe07**], à l'exception de quelques modifications mineures (dont les principales sont signalées par des notes de bas de page).

2.1. Introduction

Soit α un nombre algébrique non nul de degré D qui n'est pas une racine de l'unité. Le problème de Lehmer consiste à montrer qu'il existe une constante absolue $c > 0$, telle que

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

où $h(\alpha)$ désigne la hauteur de Weil logarithmique. Ce problème est encore ouvert et le meilleur résultat dans cette direction est un théorème de E. Dobrowolski (voir [**Dob79**]) qui montre l'existence d'une constante strictement positive C telle que

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

Cependant, si l'on se place dans des cas particuliers, on peut obtenir de meilleures minorations. En effet, le premier auteur et R. Dvornicich ont montré (voir [**AmDv00**]) que si α appartient à une extension abélienne de $\mathbb{Q}$, on a

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

Par la suite, le premier auteur et U. Zannier ont proposé une version relative du problème de Lehmer, généralisant le résultat précédent, en remplaçant le degré de α sur $\mathbb{Q}$ dans la conjecture par le degré « non abélien » de α sur un corps de nombres $\mathbb{K}$, c'est-à-dire le degré de α sur une extension abélienne de $\mathbb{K}$. Ils ont

ainsi montré dans [**AmZa00**] un analogue du théorème de Dobrowolski dans le cas relatif :

Théorème 2.1. — *Soit $\mathbb{K}$ un corps de nombres. Il existe une constante $c(\mathbb{K})$ strictement positive ne dépendant que de $\mathbb{K}$ telle que la proposition suivante soit vraie. Pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité et pour toute extension abélienne $\mathbb{L}$ de $\mathbb{K}$, on a*

$$h(\alpha) \geq \frac{c(\mathbb{K})}{D} \left(\frac{\log\log 5D}{\log 2D} \right)^{13}, \tag{2.1}$$

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

Le but de ce qui suit est double. D'une part, il s'agit d'améliorer l'exposant du terme en « log »grâce à une nouvelle preuve. D'autre part, il s'agit d'expliciter la dépendance en $\mathbb{K}$ de la constante $c(\mathbb{K})$. Cette constante dépend d'une part du degré $d = [\mathbb{K} : \mathbb{Q}]$ (car nous utiliserons dans l'extrapolation une congruence modulo un idéal premier P de l'anneau des entiers $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$) et d'autre part d'une estimation du terme reste dans le théorème des idéaux premiers dans $\mathbb{K}$, qui dépend du discriminant[(1)] $\Delta_{\mathbb{K}}$ du corps $\mathbb{K}$. Si l'on suppose l'hypothèse de Riemann généralisée (GRH), un résultat de Odlyzko et Lagarias (voir [**LO77**, Theorem 1.1]) fournit une très bonne estimation de ce reste et permet de montrer le résultat suivant :

Théorème 2.2. — *On suppose GRH. Soit α un nombre algébrique non nul qui n'est pas une racine de l'unité. Alors pour toute extension abélienne $\mathbb{L}$ de $\mathbb{K}$, on a*

$$h(\alpha) \geq \frac{c}{D} \min\left(\frac{\log\log(5D)^4}{d^5 \log(2dD)^2 \log(2D)^2}, \frac{\log\log(5D)^2}{\lambda d^2 \log(2D)} \right),$$

où c est une constante (absolue) strictement positive, $D = [\mathbb{L}(\alpha) : \mathbb{L}]$ et[(2)] *$\lambda = (\log(3|\Delta_{\mathbb{K}}|))^2 \max((\log\log(16|\Delta_{\mathbb{K}}|))^2, (\log(3d))^4)$. En particulier, on a*

$$h(\alpha) \geq \frac{c}{D} \frac{\log\log(5D)^4}{d^3 \delta^2 \log(2\delta D)^2 \log(2D)^2},$$

où $\delta = \log(3|\Delta_{\mathbb{K}}|)$.

(1) Étant donné que le symbole Δ va représenter un déterminant dans la suite, nous avons ajouté $\mathbb{K}$ en indice lorsqu'il s'agit du discriminant du corps $\mathbb{K}$, afin de ne pas provoquer de confusion.

(2) Nous avons ajouté ici des constantes dans les « log » afin que λ et δ soient bien définis et non nuls.

Sans GRH, les estimations du reste dans le théorème des idéaux premiers sont nettement moins bonnes (voir les théorèmes 1.3 et 1.4 de [**LO77**]) et ne permettent pas de trouver une dépendance polynomiale en $\Delta_{\mathbb{K}}$. Nous utiliserons alors une estimation due à Friedlander (voir [**Fri80**]), qui donne une version moins précise du théorème des idéaux premiers, avec en contrepartie une meilleure dépendance en $\Delta_{\mathbb{K}}$.

Théorème 2.3. — *Soit α un nombre algébrique non nul qui n'est pas une racine de l'unité. Alors pour toute extension abélienne $\mathbb{L}$ de $\mathbb{K}$, on a*[(3)]

$$h(\alpha) \geq \frac{(2g(d)\Delta_{\mathbb{K}})^{-c}}{D} \frac{\log\log(5D)^3}{\log(2D)^4},$$

où c est une constante (absolue) strictement positive, $D = [\mathbb{L}(\alpha) : \mathbb{L}]$ et $g(d) = 1$ s'il existe une tour d'extensions

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m = \mathbb{K},$$

avec $\mathbb{K}_i/\mathbb{K}_{i-1}$ galoisienne pour $i = 1, \ldots, m$, et $g(d) = d!$ sinon.

On peut se demander s'il est possible d'éviter la dépendance en le discriminant dans le résultat qui précède. On pourrait également conjecturer la généralisation suivante du problème de Lehmer :

$$h(\alpha) \geq \frac{c}{Dd}.$$

Or cette inégalité est fausse comme l'exemple suivant le montre. Soit $x > 1$ et soit $n = n(x)$ le produit de tous les premiers $p \leq x$. Soit $\mathbb{K}$ le corps engendré par les racines n-ièmes de l'unité ; alors $d = [\mathbb{K} : \mathbb{Q}] = \phi(n)$ et $n \gg d \log\log d$. Enfin, soient $\alpha = 2^{1/n}$ et $\mathbb{L} = \mathbb{K}(\alpha)$, extension abélienne de $\mathbb{K}$; en particulier $D = 1$. On a alors

$$h(\alpha) = \frac{\log 2}{n} \ll \frac{1}{Dd(\log\log d)}.$$

La démonstration du théorème 2.1 repose sur une dichotomie. Un ensemble Λ de premiers de $\mathcal{O}_{\mathbb{K}}$ étant fixé, on distingue deux cas, selon qu'une majorité d'éléments de Λ est « peu » ou « très » ramifiée dans l'extension abélienne $\mathbb{L}$ de $\mathbb{K}$ (tout ceci étant clairement quantifié à l'aide de paramètres). Ici, nous traitons le cas de « grande ramification » à part, en montrant qu'il ne peut y avoir de premier « très » ramifié si la hauteur de α est petite. De plus nous séparons de nouveau le cas « petite ramification » en deux parties, suivant qu'une majorité de premiers est ramifiée ou pas. Enfin, la preuve du théorème

(3) Nous avons ajouté ici un 2 afin que le théorème reste vrai quand $\mathbb{K} = \mathbb{Q}$.

2.1 suit le schéma d'une preuve de transcendance avec construction de fonctions auxiliaires nécessitant un lemme de Siegel absolu obtenu grâce à un résultat de Zhang. Ici, bien qu'il eût été possible d'utiliser les mêmes outils, nous donnons une preuve plus élémentaire, à l'aide de déterminants de type Vandermonde.

Dans un premier temps nous donnons les notations et réductions que nous utiliserons par la suite. La plupart d'entre elles sont issues de l'article [**AmZa00**]. Puis nous montrons les résultats préliminaires qui nous serviront à minorer la hauteur de α dans la dernière partie.

2.2. Notations

Dans toute la suite nous fixons $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$, que nous plongeons dans $\mathbb{C}$. Nous noterons $c_0, c_1, c_2 \ldots$ des constantes strictement positives et absolues. Nous fixons également un corps de nombres $\mathbb{K}$ et posons d (resp. $\Delta_{\mathbb{K}}$) le degré (resp. le discriminant) de $\mathbb{K}$ sur $\mathbb{Q}$; rappelons qu'on a l'inégalité $\log|\Delta_{\mathbb{K}}| \geq c_0 d$. Sauf mention explicite du contraire, lorsque l'on notera P un idéal premier de $\mathcal{O}_{\mathbb{K}}$, on désignera par p le premier rationnel sous P, c'est-à-dire tel que $(p) = P \cap \mathbb{Q}$. Soit $\mathcal{P}$ l'ensemble des idéaux premiers P de $\mathcal{O}_{\mathbb{K}}$ tels que l'indice de ramification et le degré d'inertie de P sur p soient égaux à 1 ($e(P|p) = f(P|p) = 1$).

Soient α un nombre algébrique non nul qui n'est pas racine de l'unité, $\mathbb{L}$ une extension abélienne de $\mathbb{K}$ et $D = [\mathbb{L}(\alpha) : \mathbb{L}]$. Nous nous proposons de montrer l'inégalité $h(\alpha) \geq f(d, \Delta_{\mathbb{K}}, D)$, où $D \mapsto f(d, \Delta_{\mathbb{K}}, D)$ est décroissante. Par invariance de la hauteur de Weil par multiplication par des racines de l'unité, nous pouvons faire exactement les mêmes hypothèses de minimalité et réductions que dans [**AmZa00**] (voir (2.3),(2.4),...,(2.8) de *op. cit.*). Ainsi, nous pourrons utiliser le lemme 3.2 de [**AmZa00**] (voir Proposition 2.4) et supposer que pour tout $n \in \mathbb{N}^*$, nous avons $\mathbb{L}(\alpha^n) = \mathbb{L}(\alpha)$.

Par abus de notation, nous identifierons les éléments de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ et les plongements $\mathbb{L} \hookrightarrow \bar{\mathbb{Q}}$ qui fixent $\mathbb{K}$. Chacun de ces éléments possède exactement D prolongements distincts à $\mathbb{L}(\alpha)$. Ainsi, si S est un sous-ensemble de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, l'ensemble

$$\overline{S} = \{\tau : \mathbb{L}(\alpha) \hookrightarrow \bar{\mathbb{Q}}, \tau_{|\mathbb{L}} \in S\}$$

est de cardinal $D|S|$. Enfin nous désignerons par F la clôture galoisienne de $\mathbb{L}(\alpha)$ sur $\mathbb{K}$.

Pour $P \in \mathcal{P}$, nous noterons e_P (resp. G_P) l'indice (resp. le groupe) de ramification de P dans $\mathbb{L}$ (qui ne dépendent pas du premier de $\mathcal{O}_{\mathbb{L}}$ au-dessus de

P car $\mathbb{L}/\mathbb{K}$ est abélienne). Nous désignerons par $\Phi_P \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ l'automorphisme de Frobenius associé à P. Par abus de notation, nous noterons encore P la valuation de $\mathbb{K}$ associée à P.

2.3. Résultats préliminaires

2.3.1. Congruences

Nous rappelons tout d'abord le lemme 3.2 de [**AmZa00**] :

Proposition 2.4. — *Soit $P \in \mathcal{P}$. Il existe un sous-groupe H_P de G_P vérifiant les trois propriétés suivantes :*

- $|H_P| \geq \min\{e_P, p\}$;
- *pour tout $\sigma \in H_P$, pour tout entier $\gamma \in \mathbb{L}$ et pour toute valuation v de $\bar{\mathbb{Q}}$ au-dessus de P, on a*

$$|\gamma^p - \sigma\gamma^p|_v \leq p^{-1}; \tag{2.2}$$

- *pour tout $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ prolongement d'un élément de $H_P \setminus \{\mathrm{Id}\}$, on a*

$$\tau\alpha^p \neq \alpha^p.$$

Nous aurons besoin du lemme d'approximation suivant :

Lemme 2.5. — *Soient k un corps de nombres, Σ un ensemble fini de places ultramétriques de k et $\gamma \in k$. Alors il existe $\beta \in \mathcal{O}_k$ tel que $\beta\gamma \in \mathcal{O}_k$ et $|\beta|_v = \max\{1, |\gamma|_v\}^{-1}$ pour toute place $v \in \Sigma$.*

Démonstration. — Fixons une place archimédienne quelconque v_0 et notons $\tilde{\Sigma}$ l'ensemble fini

$$\tilde{\Sigma} = \{v \in \mathcal{M}_k \mid v \nmid \infty \text{ et } |\gamma|_v > 1\} \cup \Sigma.$$

Pour toute place $v \in \tilde{\Sigma}$, on pose $\theta_v = \gamma^{-1}$ si $|\gamma|_v \geq 1$ et $\theta_v = 1$ sinon. D'après le théorème de [**CF67**, chap II, 15, page 67] il existe un élément $\beta \in k$ tel que

$$\begin{cases} |\beta - \theta_v|_v < \max\{1, |\gamma|_v\}^{-1} & \text{pour tout } v \in \tilde{\Sigma}, \\ |\beta|_v \leq 1 & \text{si } v \notin \tilde{\Sigma} \cup \{v_0\}. \end{cases}$$

En utilisant l'inégalité ultramétrique, on en déduit :

$$\begin{cases} |\beta|_v = \max\{1, |\gamma|_v\}^{-1} & \text{pour tout } v \in \tilde{\Sigma}, \\ |\beta|_v \leq 1 & \text{si } v \notin \tilde{\Sigma} \cup \{v_0\}. \end{cases}$$

En particulier, pour toute place finie v de k on a $|\beta|_v \leq 1$ et $|\beta\gamma|_v \leq 1$ donc β et $\beta\gamma$ sont des entiers de k. □

Ce dernier lemme nous permet de montrer la proposition suivante :

Proposition 2.6. — *Soit $\tau : \mathbb{L}(\alpha) \hookrightarrow \bar{\mathbb{Q}}$. Soient $P \in \mathcal{P}$, v une place de F au-dessus de P et f (resp. g) le polynôme minimal de α (resp. α^p) sur $\mathbb{L}$. Alors*

- *si $\tau_{|\mathbb{L}} \in H_P$,*

$$\forall \sigma \in H_P, \quad |g^\sigma(\tau\alpha^p)|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD} \prod_{\rho_{|\mathbb{L}}=\sigma} \max\{1, |\rho\alpha|_v\}^p \, ;$$

- *si $\tau_{|\mathbb{L}} \in G_P$,*

$$|f(\tau\alpha)|_v \leq p^{-1/e_P} \max\{1, |\tau\alpha|_v\}^D \prod_{\rho_{|\mathbb{L}}=\mathrm{Id}} \max\{1, |\rho\alpha|_v\} \, ;$$

- *si $\tau_{|\mathbb{L}} = \Phi_P^{-1}$ et $e_P = 1$,*

$$|f(\tau\alpha^p)|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD} \prod_{\rho_{|\mathbb{L}}=\mathrm{Id}} \max\{1, |\rho\alpha|_v\}.$$

Démonstration. — Nous pouvons appliquer le lemme 2.5 à α et Σ l'ensemble des places de F au-dessus de P. Ainsi, il existe $\beta \in \mathcal{O}_F$ tel que $\beta\alpha \in \mathcal{O}_F$ et $|\tau\beta|_v = \max\{1, |\tau\alpha|_v\}^{-1}$ pour tout $\tau \in \mathrm{Gal}(F/\mathbb{K})$. Notons $\tau_1, \ldots, \tau_D$ les D morphismes de $\mathbb{L}(\alpha)$ dans $\bar{\mathbb{Q}}$ qui prolongent l'inclusion $\mathbb{L} \hookrightarrow \bar{\mathbb{Q}}$ et $b = \prod_{i=1}^D \tau_i\beta \in \mathcal{O}_\mathbb{L}$. Alors $bf(X) = \sum_{k=0}^D a_k X^k \in \mathcal{O}_\mathbb{L}[X]$ et par le petit théorème de Fermat :

$$\begin{aligned}(bf(X))^p &= \prod_{i=1}^D (\tau_i\beta X - \tau_i(\beta\alpha))^p \\ &\equiv \prod_{i=1}^D (\tau_i\beta^p X^p - \tau_i(\beta\alpha)^p) \mod p\mathcal{O}_F[X] \\ &= b^p \prod_{i=1}^D (X^p - \tau_i\alpha^p)\,.\end{aligned}$$

Or $[\mathbb{L}(\alpha^p) : \mathbb{L}] = [\mathbb{L}(\alpha) : \mathbb{L}] = D$ donc $g(X) = \prod_{i=1}^D (X - \tau_i\alpha^p)$ et finalement

$$(bf(X))^p \equiv b^p g(X^p) \mod p\mathcal{O}_\mathbb{L}[X]. \tag{2.3}$$

Examinons maintenant les différents cas.

Si $\tau_{|\mathbb{L}} \in H_P$, on a pour tout $\sigma \in H_P$, d'après la proposition 2.4 et le petit théorème de Fermat

$$(b^\sigma f^\sigma(X))^p = \left(\sum_{k=0}^{D} a_k^\sigma X^k\right)^p$$
$$\equiv \sum_{k=0}^{D} (a_k^\sigma)^p X^{kp} \equiv \sum_{k=0}^{D} (a_k^\tau)^p X^{kp} \equiv (b^\tau f^\tau(X))^p \mod P\mathcal{O}_{\mathbb{L}}[X].$$

En combinant ceci avec la congruence (2.3), on obtient

$$(b^\sigma)^p g^\sigma(X^p) \equiv (b^\tau)^p f^\tau(X)^p \mod P\mathcal{O}_F[X], \tag{2.4}$$

ce qui donne, en évaluant en $\tau\alpha$,

$$|(b^\sigma)^p g^\sigma(\tau\alpha^p)|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD},$$

soit encore

$$|g^\sigma(\tau\alpha^p)|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD} \prod_{\rho_{|\mathbb{L}}=\sigma} \max\{1, |\rho\alpha|_v\}^p.$$

Si $\tau_{|\mathbb{L}} \in G_P$, on a

$$b^\tau f^\tau(X) = \sum_{k=0}^{D} a_k^\tau X^k \equiv \sum_{k=0}^{D} a_k X^k \equiv bf(X) \mod Q\mathcal{O}_L,$$

où Q est l'idéal de $\mathcal{O}_{\mathbb{L}}$ défini par $Q^{e_P} = P\mathcal{O}_{\mathbb{L}}$. En évaluant la congruence précédente en $\tau\alpha$ on obtient

$$|bf(\tau\alpha)|_v \leq p^{-1/e_P} \max\{1, |\tau\alpha|_v\}^D,$$

soit

$$|f(\tau\alpha)|_v \leq p^{-1/e_P} \max\{1, |\tau\alpha|_v\}^D \prod_{\rho_{|\mathbb{L}}=\mathrm{Id}} \max\{1, |\rho\alpha|_v\}.$$

Enfin, si $\tau_{|\mathbb{L}} = \Phi_P^{-1}$, d'après (2.3), on a

$$(b^\tau f^\tau(X))^p \equiv (b^p)^\tau g^\tau(X^p) \mod P\mathcal{O}_{\mathbb{L}}[X].$$

De plus, la caractérisation de l'automorphisme de Frobenius et le petit théorème de Fermat donnent

$$(b^\tau f^\tau(X))^p = \left(\sum_{k=0}^{D} a_k^\tau X^k\right)^p$$
$$\equiv \sum_{k=0}^{D} (a_k^\tau)^p X^{kp} \equiv \sum_{k=0}^{D} a_k X^{kp} \equiv bf(X^p) \mod P\mathcal{O}_{\mathbb{L}}[X].$$

En évaluant cette congruence en $\tau\alpha$, on obtient

$$|bf(\tau\alpha^p)|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD}$$

et

$$|f(\tau\alpha^p)|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD} \prod_{\rho_{|\mathbb{L}}=\mathrm{Id}} \max\{1, |\rho\alpha|_v\}.$$

□

2.3.2. Déterminant de Vandermonde généralisé

Pour montrer les théorèmes 2.2 et 2.3 nous utiliserons des déterminants de Vandermonde généralisés :

Lemme 2.7. — *Soient $T_1, \ldots, T_r$ des entiers positifs et $L = T_1 + \cdots + T_r$. Soit $\Delta((X_i, T_i)_{1\leq i\leq r}) \in \mathbb{Z}[X_1, \ldots, X_r]$ le déterminant de la matrice $L \times L$*

$$M = (M_1\ M_2\ \ldots\ M_r),$$

où pour tout $1 \leq j \leq r$, M_j est le bloc de taille $L \times T_j$ suivant :

$$M_j = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ X_j & 1 & \ldots & 0 \\ X_j^2 & 2X_j & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ X_j^{\mu-1} & (\mu-1)X_j^{\mu-2} & \ldots & \binom{\mu-1}{T_j-1} X_j^{\mu-T_j} \\ \vdots & \vdots & \ddots & \vdots \\ X_j^{L-1} & (L-1)X_j^{L-2} & \ldots & \binom{L-1}{T_j-1} X_j^{L-T_j} \end{pmatrix}.$$

Alors

$$\Delta((X_i, T_i)_{1\leq i\leq r}) = \prod_{i>j} (X_i - X_j)^{T_i T_j}.$$

Démonstration. — Voir [**Mér99**]. □

Lemme 2.8. — *Soient $\gamma_1, \dots, \gamma_r$ des nombres algébriques, $T_1, \dots, T_r$ des entiers positifs et $\Delta = \Delta((\gamma_i, T_i)_{1 \le i \le r})$. Si k est un corps contenant $\gamma_1, \dots, \gamma_r$ et v une place de k, alors*

– *si v est archimédienne*[(4)]*,*

$$|\Delta|_v \le L^{\sum_{i=1}^r {T_i}^2} \prod_{i=1}^r \max\{1, |\gamma_i|_v\}^{T_i(L-1)},$$

– *si v est ultramétrique,*

$$|\Delta|_v \le \prod_{i=1}^r \max\{1, |\gamma_i|_v\}^{T_i(L-1)},$$

où $L = T_1 + \cdots + T_r$.

Démonstration. — Soit v une place archimédienne de F. D'après l'inégalité d'Hadamard, on a

$$\begin{aligned} {|\Delta|_v}^2 &\le \prod_{i=1}^r \prod_{j=1}^{T_i} \sum_{k=1}^{L} \binom{k-1}{j-1}^2 \max\{1, |\gamma_i|_v\}^{2(k-1)} \\ &\le \prod_{i=1}^r \prod_{j=1}^{T_i} \binom{L}{j}^2 \max\{1, |\gamma_i|_v\}^{2(L-1)} \\ &\le L^{\sum_{i=1}^r T_i(T_i+1)} \prod_{i=1}^r \max\{1, |\gamma_i|_v\}^{2T_i(L-1)} \\ &\le L^{2\sum_{i=1}^r {T_i}^2} \prod_{i=1}^r \max\{1, |\gamma_i|_v\}^{2T_i(L-1)}. \end{aligned}$$

Soit v une place ultramétrique ; en utilisant le lemme 2.7 et l'inégalité

$$|\gamma_i - \gamma_j|_v \le \max\{1, |\gamma_i|_v\} \max\{1, |\gamma_j|_v\},$$

on obtient directement la deuxième majoration du lemme. □

2.4. Démonstration du théorème 2.2

Nous fixons deux paramètres :

$$N = C^3 \max\left(d^3 \frac{\log(2dD)^2 \log(2D)}{\log\log(5D)^2}, \lambda\right) \quad \text{et} \quad E = \left[Cd \frac{\log(2D)}{\log\log(5D)}\right],$$

(4) Nous corrigeons ici une erreur de **[AmDe07]** : il faut supprimer le facteur $\frac{1}{2}$ de l'exposant de L. Ceci modifie quelque peu la suite, mais aucunement le résultat final.

où $C > 0$ est une constante absolue que l'on supposera « assez grande » (en d'autres termes, les inégalités que nous serons amenés à écrire seront vraies asymptotiquement en C). Nous noterons Λ l'ensemble des éléments de $\mathcal{P}$ dont la norme sur $\mathbb{Q}$ est comprise entre $\sqrt{N}$ et N. Pour montrer le théorème nous procédons en trois étapes : dans un premier temps nous supposerons qu'il existe un premier $P \in \Lambda$ tel que le groupe H_P défini à la proposition 2.4 soit de cardinal supérieur à E ; puis nous étudierons le cas où la majorité des éléments de Λ ont un indice de ramification dans $\mathbb{L}$ compris entre 2 et E ; nous conclurons avec le cas où la majorité des éléments de Λ ne sont pas ramifiés dans $\mathbb{L}$.

Nous aurons besoin dans la suite de certaines estimations qui font l'objet du lemme suivant :

Lemme 2.9. — *On a les inégalités*

$$\log N \geq \log\log(5D) \tag{2.5}$$

et

$$\frac{\log\log(5D)^2}{d^3\log(2D)} N \geq C^{5/2}\log(ND)^2. \tag{2.6}$$

Démonstration. — L'inégalité (2.5) est claire. Montrons (2.6). Compte tenu du choix de N et de la majoration

$$\log(ND) \leq 3(\log C)\max\{\log(2dD), \log\lambda\},$$

il suffit de montrer qu'il existe $c_1 > 0$ tel que

$$\max\left(\log(2dD)^2, \frac{\lambda\log\log(5D)^2}{d^3\log(2D)}\right) \geq c_1\max(\log(2dD)^2, (\log\lambda)^2).$$

Cette assertion est claire si $\log\lambda \leq 6\log(2dD)$. Supposons donc $\lambda > (2dD)^6$; on a alors

$$\frac{\lambda\log\log(5D)^2}{d^3\log(2D)} \geq \frac{8D^3\lambda^{1/2}\log\log(5D)^2}{\log(2D)} \geq c_1(\log\lambda)^2.$$

□

Nous aurons également besoin d'estimer le cardinal de Λ.

Lemme 2.10. — *Si l'on suppose GRH,*

$$|\Lambda| \geq \frac{N}{2\log N}.$$

Démonstration. — Compte tenu de la définition de λ et du choix de N, le théorème 1.1 de [**LO77**] donne

$$\#\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ tel que } N_{\mathbb{K}/\mathbb{Q}}(P) \leq N\} \geq \frac{2N}{3\log N}.$$

Par ailleurs,

$$\#\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ tel que } N_{\mathbb{K}/\mathbb{Q}}(P) \leq \sqrt{N}\} \leq d\pi(\sqrt{N}),$$

où $\pi(x)$ est le nombre de premiers rationnels inférieurs à x. Soit P un idéal premier de $\mathcal{O}_{\mathbb{K}}$; si $e(P|p) > 1$, alors p divise $\Delta_{\mathbb{K}}$. Comme il y a au plus d premiers au-dessus de p, on a

$$\#\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ tel que } e(P|p) > 1\} \leq \frac{d\log|\Delta_{\mathbb{K}}|}{\log 2}.$$

De plus, si P est tel que $f(P|p) > 1$, alors $N_{\mathbb{K}/\mathbb{Q}}(P) \geq p^2$. D'où :

$$\#\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ tel que } f(P|p) > 1 \text{ et } N_{\mathbb{K}/\mathbb{Q}}(P) \leq N\} \leq d\pi(\sqrt{N}).$$

On a donc, en utilisant la majoration de Chebichev $\pi(x) \leq c_2 x/\log x$ et l'inégalité $N \geq Cd^3$,

$$|\Lambda| \geq \frac{2N}{3\log N} - \frac{2c_2 d\sqrt{N}}{\log N} - \frac{d\log|\Delta_{\mathbb{K}}|}{\log 2} - \frac{2c_2 d\sqrt{N}}{\log N} \geq \frac{N}{2\log N}.$$

□

Quitte à remplacer Λ par un sous-ensemble, on peut donc supposer

$$\frac{N}{2\log N} \leq |\Lambda| \leq \frac{N}{\log N}.$$

2.4.1. Cas où il existe un premier ayant grande ramification

Supposons tout d'abord qu'il existe un premier $P \in \Lambda$ tel que $e_P \geq E$. Le groupe H_P défini à la proposition 2.4 est alors de cardinal supérieur à E, car $p \geq \sqrt{N} \geq E$. Considérons un sous-ensemble de $S \subseteq H_P$ de cardinal E et notons $\overline{S}$ l'ensemble des DE morphismes de $\mathbb{L}(\alpha)$ dans $\bar{\mathbb{Q}}$ qui prolongent les éléments de S. On définit

$$\Delta = \Delta\left((\tau\alpha^p, 1)_{\tau\in\overline{S}}\right).$$

Ce déterminant est de taille $L = DE$ et n'est pas nul d'après la dernière assertion de la proposition 2.4.

Nous allons appliquer la formule du produit à Δ afin de minorer la hauteur de α. Étudions $|\Delta|_v$ pour chaque place $v \in \mathcal{M}_F$.

Lemme 2.11. — *Soit v une place de F. Alors*

– *si $v|\infty$,*

$$|\Delta|_v \leq L^L \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{p(L-1)},$$

– *si $v\nmid\infty$,*

$$|\Delta|_v \leq \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{p(L-1)},$$

– *si $v|P$,*

$$|\Delta|_v \leq p^{-L(E-1)/2} \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{p(L-1)}.$$

Démonstration. — Les deux premières inégalités sont données par le lemme 2.8. Supposons que v divise P. Soient $\sigma \in H_P$ et g le polynôme minimal de α^p sur $\mathbb{L}$. Étant donné que $[\mathbb{L}(\alpha^p) : \mathbb{L}] = [\mathbb{L}(\alpha) : \mathbb{L}] = D$, on a

$$g^\sigma(X) = \prod_{\substack{\rho\in\overline{H}_p \\ \rho_{|\mathbb{L}}=\sigma}} (X - \rho\alpha^p).$$

Ainsi, d'après le lemme 2.7,

$$|\Delta|_v{}^2 = \prod_{\tau\in\overline{S}} \left(\prod_{\substack{\sigma\in S \\ \sigma\neq\tau_{|\mathbb{L}}}} |g^\sigma(\tau\alpha^p)|_v \prod_{\substack{\rho_{|\mathbb{L}}=\tau_{|\mathbb{L}} \\ \rho\neq\tau}} |\tau\alpha^p - \rho\alpha^p|_v \right).$$

Fixons $\tau \in \overline{S}$; d'après la proposition 2.6, le premier produit de la parenthèse est majoré de la façon suivante :

$$\prod_{\substack{\sigma\in S \\ \sigma\neq\tau_{|\mathbb{L}}}} |g^\sigma(\tau\alpha^p)|_v \leq p^{E-1} \max\{1, |\tau\alpha|_v\}^{pD(E-1)} \prod_{\substack{\rho\in\overline{S} \\ \rho_{|\mathbb{L}}\neq\tau_{|\mathbb{L}}}} \max\{1, |\rho\alpha|_v\}^p.$$

Nous majorons le deuxième produit de manière usuelle :

$$\prod_{\substack{\rho_{|\mathbb{L}}=\tau_{|\mathbb{L}} \\ \rho\neq\tau}} |\tau\alpha^p - \rho\alpha^p|_v \ \leq \ \max\{1, |\tau\alpha^p|_v\}^{D-1} \prod_{\substack{\rho_{|\mathbb{L}}=\tau_{|\mathbb{L}} \\ \rho\neq\tau}} \max\{1, |\rho\alpha^p|_v\}.$$

Ce qui nous donne en regroupant :

$$|\Delta|_v{}^2 \leq p^{-L(E-1)} \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{2p(L-1)}.$$

□

La formule du produit appliquée à Δ nous donne alors

$$0 \leq 2L\log L - \frac{L(E-1)}{d}\log p + 2p(L-1)\sum_{\tau\in\overline{S}} h(\tau\alpha)$$

d'où

$$\frac{(E-1)}{d}\log p \leq 2\log L + 2p(L-1)h(\alpha).$$

Or,

$$\begin{aligned}\frac{(E-1)}{d}\log p - 2\log L &\geq \frac{E\log N}{4d} - 2\log D - 2\log E\\ &\geq \log(2D).\end{aligned}$$

On en déduit :

$$h(\alpha) \geq \frac{\log(2D)}{2DNE} \geq \frac{c_3}{D}\min\left(\frac{\log\log(5D)^3}{d^4\log(2dD)^2\log(2D)}, \frac{\log\log(5D)}{\lambda d}\right). \tag{2.7}$$

2.4.2. Les éléments de Λ sont peu ramifiés

Nous supposons maintenant que pour tout $P \in \Lambda$, on a $e_P \leq E$. Nous séparons la preuve en deux cas, suivant qu'une majorité de premiers est ramifiée ou non.

2.4.2.1. Une majorité est ramifiée. — Posons $\Lambda_1 = \{P \in \Lambda \mid 2 \leq e_P \leq E\}$. Supposons dans un premier temps

$$|\Lambda_1| \geq \frac{N}{4\log N}.$$

On définit alors $S = \cup_{P\in\Lambda_1} G_P$ et pour tout $\sigma \in S$

$$\Lambda(\sigma) = \{P \in \Lambda_1 \mid \sigma \in G_P\}.$$

Considérons le déterminant $\Delta = \Delta((\tau\alpha, T_\tau)_\tau)$ où τ parcourt l'ensemble $\overline{S}$ et

$$T_\tau = \begin{cases} T_{\mathrm{Id}} &= \left[\frac{N}{Cd\log(ND)}\right] & \text{si } \tau_{|\mathbb{L}} = \mathrm{Id},\\ T_\sigma &= \left[\frac{Cd\log(2D)}{\log\log(5D)}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\right] & \text{si } \tau_{|\mathbb{L}} = \sigma.\end{cases}$$

Ce déterminant est de taille $L = \sum_{\tau\in\overline{S}} T_\tau = D\sum_{\sigma\in S} T_\sigma$ et n'est pas nul car les $\tau\alpha,\ \tau \in \overline{S}$, sont deux à deux distincts. Remarquons aussi

$$2\log L \leq c_4\log(ND).$$

Étudions $|\Delta|_v$ pour chaque place $v \in \mathcal{M}_F$.

Lemme 2.12. — *Soit v une place de F. Alors*

- *si $v|\infty$,*
$$|\Delta|_v \leq L^{D\sum_{\sigma\in S} T_\sigma^2} \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{T_\tau(L-1)},$$
- *si $v\nmid\infty$,*
$$|\Delta|_v \leq \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{T_\tau(L-1)},$$
- *si $v|P$ avec $P\in\Lambda_1$,*
$$|\Delta|_v \leq p^{-\frac{DT_{\mathrm{Id}}}{2e_P}\sum_{\sigma\in G_P\setminus\{\mathrm{Id}\}} T_\sigma} \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{T_\tau(L-1)}.$$

Démonstration. — Les deux premières inégalités sont encore données par le lemme 2.8. Soit $P\in\Lambda_1$ et supposons que v divise P. Fixons $\tau\in\overline{S}$; si $\tau_{|\mathbb{L}}\notin G_P$, on a la majoration suivante :

$$\prod_{\substack{\rho\in\overline{S}\\ \rho\neq\tau}} |\tau\alpha-\rho\alpha|^{T_\tau T_\rho} \leq \max\{1, |\tau\alpha|_v\}^{T_\tau\sum_{\rho\neq\tau} T_\rho} \prod_{\substack{\rho\in\overline{S}\\ \rho\neq\tau}} \max\{1, |\rho\alpha|_v\}^{T_\tau T_\rho}.$$

Supposons maintenant $\tau_{|\mathbb{L}}=\sigma\in G_P\setminus\{\mathrm{Id}\}$, on a alors

$$\prod_{\substack{\rho\in\overline{S}\\ \rho\neq\tau}} |\tau\alpha-\rho\alpha|^{T_\tau T_\rho} = A_\tau B_\tau,$$

où

$$A_\tau = \prod_{\rho_{|\mathbb{L}}=\mathrm{Id}} |\tau\alpha-\rho\alpha|_v^{T_\tau T_\rho} = |f(\tau\alpha)|_v^{T_\tau T_\rho}$$

et

$$B_\tau = \prod_{\substack{\rho_{|\mathbb{L}}\neq\mathrm{Id}\\ \rho\neq\tau}} |\tau\alpha-\rho\alpha|_v^{T_\tau T_\rho}.$$

La proposition 2.6 nous fournit la majoration suivante pour A_τ :

$$A_\tau \leq p^{-\frac{T_\tau T_{\mathrm{Id}}}{e_P}} \max\{1, |\tau\alpha|_v\}^{DT_\tau T_{\mathrm{Id}}} \prod_{\rho_{|\mathbb{L}}=\mathrm{Id}} \max\{1, |\rho\alpha|_v\}^{T_\tau T_\rho},$$

et nous avons la majoration usuelle pour B_τ :

$$B_\tau \leq \max\{1, |\tau\alpha|_v\}^{T_\tau\sum_{\substack{\rho_{|\mathbb{L}}\neq\mathrm{Id}\\ \rho\neq\tau}} T_\rho} \prod_{\substack{\rho_{|\mathbb{L}}\neq\mathrm{Id}\\ \rho\neq\tau}} \max\{1, |\rho\alpha|_v\}^{T_\tau T_\rho}.$$

Donc en faisant le produit pour τ parcourant $\overline{S}$, on obtient

$$\begin{aligned}|\Delta|_v{}^2 &\leq p^{-\frac{T_{\mathrm{Id}}}{e_P}\sum_{\tau_{|\mathbb{L}}\in G_P\setminus\{\mathrm{Id}\}}T_\tau}\prod_{\tau\in\overline{S}}\max\{1,|\tau\alpha|\}^{2T_\tau\sum_{\rho\neq\tau}T_\tau}\\ &\leq p^{-\frac{DT_{\mathrm{Id}}}{e_P}\sum_{\sigma\in G_P\setminus\{\mathrm{Id}\}}T_\sigma}\prod_{\tau\in\overline{S}}\max\{1,|\tau\alpha|\}^{2T_\tau(L-1)},\end{aligned}$$

ce qui achève la preuve du lemme. □

Le déterminant Δ n'étant pas nul, on peut lui appliquer la formule du produit ; le lemme précédent donne alors

$$\prod_{P\in\Lambda_1}p^{\frac{DT_{\mathrm{Id}}}{d\cdot e_P}\sum_{\sigma\in G_P\setminus\{\mathrm{Id}\}}T_\sigma}\leq L^{2D\sum_{\sigma\in S}T_\sigma^2}H(\alpha)^{2L(L-1)}.$$

En posant $\lambda_\sigma=\frac{T_\sigma}{T_{\mathrm{Id}}}$, l'inégalité précédente devient

$$\frac{\log N}{2d}\sum_{P\in\Lambda_1}\sum_{\sigma\in G_P\setminus\{\mathrm{Id}\}}\frac{\lambda_\sigma}{e_P}\ \leq\ 2\left(\sum_{\sigma\in S}\lambda_\sigma^2\right)\log L+2\left(\sum_{\sigma\in S}\lambda_\sigma\right)^2Dh(\alpha). \tag{2.8}$$

Avec l'égalité suivante :

$$\sum_{P\in\Lambda_1}\sum_{\sigma\in G_P\setminus\{\mathrm{Id}\}}\frac{\lambda_\sigma}{e_P}=\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\sum_{P\in\Lambda(\sigma)}\frac{\lambda_\sigma}{e_P},$$

on peut réécrire l'inégalité (2.8) :

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\lambda_\sigma A_\sigma\Big)-c_4\log(ND)\leq 2\Big(\sum_{\sigma\in S}\lambda_\sigma\Big)^2Dh(\alpha), \tag{2.9}$$

où

$$A_\sigma=\frac{\log N}{2d}\left(\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\right)-c_4\lambda_\sigma\log(ND).$$

En utilisant la majoration

$$\lambda_\sigma\leq\frac{2C^2d^2\log(ND)\log(2D)}{N\log\log(5D)}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P} \tag{2.10}$$

valable pour $\sigma \neq \mathrm{Id}$ et les inégalités (2.5) et (2.6) du lemme 2.9, on a

$$A_\sigma \geq \left(\frac{\log N}{2d} - \frac{2c_4 C^2 d^2 \log(ND)^2 \log(2D)}{N \log\log(5D)}\right) \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P}$$

$$\geq \frac{\log N}{4d} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P},$$

d'où, en minorant $\sum_{P\in\Lambda(\sigma)} \frac{1}{e_P}$ par $1/E$,

$$A_\sigma \geq \frac{\log N}{4dE} \geq \frac{\log\log(5D)\log N}{8Cd^2\log(2D)}. \tag{2.11}$$

Remarquons que

$$\sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \sum_{p\in\Lambda(\sigma)} \frac{1}{e_P} = \sum_{P\in\Lambda_1} \frac{e_P - 1}{e_P}$$

donc

$$\frac{1}{2}|\Lambda_1| \leq \sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P} \leq |\Lambda_1|. \tag{2.12}$$

En utilisant la minoration

$$\lambda_\sigma \geq \frac{C^2 d^2 \log(ND)\log(2D)}{2N\log\log(5D)} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P}$$

et (2.12) on obtient

$$\sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \lambda_\sigma \geq \frac{C^2 d^2 \log(ND)\log(2D)}{2N\log\log(5D)} \sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P}$$

$$\geq \frac{C^2 d^2 \log(ND)\log(2D)}{2N\log\log(5D)} \times \frac{N}{8\log N}$$

$$\geq \frac{C^2 d^2 \log(ND)\log(2D)}{16\log\log(5D)\log N}.$$

Ainsi, (2.11) donne

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \lambda_\sigma A_\sigma\Big) - c_4\log(ND) \geq \log(ND). \tag{2.13}$$

Enfin, en utilisant encore (2.10) et (2.12), on obtient

$$\sum_{\sigma\in S}\lambda_\sigma \le 1+\frac{2C^2d^2\log(ND)\log(2D)}{N\log\log(5D)}\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}$$

$$\le 1+\frac{2C^2d^2\log(ND)\log(2D)}{N\log\log(5D)}\times\frac{N}{\log N} \tag{2.14}$$

$$\le \frac{4C^2d^2\log(ND)\log(2D)}{\log\log(5D)\log N}.$$

En injectant (2.13) et (2.14) dans (2.9) et en utilisant (2.5), on a alors

$$h(\alpha)\ge \frac{c_5(\log N)^2\log\log(5D)^2}{Dd^4\log(ND)\log(2D)^2}\ge\frac{c_6\log\log(5D)^4}{Dd^4\log(2D)^3}. \tag{2.15}$$

2.4.2.2. Une majorité n'est pas ramifiée. — Posons $\Lambda_2=\{P\in\Lambda\mid e_P=1\}$. Supposons maintenant

$$|\Lambda_2|\ge\frac{N}{4\log N}.$$

Pour tout $P\in\Lambda_2$, on note Φ_P le morphisme de Frobenius associé à P, c'est-à-dire le morphisme vérifiant

$$\forall\gamma\in\mathcal{O}_{\mathbb{L}},\quad \Phi_P\gamma\equiv\gamma^p \mod P\mathcal{O}_{\mathbb{L}}.$$

Notons Γ l'ensemble des premiers rationnels p tels qu'il existe $P\in\Lambda_2$ au-dessus de p. Pour $p\in\Gamma$, on définit $\Sigma_p=\{\Phi_P^{-1}\mid P\in\Lambda_2, P|p\}$. Notons également $\tau_1,\dots,\tau_D$ les D plongements distincts de $\mathbb{L}(\alpha)$ dans $\bar{\mathbb{Q}}$ qui prolongent l'inclusion $\mathbb{L}\hookrightarrow\bar{\mathbb{Q}}$. Considérons le déterminant

$$\Delta=\Delta((\tau_i\alpha,T)_{1\le i\le D},(\tau_p\alpha^p,1)_{p\in\Gamma,\tau_p\in\overline{\Sigma}_p}),$$

où

$$T=\left[\frac{N}{C^2d\log(ND)}\right].$$

Ce déterminant est de taille $L=D(T+\sum_{p\in\Gamma}|\Sigma_p|)\le D(T+|\Lambda_2|)$. On a

$$\log L\le c_7\log(ND).$$

Étudions $|\Delta|_v$ pour chaque place $v\in\mathcal{M}_F$.

Lemme 2.13. — *Soit v une place de F. Alors*

– *si $v|\infty$,*

$$|\Delta|_v\le L^{D(T^2+|\Lambda_2|)}\prod_{1\le i\le D}\max\{1,|\tau_i\alpha|_v\}^{T(L-1)}\prod_{p\in\Gamma}\prod_{\tau_p\in\overline{\Sigma}_p}\max\{1,|\tau_p\alpha|_v\}^{p(L-1)},$$

– *si* $v \nmid \infty$,

$$|\Delta|_v \leq \prod_{1\leq i\leq D} \max\{1, |\tau_i\alpha|_v\}^{T(L-1)} \prod_{p\in\Gamma} \prod_{\tau_p\in\overline{\Sigma}_p} \max\{1, |\tau_p\alpha|_v\}^{p(L-1)},$$

– *si* $v|Q$ *avec* $Q \in \Lambda_2$,

$$|\Delta|_v \leq q^{-\frac{DT}{2}} \prod_{1\leq i\leq D} \max\{1, |\tau_i\alpha|_v\}^{T(L-1)} \prod_{p\in\Gamma} \prod_{\tau_p\in\overline{\Sigma}_p} \max\{1, |\tau_p\alpha|_v\}^{p(L-1)},$$

où q *désigne le premier rationnel sous* Q.

Démonstration. — Les deux premières inégalités sont encore données par le lemme 2.8. Soient $Q \in \Lambda_2$ et $\tau_{Q,1}, \ldots, \tau_{Q,D}$ les D prolongements de Φ_Q^{-1} à $\mathbb{L}(\alpha)$. Si $v|Q$, on a

$$|\Delta|_v{}^2 \leq A_1A_2A_3A_4,$$

avec

$$\begin{cases} A_1 &= \displaystyle\prod_{i=1}^{D} \prod_{\substack{j=1\\ j\neq i}}^{D} |\tau_i\alpha - \tau_j\alpha|_v^{T^2} \\ A_2 &= \displaystyle\prod_{\substack{\tau_p\in\overline{\Sigma}_p,\ \tau_r\in\overline{\Sigma}_r\\ (p,\tau_p)\neq(r,\tau_r)}} |\tau_p\alpha^p - \tau_r\alpha^r|_v \\ A_3 &= \displaystyle\prod_{\substack{p\in\Gamma,\ \tau_p\in\overline{\Sigma}_p\\ \left(p,\tau_{p|\mathbb{L}}\right)\neq\left(q,\Phi_Q^{-1}\right)}} \prod_{i=1}^{D} |\tau_i\alpha - \tau_p\alpha^p|_v^T \\ A_4 &= \displaystyle\prod_{i=1}^{D} \prod_{j=1}^{D} |\tau_i\alpha - \tau_{Q,j}\alpha^q|_v^T \end{cases}$$

En majorant grossièrement chacun des facteurs de A_1, A_2 et A_3, on obtient

$$A_1 \leq \prod_{1\leq i\leq D} \max\{1, |\tau_i\alpha|_v\}^{2T^2(D-1)},$$

$$A_2 \leq \prod_{p\in\Gamma,\ \tau_p\in\overline{\Sigma}_p} \max\{1, |\tau_p\alpha|_v\}^{2p(D|\Lambda_2|-1)},$$

$$A_3 \leq \prod_{1\leq i\leq D} \max\{1, |\tau_i\alpha|_v\}^{2DT(|\Lambda_2|-1)} \prod_{\substack{p\in\Gamma,\ \tau_p\in\overline{\Sigma}_p\\ \left(p,\tau_{p|\mathbb{L}}\right)\neq\left(q,\Phi_Q^{-1}\right)}} \max\{1, \tau_p\alpha^p|_v\}^{DT}.$$

Enfin, si on note encore f le polynôme minimal de α sur $\mathbb{L}$, d'après la proposition 2.6 :

$$\begin{aligned} A_4 &= \prod_{j=1}^{d} |f(\tau_{Q,j}\alpha^q)|_v^T \\ &\leq q^{-DT} \max\{1, |\tau_{Q,j}\alpha|_v\}^{qDT} \prod_{1\leq i\leq D} \max\{1, |\tau_i\alpha|_v\}^T. \end{aligned}$$

Il suffit alors de multiplier ces quatre inégalités pour terminer la démonstration du lemme. □

Le déterminant Δ n'est pas nul car les $\tau_i\alpha$ et $\tau_p\alpha^p$, $p \in \Gamma, \tau_p \in \overline{\Sigma}_p$, sont deux à deux distincts. On peut donc appliquer à Δ la formule du produit ; le lemme précédent donne alors

$$\prod_{P\in\Lambda_2} p^{\frac{DT}{d}} \leq L^{2D(T^2+|\Lambda_2|)} H(\alpha)^{2D(L-1)(T+\sum_{P\in\Lambda_2} p)},$$

soit

$$\frac{T}{d} \sum_{P\in\Lambda_2} \log p \leq 2(T^2+|\Lambda_2|)\log L + 2(T+|\Lambda_2|)(T+\sum_{P\in\Lambda_2} p)Dh(\alpha). \tag{2.16}$$

Or

$$\frac{T}{d} \sum_{P\in\Lambda_2} \log p \geq \frac{T\log N}{2d} \times \frac{N}{4\log N} \geq \frac{N^2}{16C^2d^2\log(ND)}.$$

Par ailleurs, en utilisant (2.6), on déduit

$$\begin{aligned} (T^2+|\Lambda_2|)\log L &\leq c_7 \left(T^2 + \frac{N}{\log N}\right) \log(ND) \\ &\leq c_7 \left(\frac{N^2}{C^4d^2\log(ND)^2} + \frac{N}{\log\log(5D)}\right) \log(ND) \\ &\leq \frac{N^2}{C^{5/2}d^2\log(ND)} \end{aligned}$$

et

$$(T+|\Lambda_2|)(T+\sum_{P\in\Lambda_2} p) \leq \left(T+\frac{N}{\log N}\right)\left(T+\frac{N^2}{\log N}\right)$$
$$\leq \frac{4N^3}{(\log N)^2}.$$

Finalement, en utilisant (2.5), on obtient

$$h(\alpha) \geq \frac{c_8(\log N)^2}{d^2DN\log(ND)} \geq \frac{c_9\log\log(5D)^2}{d^2DN\log(2D)}$$

donc, par le choix de N,

$$h(\alpha) \geq \frac{c_{10}}{D}\min\left(\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2}, \frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right). \tag{2.17}$$

2.4.3. Conclusion de la preuve du théorème 2.2

Les inégalités (2.7), (2.15) et (2.17) donnent

$$h(\alpha) \geq \frac{c_{11}}{D}\min\left(\frac{\log\log(5D)^3}{d^4\log(2dD)^2\log(2D)}, \frac{\log\log(5D)}{d\lambda}, \frac{\log\log(5D)^4}{d^4\log(2D)^3},\right.$$
$$\left.\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2}, \frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right)$$
$$\geq \frac{c_{12}}{D}\min\left(\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2}, \frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right).$$

2.5. Démonstration du théorème 2.3

La preuve du théorème 2.3 est très similaire à celle du 2.2. Choisissons

$$E = \left[\frac{Cd\log(2D)}{\log\log(5D)}\right]$$

et posons cette fois

$$N = \frac{A^C\log(2D)^3}{\log\log(5D)},$$

où $A = 2g(d)|\Delta_{\mathbb{K}}|$. On a l'encadrement

$$\log\log(5D) \leq \log N \leq c_{13}CA\log\log(5D). \tag{2.18}$$

Nous noterons encore Λ l'ensemble des éléments de $\mathcal{P}$ dont la norme sur $\mathbb{Q}$ est comprise entre $\sqrt{N}$ et N. Le résultat principal de [**Fri80**] déjà cité dans l'introduction montre

$$\#\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ tel que } N_{\mathbb{K}/\mathbb{Q}}(P) \leq N\} \geq \frac{A^{-\rho}N}{(\log N)^2},$$

où ρ est une constante positive. D'où, en utilisant les mêmes arguments que ceux du lemme 2.10,

$$|\Lambda| \geq \frac{A^{-\rho}N}{(\log N)^2} - \frac{2c_1 d\sqrt{N}}{\log N} - \frac{d\log|\Delta_{\mathbb{K}}|}{\log 2} - \frac{2c_1 d\sqrt{N}}{\log N} \geq \frac{A^{-\rho}N}{2(\log N)^2}.$$

Quitte à remplacer Λ par un sous-ensemble, on peut donc supposer

$$\frac{A^{-\rho}N}{2(\log N)^2} \leq |\Lambda| \leq \frac{A^{-\rho}N}{(\log N)^2}.$$

L'argument du sous-paragraphe 2.4.1 montre que s'il existe un premier $P \in \Lambda$ tel que $e_P \geq E$, alors

$$h(\alpha) \geq \frac{\log(2D)}{2DNE} \geq \frac{A^{-c_{14}}}{D}\frac{\log\log(5D)^2}{\log(2D)^3}. \tag{2.19}$$

Supposons maintenant que pour tout $P \in \Lambda$ on ait $e_P \leq E$. Comme dans le sous-paragraphe 2.4.2.1, posons $\Lambda_1 = \{P \in \Lambda \mid 2 \leq e_P \leq E\}$ et supposons dans un premier temps

$$|\Lambda_1| \geq \frac{A^{-\rho}N}{4(\log N)^2}.$$

Reprenons les notations de ce sous-paragraphe, en choisissant

$$T_\tau = \begin{cases} T_{\mathrm{Id}} = \left[\frac{C^3 A d^2 \log(2D)^2}{\log\log(5D)^2}\right] & \text{si } \tau_{|\mathbb{L}} = \mathrm{Id}, \\ T_\sigma = \left[\frac{Cd\log(2D)}{\log\log(5D)}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\right] & \text{si } \tau_{|\mathbb{L}} = \sigma. \end{cases}$$

Rappelons l'inégalité (2.9) :

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\lambda_\sigma A_\sigma\Big) - c_4\log(ND) \leq 2\Big(\sum_{\sigma\in S}\lambda_\sigma\Big)^2 Dh(\alpha), \tag{2.20}$$

où

$$A_\sigma = \frac{\log N}{2d}\left(\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\right) - c_4\lambda_\sigma\log(ND).$$

En utilisant la majoration

$$\lambda_\sigma \leq \frac{2\log\log(5D)}{C^2 Ad\log(2D)} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P} \tag{2.21}$$

valable pour $\sigma \neq \mathrm{Id}$, et l'encadrement (2.18), on a :

$$\begin{aligned} A_\sigma &\geq \left(\frac{\log N}{2d} - \frac{2c_4\log(ND)\log\log(5D)}{C^2 Ad\log(2D)}\right) \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P} \\ &\geq \frac{\log\log(5D)}{4d} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P}, \end{aligned}$$

d'où, en minorant $\sum_{P\in\Lambda(\sigma)} \frac{1}{e_P}$ par $1/E$,

$$A_\sigma \geq \frac{\log\log(5D)^2}{8d^2\log(2D)}. \tag{2.22}$$

En utilisant la minoration

$$\lambda_\sigma \geq \frac{\log\log(5D)}{2C^2 Ad\log(2D)} \sum_{P\in\Lambda(\sigma)} \frac{1}{e_P},$$

l'inégalité (2.18) et la relation (2.12), on obtient

$$\begin{aligned} \sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \lambda_\sigma &\geq \frac{\log\log(5D)}{2C^2 Ad\log(2D)} \times \frac{A^{-\rho}N}{4(\log N)^2} \\ &\geq \frac{\log\log(5D)}{2C^2 Ad\log(2D)} \times \frac{A^{C-\rho}\log(2D)^3}{4c_{13}^2 C^2 A^2 \log\log(5D)^3} \\ &= \frac{A^{C-\rho-3}\log(2D)^2}{8c_{13}^2 C^4 d\log\log(5D)^2}. \end{aligned}$$

Ainsi, (2.22) donne

$$\sum_{\sigma\in S\setminus\{\mathrm{Id}\}} A_\sigma\lambda_\sigma \geq \frac{A^{C-\rho-3}\log(2D)}{64c_{13}^2 C^4 d^3}$$

et, en utilisant (2.18),

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}} \lambda_\sigma A_\sigma\Big) - c_4\log(ND) \geq \log(2D). \tag{2.23}$$

Enfin, en utilisant encore (2.21), (2.12) et (2.18), on obtient

$$\sum_{\sigma\in S}\lambda_\sigma \leq 1+\frac{2\log\log(5D)}{\log(2D)}\times\frac{N}{(\log N)^2}\leq\frac{4A^C\log(2D)^2}{\log\log(5D)^2}. \tag{2.24}$$

En injectant (2.23) et (2.24) dans (2.9), on a alors

$$h(\alpha)\geq\frac{A^{-c_{15}}\log\log(5D)^4}{D\log(2D)^3}. \tag{2.25}$$

Posons maintenant $\Lambda_2=\{P\in\Lambda\ |e_P=1\}$ et supposons

$$|\Lambda_2|\geq\frac{A^{-\rho}N}{4\log N}.$$

Choisissons

$$T=\left[\frac{C^3A^2d\log(2D)^2}{\log\log(5D)^2}\right]$$

et reprenons les notations du sous-paragraphe 2.4.2.2. Réécrivons, pour la commodité du lecteur, l'inégalité (2.16) :

$$\frac{T}{d}\sum_{P\in\Lambda_2}\log p\leq(T^2+|\Lambda_2|)\log L+2(T+|\Lambda_2|)(T+\sum_{P\in\Lambda_2}p)Dh(\alpha).$$

Or

$$\frac{T}{d}\sum_{P\in\Lambda_2}\log p\geq\frac{T\log N}{2d}\times\frac{A^{-\rho}N}{4(\log N)^2}\geq\frac{c_{16}C^2A^{C-\rho+1}\log(2D)^5}{\log\log(5D)^4}.$$

Par ailleurs,

$$\begin{aligned}(T^2+|\Lambda_2|)\log L&\leq c_7\left(T^2+\frac{A^{-\rho}N}{(\log N)^2}\right)\log(ND)\\&\leq c_{17}\left(\frac{C^6A^4d^2\log(2D)^4}{\log\log(5D)^4}+\frac{A^{C-\rho}\log(2D)^3}{\log\log(5D)^3}\right)CA\log(2D)\\&\leq\frac{c_{18}CA^{C-\rho+1}\log(2D)^5}{\log\log(5D)^4}\end{aligned}$$

et

$$(T+|\Lambda_2|)(T+\sum_{P\in\Lambda_2} p) \leq \left(T+\frac{N}{(\log N)^2}\right)\left(T+\frac{N^2}{(\log N)^2}\right)$$

$$\leq \frac{4N^3}{(\log N)^4}$$

$$\leq \frac{4A^{3C}\log(2D)^9}{\log\log(5D)^7}.$$

Finalement, on a

$$h(\alpha) \geq \frac{A^{-c_{19}}\log\log(5D)^3}{\log(2D)^4}. \tag{2.26}$$

Le théorème 2.3 découle des inégalités (2.19), (2.25) et (2.26).

PARTIE II

LE PROBLÈME DE LEHMER RELATIF EN DIMENSION SUPÉRIEURE

CHAPITRE 3

CAS DES HYPERSURFACES

Nous abordons dans ce chapitre le problème de Lehmer « relatif » pour les sous-variétés algébriques d'un tore multiplicatif. Généralisant un théorème de F. Amoroso et U. Zannier, nous montrons que la hauteur normalisée d'une hypersurface qui n'est pas de torsion est minorée en fonction de son indice d'obstruction sur $\mathbb{Q}^{\mathrm{ab}}$, l'extension abélienne maximale de $\mathbb{Q}$. La minoration ainsi obtenue correspond à un ε près à la conjecture la plus précise que l'on peut formuler dans ce cadre.

3.1. Introduction

Nous nous proposons ici de poursuivre l'étude des minorations de la hauteur normalisée des sous-variétés d'un tore amorcée par F. Amoroso et S. David dans [**AmDa99**], [**AmDa00**], [**AmDa03**] et [**AmDa04**]. Soit n un entier naturel non nul. Nous considérons le plongement « naturel » de $\mathbb{G}_{\mathrm{m}}^n$ dans $\mathbb{P}_n$. La hauteur (normalisée) d'un point $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_{\mathrm{m}}^n$ est donc la hauteur de Weil logarithmique et absolue (avec la norme du sup aux places archimédiennes) $\hat{h}(\boldsymbol{\alpha})$ du point projectif $(1 : \alpha_1 : \ldots : \alpha_n)$. P. Philippon ([**Phi91**],[**Phi94**],[**Phi95**]) définit la hauteur normalisée d'une sous-variété V de $\mathbb{G}_{\mathrm{m}}^n$ par :

$$\hat{h}(V) = \lim_{m \to +\infty} \frac{h([m]V)\deg(V)}{m \deg([m]V)},$$

où $h(V)$ (respectivement $\deg(V)$) est la hauteur projective (respectivement le degré) de l'adhérence de Zariski de V dans $\mathbb{P}_n$. L. Szpiro a également introduit le *minimum essentiel* de V, noté $\hat{\mu}^{\mathrm{ess}}(V)$, comme la borne inférieure des nombres réels $\theta > 0$ tels que l'ensemble des points $P \in V(\bar{\mathbb{Q}})$ de hauteur normalisée majorée par θ soit Zariski-dense dans V. Si V est $\bar{\mathbb{Q}}$-irréductible, on

dispose alors de la relation suivante, montrée dans [**Zha95a**] et [**Zha95b**] :

$$\frac{\hat{h}(V)}{(\dim(V)+1)\deg(V)} \leq \hat{\mu}^{\mathrm{ess}}(V) \leq \frac{\hat{h}(V)}{\deg(V)}.$$

Le minimum essentiel et la hauteur normalisée ont la propriété remarquable suivante, montrée encore par S. Zhang (voir [**Zha92**]) : $\hat{\mu}^{\mathrm{ess}}(V) = 0$ (donc $\hat{h}(V) = 0$) si et seulement si V est une variété de torsion, c'est-à-dire une réunion de translatés de sous-tores de $\mathbb{G}_{\mathrm{m}}^n$ par des points de torsion.

Il est donc naturel de chercher à minorer le minimum essentiel (ou la hauteur normalisée) d'une variété qui n'est pas de torsion.

Une telle minoration va dépendre des caractéristiques géométriques de la variété, par exemple son degré. Cependant, si l'on n'impose aucune condition géométrique sur la variété, il faudra également tenir compte de son corps de définition. En effet, soit H un sous-groupe de $\mathbb{G}_{\mathrm{m}}^n$ et soit $(\boldsymbol{\alpha}_i)_{i\geq 0}$ une suite de points qui ne sont pas de torsion et dont la hauteur tend vers 0 (par exemple $\boldsymbol{\alpha}_i = (2^{1/i}, \ldots, 2^{1/i})$). Alors les variétés $V_i = \boldsymbol{\alpha}_i H$ ont toutes même degré $\deg(H)$ mais la suite de leurs minima essentiels $\hat{\mu}^{\mathrm{ess}}(V_i) \leq h(\boldsymbol{\alpha}_i)$ converge vers 0.

Le problème consistant à trouver les meilleures bornes inférieures pour le minimum essentiel des sous-variétés de $\mathbb{G}_{\mathrm{m}}^n$ est une généralisation d'une célèbre question de D. H. Lehmer : existe-t-il une constante $c > 0$ telle que pour tout nombre algébrique α de degré d qui n'est pas une racine de l'unité on ait $h(\alpha) \geq c/d$? Si l'on ne suppose rien de plus sur α, c'est la meilleure minoration possible, étant donné que $h(2^{1/d}) = (\log 2)/d$. Dans cette direction, le meilleur résultat à ce jour est un résultat de E. Dobrowolski [**Dob79**] :

Théorème 3.1. — *Il existe une constante $c > 0$ tel que pour tout nombre algébrique α de degré d qui n'est pas une racine de l'unité :*

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

Cependant F. Amoroso et U. Zannier ont montré dans [**AmZa00**] que l'on a le même type de minoration en remplaçant le degré total de α (c'est-à-dire $[\mathbb{Q}(\alpha) : \mathbb{Q}]$) par le degré « non abélien » de α (c'est-à-dire $[\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}]$ où $\mathbb{Q}^{\mathrm{ab}}$ désigne l'extension abélienne maximale de $\mathbb{Q}$) : c'est le problème de Lehmer « relatif ». Notre but est de généraliser ce résultat en dimension supérieure.

Dans les problèmes de minoration en dimension supérieure, l'invariant le plus fin qui puisse tenir compte de la nature « arithmétique » d'une variété est l'*indice d'obstruction*. Quelques notations sont nécessaires avant d'introduire

cet invariant. Nous fixons donc $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et nous noterons $\mathbb{G}_{\mathrm{m}}^n$ pour $\mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$. Soit V une sous-variété[(1)] de $\mathbb{G}_{\mathrm{m}}^n$ et soit $\mathbb{K}$ un sous-corps de $\bar{\mathbb{Q}}$. Nous utiliserons les notations suivantes : $\mathbb{Q}(V)$ désignera le corps de définition de V, $\mathbb{K}(V)$ le corps $\mathbb{K}\cdot\mathbb{Q}(V)$ et $V_{\mathbb{K}}$ la variété définie par

$$V_{\mathbb{K}} = \bigcup_{\sigma\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{K})} \sigma V.$$

Remarquons que l'on a $\deg V_{\mathbb{K}} = [\mathbb{K}(V):\mathbb{K}]\deg V$.

Définition 3.2. — Soient $Z \subset \mathbb{G}_{\mathrm{m}}^n$ un ensemble algébrique et K un sous-corps de $\bar{\mathbb{Q}}$. On appelle *indice d'obstruction* de Z relativement à K (ou sur K) et on note $\omega_K(Z)$ le plus petit degré d'une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie sur K contenant Z.

En particulier, si V est une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$, $\omega_{\mathbb{K}}(V) = [\mathbb{K}(V):\mathbb{K}]\deg V$.

F. Amoroso et S. David énoncent alors une conjecture généralisant le problème de Lehmer en dimension supérieure et obtiennent dans cette direction le résultat suivant, analogue du théorème de E. Dobrowolski en dimension supérieure :

Théorème 3.3. — *Soit n un entier naturel non nul. Soit W une sous-variété géométriquement irréductible de $\mathbb{G}_{\mathrm{m}}^n$ de codimension k qui n'est contenue dans aucune sous-variété de torsion. Alors*

$$\hat{\mu}^{\mathrm{ess}}(W) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(W)}\log(3\omega_{\mathbb{Q}}(W))^{-\lambda(k)},$$

où $c(n)$ et $\lambda(k)$ sont des nombres réels strictement positifs ne dépendant respectivement que de n et k.

Nous pouvons ainsi énoncer la conjecture « relative » analogue :

Conjecture 3.4. — *Soit n un entier naturel non nul. Soit W une sous-variété géométriquement irréductible de $\mathbb{G}_{\mathrm{m}}^n$ qui n'est contenue dans aucune sous-variété de torsion. Soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Alors*

$$\hat{\mu}^{\mathrm{ess}}(W) \geq \frac{c(n)}{\omega_{\mathbb{L}}(W)}\ ,$$

où $c(n)$ est un nombre réel strictement positif ne dépendant que de n.

(1) Nous appelons variété un ensemble algébrique irréductible sur son corps de définition.

Dans cette direction, en « combinant » les techniques de [**AmDa00**] et [**AmZa00**], nous obtenons le résultat suivant concernant les variétés de codimension 1 :

Théorème 3.5. — *Soit n un entier naturel non nul. Soit W une hypersurface géométriquement irréductible de $\mathbb{G}_{\mathrm{m}}^n$ qui n'est pas de torsion. Soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Alors*

$$\hat{\mu}^{\mathrm{ess}}(W) \geq \frac{c(n)}{\omega_{\mathbb{L}}(W)} \left(\frac{\log 2\omega_{\mathbb{L}}(W)}{\log\log 5\omega_{\mathbb{L}}(W)} \right)^{-(1+6(n+1))},$$

où $c(n)$ est un nombre réel strictement positif ne dépendant que de n.

Remarquons également que pour les hypersurfaces, on peut attaquer ce problème d'un point de vue différent. En effet, dans [**AmDa03**], F. Amoroso et S. David obtiennent, en introduisant des hypothèses supplémentaires, une minoration uniquement de « nature géométrique ».

Théorème 3.6. — *Soit n un entier naturel non nul. Soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Soit W une sous-variété géométriquement irréductible de $\mathbb{G}_{\mathrm{m}}^n$ de codimension k qui n'est contenue dans aucun translaté de sous-tore. Alors*

$$\hat{\mu}^{\mathrm{ess}}(W) \geq \frac{c(n)}{\omega_{\bar{\mathbb{Q}}}(W)} \log(3\omega_{\bar{\mathbb{Q}}}(W))^{-\lambda(k)},$$

où $c(n)$ et $\lambda(k)$ sont des nombres réels strictement positifs ne dépendant respectivement que de n et k.

Ce résultat, appliqué aux hypersurfaces, nous indique que si W est une hypersurface géométriquement irréductible qui n'est pas le translaté d'un sous-tore alors

$$\hat{\mu}^{\mathrm{ess}}(W) \geq \frac{c(n)}{\deg W} \log(3\deg W)^{-81}. \tag{3.1}$$

Pour obtenir un résultat du même type que le théorème 3.5, il suffit donc de ne s'intéresser qu'aux hypersurfaces qui sont des translatés de sous-tores par des points d'ordre infini. Mais dans ce cas on peut facilement se ramener au cas du théorème principal de [**AmZa00**] et obtenir :

Théorème 3.7. — *Soit n un entier naturel non nul. Soit W une hypersurface géométriquement irréductible de $\mathbb{G}_{\mathrm{m}}^n$ qui est le translaté d'un sous-tore par un point d'ordre infini. Alors pour toute extension abélienne $\mathbb{L}$ de $\mathbb{Q}$, on a*

$$\hat{\mu}^{\mathrm{ess}}(W) \geq \frac{c}{n \cdot \omega_{\mathbb{L}}(W)} \left(\frac{\log(2[\mathbb{L}(W) : \mathbb{L}])}{\log\log(5[\mathbb{L}(W) : \mathbb{L}])} \right)^{-13},$$

où c est une constante strictement positive.

Démonstration. — Soient H un sous-tore géométriquement irréductible de codimension 1 et $\boldsymbol{\alpha}$ un point d'ordre infini tels que $W = \boldsymbol{\alpha}H$. En tant que sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ de codimension 1, H est donné par une équation du type $\boldsymbol{X}^{\boldsymbol{\lambda}} = 1$ avec $\boldsymbol{\lambda} \in \mathbb{Z}^n$. Si on pose $\boldsymbol{\mu} = (\mu_1, \dots, \mu_n) \in \mathbb{N}^n$ avec $\mu_i = \max(0, -\lambda_i)$ et $\alpha = \boldsymbol{\alpha}^{\boldsymbol{\lambda}} \in \bar{\mathbb{Q}}$, alors le polynôme $F(\boldsymbol{X}) = \boldsymbol{X}^{\boldsymbol{\mu}}(\boldsymbol{X}^{\boldsymbol{\lambda}} - \alpha)$ est une équation de W et il est clair que $\mathbb{L}(W) = \mathbb{L}(\alpha)$. D'une part, W est une hypersurface donc on a $\hat{h}(W) = \hat{h}(F)$. D'autre part, un simple changement de variables dans les calculs de la mesure de Mahler de F nous donne $\hat{h}(F) = \hat{h}(X - \alpha) = \hat{h}(\alpha)$ (pour les liens entre la hauteur normalisée des hypersurfaces et la mesure de Mahler de leurs équations, voir par exemple, [**Phi91**, section 2, partie B]). Ainsi en appliquant le théorème de [**AmZa00**], on obtient

$$\hat{h}(W) \geq \frac{c}{[\mathbb{L}(W) : \mathbb{L}]} \left(\frac{\log(2[\mathbb{L}(W) : \mathbb{L}])}{\log\log(5[\mathbb{L}(W) : \mathbb{L}])} \right)^{-13}.$$

On conclut alors en utilisant l'inégalité de Zhang. □

En utilisant l'inégalité (3.1) et le théorème 3.7 on peut donc obtenir un résultat du même type que le théorème 3.5 avec une constante absolue comme exposant du terme en « log ». Cependant, cette approche du problème ne fonctionne plus en codimension supérieure.

L'objet de ce chapitre est donc de donner une démonstration directe du théorème 3.5.

3.2. Notations et résultats préliminaires

Soit n un entier naturel non nul. Soient $\boldsymbol{x},\ \boldsymbol{y} \in \mathbb{G}_{\mathrm{m}}^n$ et soit $m \in \mathbb{N}^*$. On notera

$$\boldsymbol{xy} = (x_1 y_1, \cdots, x_n y_n) \quad \text{et} \quad [m]\boldsymbol{x} = (x_1^m, \cdots, x_n^m).$$

On désignera par $\ker[m]$ le noyau du morphisme de multiplication par m dans $\mathbb{G}_{\mathrm{m}}^n$, c'est-à-dire l'ensemble des points dont les coordonnées sont des racines m-ièmes de l'unité. Si V est une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$, on notera G_V son stabilisateur :

$$G_V = \{\boldsymbol{x} \in \mathbb{G}_{\mathrm{m}}^n,\ \boldsymbol{x}V = V\} = \bigcap_{\boldsymbol{y} \in V} \boldsymbol{y}^{-1}V$$

et G_V^0 la composante neutre de G_V. Le stabilisateur de V possède les propriétés suivantes :

$$\dim(G_V) \leq \dim(V) \quad \text{et} \quad \deg(G_V) \leq \deg(V)^{\dim(V)+1}.$$

Par ailleurs, si W est une sous-variété stricte et *géométriquement irréductible* de $\mathbb{G}_{\mathrm{m}}^n$, le degré de son image par le morphisme de multiplication par m vérifie

$$\deg([m]W) = \frac{m^{\dim(W)}\deg(W)}{|\ker[m] \cap G_W|} = \frac{m^{\dim(W)-\dim G_W}\deg(W)}{|\ker[m] \cap (G_W/G_W^0)|},$$

où l'on a encore noté $\ker[m]$ le noyau de la multiplication par m dans $\mathbb{G}_{\mathrm{m}}^n/G_W^0$. On pourra trouver une démonstration de ces résultats dans [**AmDa99**] et [**Hin88**]. Enfin, nous aurons besoin du lemme suivant :

Lemme 3.8. — *Soit W une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ géométriquement irréductible. Soient $\mathbb{K}$ un corps de nombres, p un nombre premier et ζ_p une racine primitive p-ième de l'unité. Alors l'extension*

$$\mathbb{K}([p]W, \zeta_p) \subseteq \mathbb{K}(W, \zeta_p)$$

est abélienne de degré une puissance de p. De plus, si $\mathbb{K}(W, \zeta_p) = \mathbb{K}([p]W, \zeta_p)$, il existe $\boldsymbol{\zeta} \in \ker[p]$ tel que $\mathbb{K}(\boldsymbol{\zeta}W) = \mathbb{K}([p]W)$.

Démonstration. — Soit $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{K}([p]W, \zeta_p))$. Montrons que $\mathbb{K}(W, \zeta_p)$ est globalement stable sous l'action de τ. Pour cela, il suffit de montrer que $\tau(W)$ est définie sur $\mathbb{K}(W, \zeta_p)$. On a

$$[p]\tau(W) = \tau([p]W) = [p]W.$$

Il existe donc $\boldsymbol{\xi} \in \ker[p]$ tel que $\tau(W) = \boldsymbol{\xi}W$ et $\tau(W)$ est définie sur $\mathbb{K}(W, \zeta_p)$. L'extension $\mathbb{K}([p]W, \zeta_p) \subseteq \mathbb{K}(W, \zeta_p)$ est donc galoisienne. D'autre part, si l'on considère l'application

$$\begin{array}{rccc} \phi : & \mathrm{Gal}(\mathbb{K}(W, \zeta_p)/\mathbb{K}([p]W, \zeta_p)) & \longrightarrow & {}^{\ker[p]}/_{\ker[p]\cap G_W} \\ & \tau & \longmapsto & \bar{\boldsymbol{\xi}} \end{array}$$

on vérifie aisément que ϕ est bien définie et que c'est un morphisme injectif. Ainsi $\mathrm{Gal}(\mathbb{K}(W, \zeta_p)/\mathbb{K}([p]W, \zeta_p))$ est isomorphe à son image par ϕ donc est abélien. La première partie du lemme est donc démontrée, passons à la seconde.

Remarquons d'abord que, par hypothèse,

$$\mathbb{K}([p]W) \subseteq \mathbb{K}(W) \subseteq \mathbb{K}(W, \zeta_p) = \mathbb{K}([p]W, \zeta_p).$$

Si $\mathbb{K}(W) = \mathbb{K}([p]W)$ le résultat est trivial. Supposons donc que $\mathbb{K}([p]W) \subsetneq \mathbb{K}(W)$. Soit σ un générateur du groupe cyclique

$$G = \mathrm{Gal}(\mathbb{K}([p]W, \zeta_p)/\mathbb{K}([p]W))$$

et notons $\tilde{\sigma}$ un de ses prolongements à $\bar{\mathbb{Q}}$. Comme $\tilde{\sigma}$ fixe $\mathbb{K}([p]W)$ et *a fortiori* $\mathbb{Q}([p]W)$, on a

$$[p]\tilde{\sigma}(W) = \tilde{\sigma}([p]W) = [p]W.$$

Il existe donc $\boldsymbol{\xi} \in \ker[p]$ tel que $\tilde{\sigma}(W) = \boldsymbol{\xi}W$.

Montrons que $\sigma(\boldsymbol{\xi}) \neq \boldsymbol{\xi}$. Si $\boldsymbol{\xi} = (1, \dots, 1)$ alors $\tilde{\sigma}(W) = W$ et $\mathbb{Q}(W)$ est stable sous l'action de G ; on en déduit que $\mathbb{K}(W) = \mathbb{K}([p]W)$. Par ailleurs, si $\boldsymbol{\xi} \neq (1, \dots, 1)$ et $\sigma\boldsymbol{\xi} = \boldsymbol{\xi}$, alors $\mathbb{K}(\boldsymbol{\xi}) = \mathbb{K}(\zeta_p)$ est stable sous l'action de G ; il s'en suit que G est réduit à l'identité et $\mathbb{K}([p]W) = \mathbb{K}([p]W, \zeta_p)$; *a fortiori* on a encore $\mathbb{K}(W) = \mathbb{K}([p]W)$. Dans les deux cas, on obtient une contradiction avec l'hypothèse $\mathbb{K}(W) \neq \mathbb{K}([p]W)$.

On a donc $\sigma(\boldsymbol{\xi}) = \boldsymbol{\xi}^{\lambda}$, avec $\lambda \in \mathbb{Z}$ et $\lambda \not\equiv 1 \mod p$. Soit u une solution de la congruence

$$(\lambda - 1)u + 1 \equiv 0 \mod p$$

et soit $\boldsymbol{\zeta} = \boldsymbol{\xi}^u$. On a

$$\tilde{\sigma}(\boldsymbol{\zeta}W) = \sigma(\boldsymbol{\zeta})\tilde{\sigma}(W) = \boldsymbol{\xi}^{\lambda u+1}W = \boldsymbol{\zeta}W,$$

ce qui montre que $\mathbb{Q}(\boldsymbol{\zeta}W)$ (donc $\mathbb{K}(\boldsymbol{\zeta}W)$) est stable sous l'action de G, et ainsi $\mathbb{K}(\boldsymbol{\zeta}W) \subseteq \mathbb{K}([p]W)$. D'autre part, $[p](\boldsymbol{\zeta}W) = [p]W$, donc ces deux corps sont égaux, ce qui achève la démonstration. □

3.3. Réductions

Soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. D'après le théorème de Kronecker-Weber, $\mathbb{L}$ est contenu dans une extension cyclotomique de $\mathbb{Q}$. Soit $m \in \mathbb{N}^*$ minimal tel que $\mathbb{L} \subseteq \mathbb{Q}(\zeta_m)$. Si p est un nombre premier, on note $e_p(\mathbb{L})$ son indice de ramification dans $\mathbb{L}$ et $\tilde{e_p}(\mathbb{L})$ la puissance maximale de p divisant m. On définit également

$$\tilde{e}(\mathbb{L}) = \sum_{p \text{ premier}} (\tilde{e_p}(\mathbb{L}) - 1).$$

Remarquons que si $\mathbb{L}' \subseteq \mathbb{L}$ sont deux extensions abéliennes de $\mathbb{Q}$ alors $\tilde{e}(\mathbb{L}') \leq \tilde{e}(\mathbb{L})$.

Pour démontrer le théorème 3.5, on raisonne par l'absurde. Supposons donc qu'il existe $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et W une hypersurface géométriquement irréductible de $\mathbb{G}_{\mathrm{m}}^n$ non de torsion telles que le théorème 3.5 soit faux :

$$\hat{\mu}^{\mathrm{ess}}(W) < \frac{c(n)}{\omega_{\mathbb{L}}(W)} \left(\frac{\log 2\omega_{\mathbb{L}}(W)}{\log\log 5\omega_{\mathbb{L}}(W)} \right)^{-(1+6(n+1))}. \tag{3.2}$$

Nous pouvons supposer de plus que le degré $\delta = [\mathbb{L}(W) : \mathbb{L}]$ est minimal dans (3.2) : pour toute hypersurface géométriquement irréductible W' qui n'est pas de torsion et telle qu'il existe une extension abélienne $\mathbb{L}'$ de $\mathbb{Q}$ vérifiant $[\mathbb{L}'(W') : \mathbb{L}'] < \delta$, on a

$$\hat{\mu}^{\mathrm{ess}}(W') \geq \frac{c(n)}{\omega_{\mathbb{L}'}(W')} \left(\frac{\log 2\omega_{\mathbb{L}'}(W')}{\log\log 5\omega_{\mathbb{L}'}(W')} \right)^{-(1+6(n+1))}. \tag{3.3}$$

Remarquons ensuite que la fonction

$$t \mapsto t \left(\frac{\log(2(\deg W)t)}{\log\log(5(\deg W)t)} \right)^{1+6(n+1)}$$

est croissante sur $[1; +\infty[$. De plus, pour tout $\boldsymbol{\zeta} \in (\mathbb{G}_{\mathrm{m}}^n)_{\mathrm{tors}}$, on a $\deg(\boldsymbol{\zeta}W) = \deg(W)$ et $\hat{\mu}^{\mathrm{ess}}(\boldsymbol{\zeta}W) = \hat{\mu}^{\mathrm{ess}}(W)$. En particulier, (3.2) et (3.3) impliquent que pour tout $\boldsymbol{\zeta} \in (\mathbb{G}_{\mathrm{m}}^n)_{\mathrm{tors}}$ et toute extension abélienne $\mathbb{L}'$ de $\mathbb{Q}$, on a

$$[\mathbb{L}'(\boldsymbol{\zeta}W) : \mathbb{L}'] \geq \delta. \tag{3.4}$$

Enfin, soit $\mathcal{A}$ l'ensemble des extensions abéliennes $\mathbb{L}'$ de $\mathbb{Q}$ telles qu'il existe $\boldsymbol{\zeta} \in (\mathbb{G}_{\mathrm{m}}^n)_{\mathrm{tors}}$ vérifiant $[\mathbb{L}'(\boldsymbol{\zeta}W) : \mathbb{L}'] = \delta$. Posons

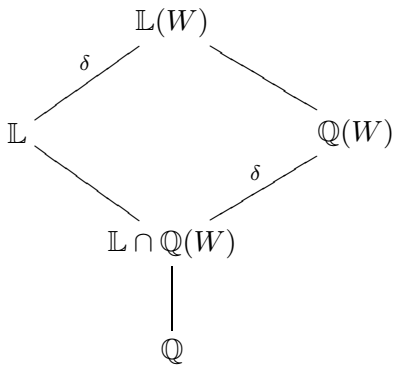
$$\tilde{e} = \min_{\mathbb{L} \in \mathcal{A}} \tilde{e}(\mathbb{L}).$$

Quitte à remplacer W par $\boldsymbol{\zeta}W$ pour un certain $\boldsymbol{\zeta} \in (\mathbb{G}_{\mathrm{m}}^n)_{\mathrm{tors}}$ et $\mathbb{L}$ par $\mathbb{L}' \in \mathcal{A}$, nous pouvons supposer que $\mathbb{L}$ vérifie les deux conditions suivantes :

$$[\mathbb{L}(W) : \mathbb{L}] = \delta, \tag{3.5}$$

$$\tilde{e}(\mathbb{L}) = \tilde{e}. \tag{3.6}$$

De plus, par un argument galoisien, nous avons le diagramme



Étant donné que $\mathbb{L} \cap \mathbb{Q}(W)$ est une extension abélienne de $\mathbb{Q}$ et que

$$\tilde{e}(\mathbb{L} \cap \mathbb{Q}(W)) \leq \tilde{e}(\mathbb{L}) = \tilde{e},$$

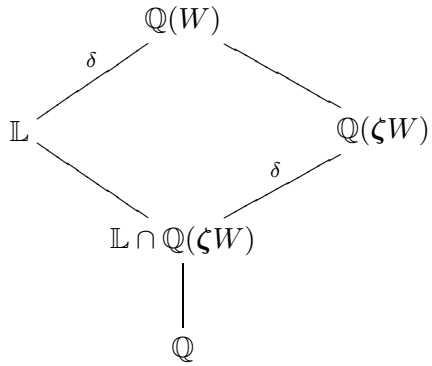
on a $\tilde{e}(\mathbb{L} \cap \mathbb{Q}(W)) = \tilde{e}$. Cela nous permet de supposer, quitte à remplacer $\mathbb{L}$ par $\mathbb{L} \cap \mathbb{Q}(W)$, que $\mathbb{L} \subseteq \mathbb{Q}(W)$, c'est-à-dire

$$\mathbb{Q}(W) = \mathbb{L}(W). \tag{3.7}$$

Remarquons enfin que l'on peut également supposer

$$\forall \boldsymbol{\zeta} \in (\mathbb{G}_{\mathrm{m}}^n)_{\mathrm{tors}}, \quad \mathbb{Q}(\boldsymbol{\zeta}W) \subseteq \mathbb{Q}(W) \Rightarrow \mathbb{Q}(\boldsymbol{\zeta}W) = \mathbb{Q}(W). \tag{3.8}$$

En effet, s'il existe $\boldsymbol{\zeta}$ tel que $\mathbb{Q}(\boldsymbol{\zeta}W) \subsetneq \mathbb{Q}(W)$, nous avons $\mathbb{L}(\boldsymbol{\zeta}W) \subseteq \mathbb{L}(W)$, ce qui implique nécessairement (par 3.4) $\mathbb{L}(\boldsymbol{\zeta}W) = \mathbb{L}(W) = \mathbb{Q}(W)$. Nous avons ainsi le diagramme



Par le même argument, nous pouvons donc remplacer W par $\boldsymbol{\zeta}W$ et $\mathbb{L}$ par $\mathbb{L} \cap \mathbb{Q}(\boldsymbol{\zeta}W)$. Nous pouvons itérer ce procédé, jusqu'à obtenir (3.8) (nombre d'itérations fini car le degré décroît strictement à chaque étape).

Ainsi, nous considérons désormais une hypersurface géométriquement irréductible W qui n'est pas de torsion et une extension abélienne $\mathbb{L}$ de $\mathbb{Q}$ contenue dans $\mathbb{Q}(W)$ qui satisfont (3.2), (3.3), (3.4), (3.5), (3.6), (3.7) et (3.8).

Notation. Soit $m \in \mathbb{N}^*$. Dans toute la suite, nous noterons V_m la variété définie par

$$V_m = \bigcup_{\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L})} [m]\sigma(W) = [m]W_{\mathbb{L}}. \tag{3.9}$$

On définit également un ensemble de premiers « exceptionnels » :

$$E_{\mathrm{exc}}(V_1) = \{p \text{ premiers}, p \mid |G_{V_1}/G_{V_1}^0|\},$$

et on note $\mathcal{P}$ son complémentaire dans l'ensemble des nombres premiers. Enfin, nous noterons s la dimension du stabilisateur de W.

Lemme 3.9. — *Soit $p \in \mathcal{P}$. Alors*

i) p ne divise pas $|G_W/G_W^0|$,

ii) $\mathbb{L}([p]W) = \mathbb{L}(W)$,
iii) $\deg(V_p) = p^{n-1-s}\omega_{\mathbb{L}}(W)$.

Démonstration. — *i)* On montre facilement que $G_W \subseteq G_{V_1}$ et $G_W^0 = G_{V_1}^0$. Ainsi G_W/G_W^0 est un sous-groupe de $G_{V_1}/G_{V_1}^0$ et p ne divise pas $|G_W/G_W^0|$.

ii) Il suffit de montrer que $\mathbb{L}([p]W, \zeta_p) = \mathbb{L}(W, \zeta_p)$: le lemme 3.8 nous indique alors l'existence de $\boldsymbol{\zeta} \in \ker([p])$ tel que $\mathbb{L}(\boldsymbol{\zeta}W) = \mathbb{L}([p]W)$. Les hypothèses (3.4) et (3.5) faites sur W nous donnent ainsi :

$$\delta = [\mathbb{L}(W) : \mathbb{L}] \geq [\mathbb{L}([p]W) : \mathbb{L}] = [\mathbb{L}(\boldsymbol{\zeta}W) : \mathbb{L}] \geq \delta.$$

On en déduit $\mathbb{L}([p]W) = \mathbb{L}(W)$.

Considérons l'extension abélienne

$$\mathbb{L}([p]W, \zeta_p) \subseteq \mathbb{L}(W, \zeta_p).$$

Supposons qu'il existe un élément $\sigma \neq \mathrm{Id}$ dans $\mathrm{Gal}(\mathbb{L}(W, \zeta_p)/\mathbb{L}([p]W, \zeta_p))$ et notons $\tilde{\sigma}$ un de ses prolongements à $\bar{\mathbb{Q}}$. On a

$$[p]\tilde{\sigma}W = \tilde{\sigma}[p]W = [p]W$$

donc il existe $\boldsymbol{\xi} \in \ker[p]$ différent de $(1, \ldots, 1)$ vérifiant $\tilde{\sigma}(W) = \boldsymbol{\xi}W$. Pour $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L})$, il existe $l \in \mathbb{Z}$ tel que que $\tau^{-1}\boldsymbol{\xi} = \boldsymbol{\xi}^l$. Puisque $\sigma(\boldsymbol{\xi}) = \boldsymbol{\xi}$ on a

$$\boldsymbol{\xi}\tau(W) = \tau(\boldsymbol{\xi}^l W) = (\tau \circ \tilde{\sigma}^l)(W).$$

Donc $\boldsymbol{\xi} \in G_{V_1}$. Mais comme $G_{V_1}^0 = G_W^0$ et $\sigma \neq \mathrm{Id}$, on a $\boldsymbol{\xi} \notin G_{V_1}^0$. On en déduit que p divise $|G_{V_1}/G_{V_1}^0|$, ce qui contredit l'hypothèse $p \in \mathcal{P}$. On a donc bien $\mathbb{L}([p]W, \zeta_p) = \mathbb{L}(W, \zeta_p)$ et le point (ii) est établi.

iii) Le point précédent nous assure que $[p]W$ et W ont le même nombre $[\mathbb{L}(W) : \mathbb{L}]$ de conjugués au-dessus de $\mathbb{L}$. D'où

$$\deg(V_p) = [\mathbb{L}(W) : \mathbb{L}] \deg([p]W).$$

Or, d'après (i), $|\ker[p] \cap G_W/G_W^0| = 1$. Donc $\deg([p]W) = p^{n-1-s} \deg W$, et la preuve du lemme est achevée.

□

3.4. Lemmes pour l'extrapolation

Lemme 3.10. — *Soit p un nombre premier. Soit $(\pi_1 \cdots \pi_r)^{e_p(\mathbb{L})}$ la décomposition de (p) dans $\mathcal{O}_{\mathbb{L}}$. Alors il existe un élément Φ_p du groupe de Galois $Gal(\mathbb{L}/\mathbb{Q})$ tel que pour tout entier algébrique $\gamma \in \mathbb{L}$, on a*

$$\gamma^p - \Phi_p\gamma \equiv 0 \mod \pi_1 \cdots \pi_r.$$

Démonstration. — Voir le lemme 3.1 de [**AmZa00**]. □

Lemme 3.11. — *Soit $p \in \mathcal{P}$. Alors il existe un sous-groupe H_p de* $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ *d'ordre*

$$|H_p| \geq \min\{e_p(\mathbb{L}), p\}$$

tel que, pour tout entier algébrique $\gamma \in \mathbb{L}$ et pour tout $\sigma \in H_p$, on a

$$\gamma^p - \sigma\gamma^p \equiv 0 \mod p\mathcal{O}_{\mathbb{L}}. \tag{3.10}$$

et, pour tout prolongement $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ de $\sigma \in H_p \backslash \{\mathrm{Id}\}$,

$$\tau[p]W \neq [p]W.$$

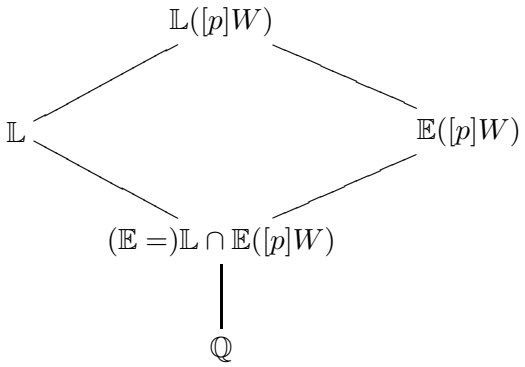
Démonstration. — Si p n'est pas ramifié dans $\mathbb{L}$ alors $e_p(\mathbb{L}) = 1$ et $H_p = \{\mathrm{Id}\}$, auquel cas le lemme est trivial. Si p est ramifié dans $\mathbb{L}$ alors p est également ramifié dans $\mathbb{Q}(\zeta_m)$, donc $p|m$. Notons G_p le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p}))$ qui est cyclique d'ordre p si $p^2|m$, d'ordre $p-1$ sinon. Par minimalité de m, $\mathbb{L}$ n'est pas stable sous l'action de G_p donc G_p induit par restriction un sous-groupe non trivial H_p de $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Si $p^2|m$, alors nécessairement $|H_p| = p$. Si $p^2 \nmid m$, alors $|H_p|$ divise $(p-1)$ et $|H_p| \geq e_p(\mathbb{L})$ car p n'est pas ramifié dans $\mathbb{Q}(\zeta_{m/p})$.

Soit $\gamma \in \mathbb{L}$ un entier algébrique. En particulier, γ est un entier de $\mathbb{Q}(\zeta_m)$, donc s'écrit $\gamma = f(\zeta_m)$, avec $f \in \mathbb{Z}[X]$. Soit $\sigma \in H_p$. Cet automorphisme est la restriction à $\mathbb{L}$ d'un certain $\tilde{\sigma} \in G_p$. Comme $\mathbb{Q}(\zeta_{m/p})$ est stable par l'action de $\tilde{\sigma}$, on a $\tilde{\sigma}(\zeta_m^p) = \zeta_m^p$. On obtient ainsi, à l'aide du petit théorème de Fermat :

$$\tilde{\sigma}\gamma^p = \tilde{\sigma}f(\zeta_m)^p \equiv \tilde{\sigma}f(\zeta_m^p) = f(\zeta_m^p) \equiv \gamma^p \mod p\mathbb{Z}[\zeta_m].$$

Ce qui, par restriction à $\mathbb{L}$, nous donne (3.10).

Enfin, soient $\sigma \in H_p \backslash \{\mathrm{Id}\}$ et $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ un prolongement de σ. Supposons que $\tau[p]W = [p]W$. Ceci équivaut à dire que $\mathbb{Q}([p]W)$ est stable sous l'action de τ. Notons $\mathbb{E}$ le sous-corps de $\mathbb{L}$ fixé par σ. On a alors $\mathbb{Q}([p]W) \cap \mathbb{L} \subseteq \mathbb{E}$ donc $\mathbb{E}([p]W) \cap \mathbb{L} = \mathbb{E}$. Par un argument galoisien, les « côtés » opposés du diagramme suivant ont même degré :



On en déduit

$$[\mathbb{L}([p]W) : \mathbb{E}([p]W)] = [\mathbb{L} : \mathbb{E}].$$

De plus, par le lemme 3.9 et l'égalité (3.7), on a

$$\mathbb{L}([p]W) = \mathbb{L}(W) = \mathbb{Q}(W). \tag{3.11}$$

Ainsi $[\mathbb{Q}(W) : \mathbb{E}([p]W)] = [\mathbb{L} : \mathbb{E}]$. D'une part, comme $\mathbb{E} \subsetneq \mathbb{L}$ (sinon $\sigma = \mathrm{Id}$), on a $[\mathbb{L} : \mathbb{E}] > 1$. D'autre part, comme l'extension $\mathbb{L}/\mathbb{E}$ est galoisienne,

$$[\mathbb{L} : \mathbb{E}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{E})| = \mathrm{ordre}(\sigma) \leq |H_p| \leq p. \tag{3.12}$$

On a donc l'encadrement

$$2 \leq [\mathbb{Q}(W) : \mathbb{E}([p]W)] \leq p. \tag{3.13}$$

Nous allons montrer que ce degré est exactement p. Pour cela considérons une racine primitive p-ième de l'unité, notons-la ζ_p, et les extensions cycliques $\mathbb{Q}(W, \zeta_p)/\mathbb{Q}(W)$, $\mathbb{E}([p]W, \zeta_p)/\mathbb{E}([p]W)$ et $\mathbb{Q}([p]W, \zeta_p)/\mathbb{Q}([p]W)$ dont le degré divise $p - 1$. Remarquons que l'on a (voir (3.11))

$$\mathbb{Q}([p]W, \zeta_p) \subseteq \mathbb{E}([p]W, \zeta_p) \subseteq \mathbb{L}([p]W, \zeta_p) = \mathbb{L}(W, \zeta_p) = \mathbb{Q}(W, \zeta_p).$$

Par ailleurs, par le lemme 3.8, l'extension $\mathbb{Q}(W, \zeta_p)/\mathbb{Q}([p]W, \zeta_p)$ est abélienne de degré une puissance de p. Il en est donc de même pour l'extension intermédiaire $\mathbb{Q}(W, \zeta_p)/\mathbb{E}([p]W, \zeta_p)$. Supposons que $\mathbb{Q}(W, \zeta_p) = \mathbb{E}([p]W, \zeta_p)$. On a

$$\mathbb{E}([p]W, \zeta_p) \subseteq \mathbb{E}(W, \zeta_p) \subseteq \mathbb{L}(W, \zeta_p) = \mathbb{Q}(W, \zeta_p)$$

donc $\mathbb{E}(W, \zeta_p) = \mathbb{E}([p]W, \zeta_p)$. Le lemme 3.8 implique alors l'existence d'un $\boldsymbol{\zeta} \in \ker[p]$ tel que $\mathbb{E}(\boldsymbol{\zeta}W) = \mathbb{E}([p]W)$. Ainsi :

$$\mathbb{Q}(\boldsymbol{\zeta}W) \subseteq \mathbb{E}(\boldsymbol{\zeta}W) = \mathbb{E}([p]W) \subseteq \mathbb{L}([p]W) = \mathbb{L}(W) = \mathbb{Q}(W).$$

L'hypothèse (3.8) faite sur W implique que ces six corps sont égaux ; en particulier $\mathbb{Q}(W) = \mathbb{E}([p]W)$, ce qui est impossible d'après (3.13). Donc $[\mathbb{Q}(W,\zeta_p) : \mathbb{E}([p]W,\zeta_p)] = p^\alpha$, avec $\alpha \geq 1$. Ainsi p divise

$$[\mathbb{Q}(W,\zeta_p) : \mathbb{E}([p]W)] = [\mathbb{Q}(W,\zeta_p) : \mathbb{Q}(W)][\mathbb{Q}(W) : \mathbb{E}([p]W)].$$

Or $[\mathbb{Q}(W,\zeta_p) : \mathbb{Q}(W)]$ divise $p-1$ donc, par le lemme de Gauss, p divise $[\mathbb{Q}(W) : \mathbb{E}([p]W)]$. L'encadrement (3.13) implique alors

$$[\mathbb{Q}(W) : \mathbb{E}([p]W)] = p.$$

On a ainsi montré que $[\mathbb{L} : \mathbb{E}] = [\mathbb{Q}(W) : \mathbb{E}([p]W)] = p$. On déduit alors de (3.12) que le cardinal de H_p est p. Il en est donc de même pour G_p. Notons q la quantité $\tilde{e}_p(\mathbb{L})$ et fixons une racine primitive q-ième de l'unité $\zeta_q = \zeta_m^{(m/q)}$. Comme $\mathbb{L}(\zeta_q) \subseteq \mathbb{Q}(\zeta_m)$, le groupe de Galois G_p induit par restriction un sous-groupe non trivial de $\mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{Q})$, qui est nécessairement cyclique d'ordre p. Notons $\mathbb{F}$ le corps fixé par ce sous-groupe et ρ un générateur de $\mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{F})$. Alors $\mathbb{E} \subseteq \mathbb{F}$ et

$$\rho\zeta_q = \tilde{\zeta}_p\zeta_q \tag{3.14}$$

où $\tilde{\zeta}_p$ est une racine primitive p-ième de l'unité.

Nous allons montrer qu'il existe $\boldsymbol{\zeta} \in (\mathbb{G}_{\mathrm{m}}^n)_{\mathrm{tors}}$ tel que $\mathbb{F}(\boldsymbol{\zeta}W) \subseteq \mathbb{F}([p]W)$. Nous pouvons supposer que $\mathbb{F}([p]W) \subsetneq \mathbb{F}(W)$, sinon notre affirmation est triviale ; donc $\mathbb{F}([p]W) \subsetneq \mathbb{L}(W,\zeta_q)$. De plus, par un argument galoisien, on a $[\mathbb{L}([p]W,\zeta_q) : \mathbb{F}([p]W)]$ qui divise $[\mathbb{L}(\zeta_q) : \mathbb{F}] = p$. Or $\mathbb{L}([p]W,\zeta_q) = \mathbb{L}(W,\zeta_q)$, donc

$$[\mathbb{L}(W,\zeta_q) : \mathbb{F}([p]W)] = [\mathbb{L}([p]W,\zeta_q) : \mathbb{F}([p]W)] = p.$$

En utilisant de nouveau un argument galoisien, on obtient que la restriction

$$r : \mathrm{Gal}(\mathbb{L}(W,\zeta_q)/\mathbb{F}([p]W)) \to \mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{F})$$

est un isomorphisme de groupes. Soit $\tilde{\rho}$ un générateur de $\mathrm{Gal}(\mathbb{L}(W,\zeta_q)/\mathbb{F}([p]W))$ tel que $\tilde{\rho}_{|\mathbb{L}(\zeta_q)} = \rho$. Il existe alors $\boldsymbol{\xi} = (\tilde{\zeta}_p^{\alpha_1}, \ldots, \tilde{\zeta}_p^{\alpha_n}) \in \ker[p]$ tel que

$$\tilde{\rho}W = \boldsymbol{\xi}W$$

et, par (3.14),

$$\tilde{\rho}\zeta_q = \tilde{\zeta}_p\zeta_q.$$

Si on pose $\boldsymbol{\zeta} = (\zeta_q^{-\alpha_1}, \ldots, \zeta_q^{-\alpha_n})$, alors on a

$$\tilde{\rho}(\boldsymbol{\zeta}W) = \tilde{\rho}(\boldsymbol{\zeta})\tilde{\rho}(W) = (\tilde{\zeta}_p^{-\alpha_1}\zeta_q^{-\alpha_1}, \ldots, \tilde{\zeta}_p^{-\alpha_n}\zeta_q^{-\alpha_n})\boldsymbol{\xi}W = \boldsymbol{\zeta}W.$$

Ainsi $\boldsymbol{\zeta}W$ est stable sous l'action de $\mathrm{Gal}(\mathbb{L}(W,\zeta_q)/\mathbb{F}([p]W))$ donc $\mathbb{F}(\boldsymbol{\zeta}W) \subseteq \mathbb{F}([p]W)$.

On en déduit

$$[\mathbb{F}(\boldsymbol{\zeta}W):\mathbb{F}] \leq [\mathbb{F}([p]W):\mathbb{F}] \leq [\mathbb{E}([p]W):\mathbb{E}] = \delta.$$

Or, comme $\mathbb{F} \subseteq \mathbb{Q}(\zeta_{m/p})$, on a $\tilde{e}(\mathbb{F}) < \tilde{e}(\mathbb{L})$. On vient ainsi de contredire l'hypothèse (3.6) faite sur W, ce qui achève la démonstration du lemme. □

3.5. Construction de la fonction auxiliaire

Soit S un sous-espace vectoriel de $\bar{\mathbb{Q}}^l$ de dimension d. On définit la hauteur h_2 de S comme le fait W. Schmidt (voir [**Sch96**, chap 1, §8]) par

$$h_2(S) = \sum_v \frac{[\mathbb{F}_v : \mathbb{Q}_v]}{[\mathbb{F} : \mathbb{Q}]} \log ||\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_d||_{v,L_2} \ ,$$

où $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d$ est une base de S sur un corps de nombres $\mathbb{F}$ quelconque sur lequel S est rationnel, et $||\cdot||_{v,L_2}$ est la norme du sup si v est ultramétrique, la norme euclidienne sinon. Pour $\boldsymbol{x} \in \bar{\mathbb{Q}}^l$, nous noterons $h_2(\boldsymbol{x})$ la hauteur du sous-espace engendré par $\boldsymbol{x}$.

Nous énonçons maintenant un théorème permettant de construire une fonction auxiliaire dont le degré et la hauteur sont contrôlés.

Théorème 3.12. — *Soit V une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ de degré Ω. Soient L et T deux entiers naturels non nuls tels que $L \geq \Omega T$. Alors, pour tout ε strictement positif, il existe un polynôme non nul $F \in \bar{\mathbb{Q}}[X_1, \cdots, X_n]$ à coefficients entiers algébriques, de degré inférieur ou égal à L, identiquement nul sur V à un ordre supérieur ou égal à T tel que*

$$h_2(F) \leq r\Big((T+n)\log(L+1) + L(\hat{\mu}^{\mathrm{ess}}(V) + \varepsilon)\Big) + \frac{1}{2}\log\binom{L+n}{n}$$

avec

$$r = \frac{\binom{L+n}{n} - \binom{L-\Omega T+n}{n}}{\binom{L-\Omega T+n}{n}}$$

et où, par définition, la hauteur d'un polynôme est la hauteur de la famille de ses coefficients.

Démonstration. — Nous noterons encore V l'adhérence de Zariski de V dans $\mathbb{P}_n$. Soit $P \in \bar{\mathbb{Q}}[X_0, \cdots, X_n]$, homogène, générateur de l'idéal associé à V (on a $\deg P = \Omega$). L'ensemble E des polynômes homogènes de $\bar{\mathbb{Q}}[X_0, \cdots, X_n]$ de degré L identiquement nuls à un ordre supérieur ou égal à T sur V est constitué des polynômes $G.P^T$, où $G \in \bar{\mathbb{Q}}[X_0, \cdots, X_n]$ est homogène de degré $L-\Omega T$. Si on y ajoute le polynôme nul, c'est un $\bar{\mathbb{Q}}$-espace vectoriel de dimension $\binom{L-\Omega T+n}{n}$.

La démonstration est alors exactement celle du théorème 2.2 de [**AmDa03**] où l'on a substitué $E \cup \{0\}$ à $[\mathfrak{P}^{(T)}]_L$ et $H(\mathfrak{P}^{(T)}; L)$ à $\binom{L+n}{n} - \binom{L-\Omega T+n}{n}$. Nous obtenons ainsi un polynôme F à coefficients algébriques qui satisfait les propriétés voulues. Quitte à multiplier F par un entier algébrique (ce qui ne modifie en rien sa hauteur), on peut supposer que F est à coefficients entiers algébriques, ce qui donne le résultat souhaité. □

Corollaire 3.13. — *Soit V une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ de degré Ω, qui n'est pas de torsion. Soient L et T deux entiers naturels non nuls tels que $L \geq 2\Omega T$. Alors il existe un polynôme non nul $F \in \bar{\mathbb{Q}}[X_1, \cdots, X_n]$ à coefficients entiers algébriques, de degré inférieur ou égal à L, nul sur V à un ordre supérieur ou égal à T tel que*

$$h_2(F) \leq \frac{2^{n+1}\Omega T}{L}\Big((T+n)\log(L+1) + 2L\hat{\mu}^{\mathrm{ess}}(V)\Big) + \frac{n}{2}\log(L+1).$$

Démonstration. — Comme V n'est pas de torsion, il suffit d'appliquer le théorème précédent avec $\varepsilon = \hat{\mu}^{\mathrm{ess}}(V)$, d'utiliser l'inégalité $\binom{L+n}{n} \leq (L+1)^n$ et de remarquer que si $L \geq 2\Omega T$, on a

$$\frac{\binom{L+n}{n} - \binom{L-\Omega T+n}{n}}{\binom{L-\Omega T+n}{n}} \leq \frac{2^{n+1}\Omega T}{L}.$$

□

3.6. Extrapolation

Nous utiliserons à plusieurs reprises un lemme d'approximation qui permet d'exhiber un « dénominateur commun » local :

Lemme 3.14. — *Soient $\mathbb{K}$ un corps de nombres, v_0 une place ultramétrique de $\mathbb{K}$ et $\gamma_1, \ldots, \gamma_n$ des éléments de $\mathbb{K}$. Alors il existe un élément $\beta \in \mathcal{O}_{\mathbb{K}}$ tel que $\beta\gamma_1, \ldots, \beta\gamma_n \in \mathcal{O}_{\mathbb{K}}$ et $|\beta|_{v_0} = \max\{1, |\gamma_1|_{v_0}, \ldots, |\gamma_n|_{v_0}\}^{-1}$.*

Démonstration. — Fixons une place archimédienne quelconque $\tilde{v}$ et notons Σ l'ensemble fini

$$\Sigma = \{v \in \mathcal{M}_k \mid v \nmid \infty \text{ et } \max\{|\gamma_1|_v, \ldots, |\gamma_n|_v\} > 1\} \cup \{v_0\}.$$

Pour toute place $v \in \Sigma$, notons θ_v^{-1} celui des éléments de $\gamma_1, \ldots, \gamma_n$ de valeur absolue maximale en v (si $v = v_0$ et si $\max\{|\gamma_1|_{v_0}, \ldots, |\gamma_n|_{v_0}\} < 1$, on pose

$\theta_{v_0} = 1$). D'après le théorème de [**CF67**, chap. II, 15, page 67], il existe un élément $\beta \in \mathbb{K}$ tel que

$$\begin{cases} |\beta - \theta_v|_v < \max\{1, |\gamma_1|_v, \dots, |\gamma_n|_v\}^{-1} & \text{pour tout } v \in \Sigma, \\ |\beta|_v \leq 1 & \text{si } v \notin \Sigma \cup \{\tilde{v}\}. \end{cases}$$

En utilisant l'inégalité ultramétrique, on en déduit

$$\begin{cases} |\beta|_v = \max\{1, |\gamma_1|_v, \dots, |\gamma_n|_v\}^{-1} & \text{pour tout } v \in \Sigma, \\ |\beta|_v \leq 1 & \text{si } v \notin \Sigma \cup \{\tilde{v}\}. \end{cases}$$

En particulier, pour toute place finie v de $\mathbb{K}$ on a $|\beta|_v \leq 1$ (donc $\beta \in \mathcal{O}_{\mathbb{K}}$) et pour tout $i \in [\![1, n]\!]$, $|\beta\gamma_i|_v \leq 1$ (donc $\beta\gamma_i \in \mathcal{O}_{\mathbb{K}}$). Enfin, on a bien $|\beta|_{v_0} = \max\{1, |\gamma_1|_{v_0}, \dots, |\gamma_n|_{v_0}\}^{-1}$ car $v_0 \in \Sigma$. Le lemme est donc établi. □

Proposition 3.15. — *Soit p un nombre premier et soient T_1 et L_1 deux entiers naturels non nuls. Supposons qu'il existe un polynôme non nul F_1 à coefficients entiers algébriques, de degré au plus L_1, identiquement nul sur V_1 avec multiplicité supérieure ou égale à T_1. Soit v une valuation sur $\bar{\mathbb{Q}}$ qui prolonge la valuation p-adique. Alors, pour tout $\boldsymbol{\alpha} \in W$ et pour tout τ qui prolonge Φ_p, on a*

$$|F_1^\tau(\boldsymbol{\alpha}^p)|_v \leq p^{-T_1/e_p(\mathbb{L})} \max\{1, |\alpha_1|_v, \cdots, |\alpha_n|_v\}^{pL_1}.$$

Démonstration. — Si $p\mathcal{O}_{\mathbb{L}} = (\pi_1 \cdots \pi_r)^{e_p(\mathbb{L})}$, notons Q l'idéal $\pi_1 \cdots \pi_r$. Soient $\alpha \in W$ et $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ un prolongement de Φ_p. D'après le lemme 3.14, il existe une équation réduite $f \in \mathcal{O}_{\mathbb{L}}[\boldsymbol{X}]$ de V_1 telle que $|f^\tau|_v = 1$.

Par le petit théorème de Fermat et le lemme 3.10, on a

$$f(\boldsymbol{X})^p \equiv f^\tau(\boldsymbol{X}^p) \mod Q\mathcal{O}_{\mathbb{L}}[\boldsymbol{X}].$$

En utilisant de nouveau le lemme 3.14, il existe $\eta \in \mathcal{O}_{\mathbb{Q}(\boldsymbol{\alpha})}$ tel que

$$\eta\alpha_1, \dots, \eta\alpha_n \in \mathcal{O}_{\mathbb{Q}(\boldsymbol{\alpha})} \quad \text{et} \quad |\eta|_v = \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{-1}.$$

On a alors

$$|\eta^{p\deg(f)} f^\tau(\boldsymbol{\alpha}^p)|_v = |\eta^{p\deg(f)} f(\boldsymbol{\alpha})^p - \eta^{p\deg(f)} f^\tau(\boldsymbol{\alpha}^p)|_v \leq p^{-1/e_p(\mathbb{L})}.$$

Donc

$$|f^\tau(\boldsymbol{\alpha}^p)|_v \leq p^{-1/e_p(\mathbb{L})} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{p\deg(f)}.$$

Comme F_1 est à coefficients entiers algébriques et $|f^\tau|_v = 1$, nous avons la factorisation $F_1 = q \cdot f^{T_1}$ avec $|q^\tau|_v \leq 1$. Ainsi

$$|F_1^\tau(\boldsymbol{\alpha}^p)|_v \leq p^{-T_1/e_p(\mathbb{L})} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{pL_1}.$$

□

Dans le cas où la ramification est « grande », l'étape d'extrapolation est différente. Nous devons au préalable établir un lemme technique.

Notation. Soit $n \in \mathbb{N}^*$ et f un polynôme. Nous noterons f_n le polynôme dont les coefficients sont obtenus en élevant ceux de f à la puissance n.

Lemme 3.16. — *Soient p un nombre premier, $\mathbb{K}$ un corps de nombres et $\mathcal{O}_\mathbb{K}$ son anneau d'entiers. Soient $f \in \mathcal{O}_\mathbb{K}[\boldsymbol{X}]$ et $\boldsymbol{\zeta} \in \ker[p]$. Alors $\prod_{j=0}^{p-1} f(\boldsymbol{\zeta}^j \boldsymbol{X}) \in \mathcal{O}_\mathbb{K}[\boldsymbol{X}]$ et*

$$\prod_{j=0}^{p-1} f(\boldsymbol{\zeta}^j \boldsymbol{X}) \equiv f_p(\boldsymbol{X}^p) \mod p\mathcal{O}_\mathbb{K}[\boldsymbol{X}].$$

Démonstration. — Soit ζ_p une racine primitive p-ième de l'unité. Il existe $(a_1, \dots, a_n) \in \mathbb{N}^n$ tels que $\boldsymbol{\zeta} = (\zeta_p^{a_1}, \dots, \zeta_p^{a_n})$. On peut alors écrire le produit $\prod_{j=0}^{p-1} f(\boldsymbol{\zeta}^j \boldsymbol{X})$ comme un résultant :

$$\prod_{j=0}^{p-1} f(\boldsymbol{\zeta}^j \boldsymbol{X}) = \mathrm{Res}_Y(f(Y^{a_1}X_1, \dots, Y^{a_n}X_n), Y^p - 1).$$

Ceci implique que ce produit est un polynôme à coefficients dans $\mathcal{O}_\mathbb{K}$. De plus, modulo $p\mathcal{O}_\mathbb{K}[\boldsymbol{X}]$, on a

$$\begin{aligned} \prod_{j=0}^{p-1} f(\boldsymbol{\zeta}^j \boldsymbol{X}) &\equiv \mathrm{Res}_Y(f(Y^{a_1}X_1, \dots, Y^{a_n}X_n), (Y-1)^p) \\ &\equiv f(\boldsymbol{X})^p \\ &\equiv f_p(\boldsymbol{X}^p)\ , \end{aligned}$$

ce qui nous donne la congruence annoncée. □

Lemme 3.17. — *Soient $p \in \mathcal{P}$, v une place de $\mathcal{O}_\mathbb{L}$ au-dessus de p et $\tau \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{|\mathbb{L}} \in H_p$. Il existe alors un polynôme $g \in \mathcal{O}_\mathbb{L}[\boldsymbol{X}]$ tel que*

- *g est une équation réduite de V_p,*
- *$|g^\tau|_v = 1$,*
- *il existe $t \in \mathbb{N}^*$ tel que $g(\boldsymbol{X}^p) \equiv f_{(p^t)}(\boldsymbol{X}^{p^t}) \mod p\mathcal{O}_\mathbb{L}[\boldsymbol{X}]$, où $f \in \mathcal{O}_\mathbb{L}[\boldsymbol{X}]$ est une équation réduite de V_1.*

Démonstration. — Considérons l'ensemble algébrique

$$[p]^{-1}V_p = \bigcup_{\boldsymbol{\zeta} \in \ker[p]} \boldsymbol{\zeta} V_1 = \bigcup_{\boldsymbol{\zeta} \in \mathcal{H}} \boldsymbol{\zeta} V_1\ , \tag{3.15}$$

où $\mathcal{H}$ est le groupe quotient

$$\mathcal{H} = \left({}^{\ker[p]}\!/_{\ker[p]\cap G_{V_1}} \right).$$

(Remarquons que pour $\boldsymbol{\zeta} \in \mathcal{H}$ la variété $\boldsymbol{\zeta} V_1$ est bien définie car celle-ci ne dépend pas, par construction de $\mathcal{H}$, du représentant de $\boldsymbol{\zeta}$ choisi dans $\ker[p]$.) Dans le dernier membre de la suite d'égalités (3.15), la réunion est constituée d'hypersurfaces n'ayant aucune composante irréductible commune. En effet, d'une part la réunion est faite modulo le stabilisateur de V_1, ce qui nous assure que pour deux éléments distincts $\boldsymbol{\zeta}$ et $\tilde{\boldsymbol{\zeta}}$ de $\mathcal{H}$, on a $\boldsymbol{\zeta} V_1 \neq \tilde{\boldsymbol{\zeta}} V_1$; d'autre part, pour tout plongement $\sigma : \mathbb{L}(W) \hookrightarrow \bar{\mathbb{Q}}$ qui fixe $\mathbb{L}$, on a $G_{\sigma(W)} \subseteq G_{V_1}$ donc, de même, $\boldsymbol{\zeta}\sigma(W) \neq \tilde{\boldsymbol{\zeta}}\sigma(W)$. Enfin, si l'on suppose l'existence de σ et $\tilde{\sigma}$ deux plongements distincts de $\mathbb{L}(W)$ dans $\bar{\mathbb{Q}}$ tels que $\sigma_{|\mathbb{L}} = \tilde{\sigma}_{|\mathbb{L}} = \mathrm{Id}$ et pour lesquels on a $\boldsymbol{\zeta}\sigma(W) = \tilde{\boldsymbol{\zeta}}\tilde{\sigma}(W)$ (avec $\boldsymbol{\zeta},\ \tilde{\boldsymbol{\zeta}} \in \ker[p]$), ceci implique, par multiplication par p, que $\sigma([p]W) = \tilde{\sigma}([p]W)$, ce qui est impossible car $\mathbb{L}(W) = \mathbb{L}([p]W)$ (voir lemme 3.9).

Soit $f \in \mathcal{O}_{\mathbb{L}}[\boldsymbol{X}]$ une équation réduite de V_1 telle que $|f^{\tau}|_v = 1$ (voir proposition 3.15) ; on pose

$$h(\boldsymbol{X}) \ = \prod_{\boldsymbol{\zeta}\in\mathcal{H}} f(\boldsymbol{\zeta}\boldsymbol{X}),$$

où l'on choisit pour chaque facteur du produit un représentant de la classe d'équivalence. Alors, d'après ce qui précède, le polynôme h est une équation réduite pour $[p]^{-1}V_p$. En effet, soient s la dimension du stabilisateur de V_1 et $\boldsymbol{\zeta}_1, \cdots, \boldsymbol{\zeta}_{n-s}$ une base d'un supplémentaire de $\ker[p] \cap G_{V_1}$ dans $\ker[p]$. Posons

$$h(\boldsymbol{X}) \ = \prod_{(a_1,\ldots,a_{n-s})\in(\mathbb{Z}/p\mathbb{Z})^{n-s}} f(\boldsymbol{\zeta}_1^{a_1}\cdots\boldsymbol{\zeta}_{n-s}^{a_{n-s}}\boldsymbol{X}).$$

Grâce au lemme 3.16 et par récurrence, on a

$$h \in \mathcal{O}_{\mathbb{L}}[\boldsymbol{X}] \quad \text{et} \quad h(X) \equiv f_{p^{n-s}}(X^{p^{n-s}}) \mod p\mathcal{O}_{\mathbb{L}}[X]. \tag{3.16}$$

Par ailleurs, on a également

$$\prod_{\boldsymbol{\zeta}\in\ker[p]} f(\boldsymbol{\zeta}\boldsymbol{X}) \in \mathcal{O}_{\mathbb{L}}[\boldsymbol{X}^p],$$

et pour tout $\tilde{\boldsymbol{\zeta}} \in \ker[p]$,

$$\prod_{\boldsymbol{\zeta}\in\ker[p]\cap G_{V_1}} f(\tilde{\boldsymbol{\zeta}}\boldsymbol{\zeta}\boldsymbol{X}) = (f(\tilde{\boldsymbol{\zeta}}\boldsymbol{X}))^{p^s}.$$

On en déduit $h(\boldsymbol{X})^{p^s} \in \mathcal{O}_{\mathbb{L}}[\boldsymbol{X}^p]$. Comme h n'est pas un monôme (h définit une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$), on a également $h \in \mathcal{O}_{\mathbb{L}}[\boldsymbol{X}^p]$. On définit alors g par

$$g(\boldsymbol{X}^p) = h(\boldsymbol{X}).$$

Ainsi, g est à coefficients dans $\mathcal{O}_{\mathbb{L}}$ et est une équation réduite de V_p ; par construction, ayant choisi f tel que $|f^\tau|_v = 1$, on a également $|g^\tau|_v = 1$; enfin, comme $s \leq n-2$, la congruence (3.16) nous assure la dernière assertion du lemme. □

Proposition 3.18. — *Soit $p \in \mathcal{P}$ et soient T_2 et L_2 deux entiers naturels non nuls. Supposons qu'il existe un polynôme non nul F_2 à coefficients entiers algébriques, de degré au plus L_2, identiquement nul sur V_p avec multiplicité supérieure ou égale à T_2. Soit v une valuation de $\bar{\mathbb{Q}}$ qui prolonge la valuation p-adique. Alors, pour tout $\boldsymbol{\alpha} \in W$ et pour tout τ qui prolonge un élément H_p, on a*

$$|F_2^\tau(\boldsymbol{\alpha}^p)|_v \leq p^{-T_2} \max\{1, |\alpha_1|_v, \cdots, |\alpha_n|_v\}^{pL_2}.$$

Démonstration. — Soient $\boldsymbol{\alpha} \in W$ et $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{|\mathbb{L}} \in H_p$. On suit alors exactement le même raisonnement que dans la preuve de la proposition 3.15, en substituant le polynôme g construit dans le lemme 3.17 à f, l'idéal (p) à Q, et en remarquant

$$\begin{aligned} g^\tau(\boldsymbol{X}^p) &\equiv \left(f_{p^t}\right)^\tau(\boldsymbol{X}^{p^t}) && \bmod p\mathcal{O}_{\mathbb{L}}[\boldsymbol{X}] \quad \text{(lemme 3.17)} \\ &\equiv f_{p^t}(\boldsymbol{X}^{p^t}) && \bmod p\mathcal{O}_{\mathbb{L}}[\boldsymbol{X}] \quad \text{(lemme 3.11)} \\ &\equiv f(\boldsymbol{X})^{p^t} && \bmod p\mathcal{O}_{\mathbb{L}}[\boldsymbol{X}]. \end{aligned}$$

□

3.7. Démonstration du théorème 3.5

La démonstration suit le schéma classique d'une preuve de transcendance : nous construisons tout d'abord une fonction auxiliaire s'annulant avec forte multiplicité sur une certaine variété (étape d'interpolation) ; puis nous en déduisons l'annulation de cette fonction sur une variété de « grand » degré (étape d'extrapolation) pour aboutir à une contradiction.

Dans toute la suite, nous noterons c_i, $i \in \mathbb{N}$, des nombres réels strictement positifs ne dépendant (éventuellement) que de n. Nous noterons également C un nombre réel strictement positif ne dépendant que de n et suffisamment grand pour que les inégalités ci-dessous soient vraies. Enfin, pour alléger les

notations, on pose

$$\Delta(W) = \frac{\log(2\omega_{\mathbb{L}}(W))}{\log\log(5\omega_{\mathbb{L}}(W))}.$$

Nous fixons maintenant deux paramètres :

$$\begin{aligned} N &= C^9\Delta(W)^5\log(2\omega_{\mathbb{L}}(W)) \\ \text{et} \quad E &= C^3\Delta(W)^2. \end{aligned}$$

Soit Λ l'ensemble de nombres premiers $p \in \mathcal{P}$ tels que $N/2 \leq p \leq N$. Le lemme suivant nous renseigne sur le cardinal de Λ.

Lemme 3.19. — *On a*

$$|\Lambda| \geq c_1 \frac{N}{\log C \cdot \log\log(5\omega_{\mathbb{L}}(W))}.$$

Démonstration. — Par le théorème des nombres premiers, il existe $c_2 > 0$ tel que l'ensemble des nombres premiers compris entre $N/2$ et N soit de cardinal supérieur à

$$c_2\frac{N}{\log N} \geq c_3 \frac{N}{\log C \cdot \log\log(5\omega_{\mathbb{L}}(W))}.$$

Par ailleurs, il y a au plus $\log(|G_{V_1}/G^0_{V_1}|)/\log 2$ premiers qui divisent $|G_{V_1}/G^0_{V_1}|$ et l'on a

$$|G_{V_1}/G^0_{V_1}| \leq \deg(G_{V_1}) \leq \deg(V_1)^n = \omega_{\mathbb{L}}(W)^n.$$

Nous pouvons ainsi majorer le cardinal de $E_{\text{exc}}(V_1)$:

$$|E_{\text{exc}}(V_1)| \leq \frac{n}{\log 2}\log\omega_{\mathbb{L}}(W).$$

Il existe donc un réel c_1 strictement positif tel que le lemme soit vrai. □

Notons maintenant Λ_1 l'ensemble des premiers $p \in \Lambda$ tels que $e_p(\mathbb{L}) \leq E$ et Λ_2 son complémentaire dans Λ. Nous distinguons alors deux cas.

3.7.1. Une majorité de premiers de Λ sont « peu » ramifiés.

Supposons en effet

$$|\Lambda_1| \geq \frac{c_1}{2}\frac{N}{\log C \cdot \log\log(5\omega_{\mathbb{L}}(W))}.$$

Nous introduisons alors les deux nouveaux paramètres suivants :

$$L_1 = \left[C^8\omega_{\mathbb{L}}(W)\Delta(W)^6\right] \quad \text{et} \quad T_1 = \left[C^4\Delta(W)^3\right].$$

L'étape d'interpolation consiste en la construction d'une fonction auxiliaire de petite hauteur s'annulant avec forte multiplicité sur V_1 :

Proposition 3.20. — *Il existe un polynôme non nul F_1 à coefficients entiers algébriques de degré inférieur ou égal à L_1, nul à un ordre supérieur ou égal à T_1 sur V_1 et tel que*

$$h_2(F_1) \leq c_4 \log C \cdot \log(2\omega_{\mathbb{L}}(W)). \tag{3.17}$$

Démonstration. — Remarquons tout d'abord que l'on a

$$\hat{\mu}^{\mathrm{ess}}(V_1) = \hat{\mu}^{\mathrm{ess}}(W) \ \text{ et } \ \deg(V_1) = \omega_{\mathbb{L}}(W).$$

Ainsi $L_1 \geq 2\deg(V_1)T_1$. Le corollaire 3.13 nous indique alors l'existence d'un polynôme non nul F_1 à coefficients entiers algébriques, de degré inférieur ou égal à L_1, s'annulant sur V_1 avec multiplicité supérieure ou égale à T_1, tel que

$$h_2(F_1) \leq \frac{2^{n+1}\omega_{\mathbb{L}}(W)T_1}{L_1}\Big((T_1+n)\log(L_1+1) + 2L_1\hat{\mu}^{\mathrm{ess}}(W)\Big) + \frac{n}{2}\log(L_1+1).$$

Grâce au choix des paramètres et à la majoration (3.2) de $\hat{\mu}^{\mathrm{ess}}(W)$, on a

$$\begin{aligned} h_2(F_1) &\leq c_5 \log C \cdot \log(2\omega_{\mathbb{L}}(W)) + c_6 C^4 \omega_{\mathbb{L}}(W)\Delta(W)^3 \hat{\mu}^{\mathrm{ess}}(W) \\ &\leq c_5 \log C \cdot \log(2\omega_{\mathbb{L}}(W)) + c_6 C^4 c(n)\Delta(W)^{2-6(n+1)}. \end{aligned}$$

Si $c(n) \leq C^{-4}\log C$, on a alors

$$h_2(F_1) \leq c_4 \log C \cdot \log(2\omega_{\mathbb{L}}(W)).$$

□

La fonction auxiliaire ainsi construite s'annule alors sur des conjugués de multiples de W :

Proposition 3.21. — *Avec les notations précédentes, le polynôme F_1 est identiquement nul sur $\tau^{-1}[p]W$ pour tout $p \in \Lambda_1$ et tout $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ qui prolonge Φ_p.*

Démonstration. — Supposons qu'il existe un premier $p \in \Lambda_1$ et un automorphisme $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ qui prolonge Φ_p tel que F_1^τ ne soit pas identiquement nul sur $[p]W$. Alors il existe $\boldsymbol{\alpha} \in W$ de hauteur inférieure à $2\hat{\mu}^{\mathrm{ess}}(W)$ tel que $F_1^\tau(\boldsymbol{\alpha}^p) \neq 0$. Soit $\mathbb{F}$ un corps contenant les coefficients de F_1^τ et $\boldsymbol{\alpha}$. Soit v une place de $\mathbb{F}$. Alors, par la proposition 3.15,

$$\text{si } v \mid p, \quad |F_1^\tau(\boldsymbol{\alpha}^p)|_v \ \leq \ p^{-T_1/e_p(\mathbb{L})} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL_1}.$$

Par ailleurs, on a les majorations usuelles :

$$\begin{aligned} \text{si } v \mid \infty, \quad |F_1^\tau(\boldsymbol{\alpha}^p)|_v &\leq |F_1^\tau|_v (L_1+1)^n \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL_1}, \\ \text{si } v \nmid \infty, \quad |F_1^\tau(\boldsymbol{\alpha}^p)|_v &\leq \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL_1}. \end{aligned}$$

La formule du produit donne alors

$$\begin{aligned} 0 &= \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_{v \in \mathcal{M}_{\mathbb{F}}} [\mathbb{F}_v : \mathbb{Q}_v] \log |F_1^{\tau}(\boldsymbol{\alpha}^p)|_v \\ &\leq -\frac{T_1}{e_p(\mathbb{L})} \log p + pL_1 h(\boldsymbol{\alpha}) + h(F_1) + n \log(L+1). \end{aligned}$$

En utilisant le fait que $e_p(\mathbb{L}) \leq E$ puis les inégalités (3.17) (en remarquant que $h(F_1) \leq h_2(F_1)$) et (3.2), on obtient

$$\begin{aligned} 0 &\leq -\frac{T_1}{E} \log \frac{N}{2} + 2NL_1 \hat{\mu}^{\mathrm{ess}}(W) + h_2(F_1) + n \log(L+1) \\ &\leq -c_7 C \log(2\omega_{\mathbb{L}}(W)) + 2c_8 C^{17} \omega_{\mathbb{L}}(W) \Delta(W)^{11} \log(2\omega_{\mathbb{L}}(W)) \hat{\mu}^{\mathrm{ess}}(W) \\ &\qquad + c_6 \log C \cdot \log(2\omega_{\mathbb{L}}(W)) + c_9 \log C \cdot \log(2\omega_{\mathbb{L}}(W)) \\ &\leq -c_{10} C \log(2\omega_{\mathbb{L}}(W)) + c_8 C^{17} c(n) \Delta(W)^{11-6(n+1)} \log(2\omega_{\mathbb{L}}(W)). \end{aligned}$$

Si $c(n) < c_8^{-1} c_{10} C^{-16}$, on aboutit alors à une contradiction. □

On déduit de cette proposition que F_1 s'annule sur

$$\tilde{V_1} = \bigcup_{p \in \Lambda_1} \bigcup_{\substack{\tau : \mathbb{L}([p]W) \hookrightarrow \bar{\mathbb{Q}} \\ \tau_{|\mathbb{L}} = \Phi_p}} \tau^{-1}[p]W.$$

Par ailleurs, d'après le lemme 3.9, si $p \in \Lambda_1$, on a

$$[\mathbb{L}([p]W) : \mathbb{L}] = [\mathbb{L}(W) : \mathbb{L}] = \delta.$$

Il existe donc exactement δ morphismes distincts $\tau : \mathbb{L}([p]W) \hookrightarrow \bar{\mathbb{Q}}$ qui prolongent Φ_p. De plus, le lemme 2.3 de [**AmDa99**] assure que si $p \neq q$ et si τ_1

et τ_2 sont deux éléments de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, alors $\tau_1([p]W) \neq \tau_2([q]W)$. D'où :

$$\begin{aligned}
\deg \tilde{V}_1 &= \sum_{p\in\Lambda_1} \delta \deg([p]W) \\
&= \sum_{p\in\Lambda_1} p^{n-1-s}\delta \deg W \\
&\geq |\Lambda_1|\omega_{\mathbb{L}}(W)\left(\frac{N}{2}\right)^{n-1-s} \\
&\geq c_{11}\frac{N^{n-s}}{\log C\cdot \log\log(5\omega_{\mathbb{L}}(W))}\omega_{\mathbb{L}}(W) \\
&\geq c_{11}\frac{N}{\log C\cdot \log\log(5\omega_{\mathbb{L}}(W))}\omega_{\mathbb{L}}(W) \\
&\geq c_{11}\frac{C}{\log C}L_1,
\end{aligned}$$

ce qui constitue une contradiction (pour C assez grand) puisque F_1 est nul sur $\tilde{V}_1$ et $\deg F_1 \leq L_1$.

3.7.2. Une majorité de premiers de Λ sont « très » ramifiés.

Supposons maintenant

$$|\Lambda_2| \geq \frac{c_1}{2}\frac{N}{\log C\cdot \log\log(5\omega_{\mathbb{L}}(W))}.$$

Nous introduisons alors les deux nouveaux paramètres

$$L_2 = \left[C^{9(n-s)+2}\omega_{\mathbb{L}}(W)\Delta(W)^{6(n-s)+2}\right] \quad \text{et} \quad T_2 = [C\Delta(W)]$$

et nous considérons l'ensemble algébrique U, réunion d'hypersurfaces :

$$U = \bigcup_{p\in\Lambda_2} V_p\ .$$

Du lemme 3.9, on déduit

$$\deg U \leq |\Lambda_2|N^{n-1-s}\omega_{\mathbb{L}}(W) \leq c_{12}\frac{N^{n-s}}{\log C\cdot \log\log 5\omega_{\mathbb{L}}(W)}\omega_{\mathbb{L}}(W)$$

et

$$\hat{\mu}^{\mathrm{ess}}(U) = \max_{p\in\Lambda_2}\hat{\mu}^{\mathrm{ess}}([p]W_{\mathbb{L}}) \leq N\hat{\mu}^{\mathrm{ess}}(W).$$

Comme dans le cas précédent, nous avons la proposition suivante :

Proposition 3.22. — *Il existe un polynôme non nul F_2 à coefficients entiers algébriques de degré inférieur ou égal à L_2, nul à un ordre supérieur ou égal à T_2 sur U et tel que*

$$h_2(F_2) \leq c_{13} \log C \cdot \log(2\omega_{\mathbb{L}}(W)). \tag{3.18}$$

Démonstration. — On a $L_2 \geq 2T_2 \deg U$. D'après le corollaire 3.13, il existe donc un polynôme non nul F_2 à coefficients entiers algébriques, de degré inférieur ou égal à L_2, s'annulant sur U avec multiplicité supérieure ou égale à T_2, tel que

$$h_2(F_2) \leq \frac{2^{n+1} T_2 \deg U}{L_2} \Big((T_2+n)\log(L_2+1) + 2L_2 N \hat{\mu}^{\mathrm{ess}}(W) \Big) + \frac{n}{2}\log(L_2+1).$$

Grâce aux choix des paramètres et à la majoration (3.2) de $\hat{\mu}^{\mathrm{ess}}(W)$, on a

$$\begin{aligned} h_2(F_2) &\leq c_{14} \log C \cdot \log(2\omega_{\mathbb{L}}(W)) \\ &\qquad + c_{15} C^{1+9(n+1-s)} \omega_{\mathbb{L}}(W) \Delta(W)^{1+6(n-s+1)} \hat{\mu}^{\mathrm{ess}}(W) \\ &\leq c_{14} \log C \cdot \log(2\omega_{\mathbb{L}}(W)) + c_{15} C^{1+9(n+s)} c(n). \end{aligned}$$

Si $c(n) \leq C^{-(1+9(n-s+1))} \log C$, on a alors

$$h_2(F_2) \leq c_{13} \log C \cdot \log(2\omega_{\mathbb{L}}(W)).$$

□

Passons maintenant à l'extrapolation.

Proposition 3.23. — *Avec les notations précédentes, le polynôme F_2 est identiquement nul sur $\tau[p]W$ pour tout $p \in \Lambda_2$ et tout $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{|\mathbb{L}} \in H_p$.*

Démonstration. — Supposons qu'il existe un premier $p \in \Lambda_2$ et un automorphisme $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ qui prolonge un élément de H_p tel que F_2^τ ne soit pas identiquement nul sur $[p]W$. Alors il existe $\boldsymbol{\alpha} \in W$ de hauteur inférieure à $2\hat{\mu}^{\mathrm{ess}}(W)$ tel que $F_2^\tau(\boldsymbol{\alpha}^p) \neq 0$. Soit $\mathbb{F}$ un corps contenant les coefficients de F_2^τ et $\boldsymbol{\alpha}$. Soit v une place de $\mathbb{F}$. Alors, par la proposition 3.18,

$$\text{si } v \mid p, \quad |F_2^\tau(\boldsymbol{\alpha}^p)|_v \;\leq\; p^{-T_2} \max\{1, |\alpha_2|_v, \dots, |\alpha_n|_v\}^{pL_2}.$$

La formule du produit donne alors

$$\begin{aligned} 0 &= \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_{v \in \mathcal{M}_{\mathbb{F}}} [\mathbb{F}_v : \mathbb{Q}_v] \log |F_2^\tau(\boldsymbol{\alpha}^p)|_v \\ &\leq -T_2 \log p + pL_2 h(\boldsymbol{\alpha}) + h(F_2) + n\log(L+1). \end{aligned}$$

En utilisant les inégalités (3.18) et (3.2), on obtient

$$\begin{aligned} 0 &\leq -T_2 \log \frac{N}{2} + 2NL_2\hat{\mu}^{\mathrm{ess}}(W) + h_2(F_2) + n\log(L+1) \\ &\leq -c_{17}C\log(2\omega_{\mathbb{L}}(W)) \\ &\qquad + c_{18}\omega_{\mathbb{L}}(W)C^{2+9(n-s+1)}\Delta(W)^{1+6(n-s+1)}\log\log(5\omega_{\mathbb{L}}(W))\hat{\mu}^{\mathrm{ess}}(W) \\ &\leq -c_{17}C\log(2\omega_{\mathbb{L}}(W)) + c_{18}C^{2+9(n+1)}c(n)\log\log(5\omega_{\mathbb{L}}(W)), \end{aligned}$$

ce qui constitue une contradiction dès que $c(n) < {c_{18}}^{-1}c_{17}C^{-(1+9(n+1))}$. □

On déduit de cette proposition que F_2 s'annule sur $\tilde{U}$, où

$$\tilde{U} = \bigcup_{p\in\Lambda_2} \bigcup_{\substack{\tau:\mathbb{L}([p]W)\hookrightarrow\bar{\mathbb{Q}} \\ \tau_{|\mathbb{L}}\in H_p}} \tau[p]W.$$

Soient $p \in \Lambda_2$ et $\sigma \in H_p$. Comme dans le cas précédent, il existe exactement δ morphismes distincts $\tau : \mathbb{L}([p]W) \hookrightarrow \bar{\mathbb{Q}}$ qui prolongent σ. De plus, la dernière assertion du lemme 3.11 assure que si $\tilde{\sigma} \in H_p\backslash\{\sigma\}$ et si τ et $\tilde{\tau} \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sont tels que $\tau_{|\mathbb{L}} = \sigma$ et $\tilde{\tau}_{|\mathbb{L}} = \tilde{\sigma}$, alors $\tau([p]W) \neq \tilde{\tau}([p]W)$. Associant cela au fait que si $p \neq q$ et si $\tau_1,\ \tau_2 \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, alors $\tau_1([p]W) \neq \tau_2([q]W)$, on obtient

$$\begin{aligned} \deg\tilde{U} &= \sum_{p\in\Lambda_2} \delta|H_p|\deg([p]W) \\ &= \omega_{\mathbb{L}}(W)\sum_{p\in\Lambda_2}|H_p|p^{n-1-s}. \end{aligned}$$

Enfin remarquons que le cardinal de H_p vérifie

$$|H_p| \geq \max(p, e_p(\mathbb{L})) \geq \max(N/2, E) \geq E.$$

On a alors

$$\begin{aligned} \deg\tilde{U} &\geq \omega_{\mathbb{L}}(W)|\Lambda_2|E\left(\frac{N}{2}\right)^{n-1-s} \\ &\geq c_{19}\frac{N^{n-s}}{\log C\cdot\log\log(5\omega_{\mathbb{L}}(W))}E\omega_{\mathbb{L}}(W) \\ &\geq c_{20}\frac{C}{\log C}L_2, \end{aligned}$$

ce qui est de nouveau une contradiction et achève la preuve du théorème.

CHAPITRE 4

CAS DES POINTS

4.1. Introduction

Nous nous proposons dans ce chapitre de poursuivre l'étude du problème de Lehmer dans un tore, amorcée par F. Amoroso et S. David dans [**AmDa99**] et [**AmDa04**]. Soit n un entier naturel non nul. Nous considérons le plongement « naturel » de $\mathbb{G}_{\mathrm{m}}^n$ dans $\mathbb{P}_n$. La hauteur (normalisée) d'un point $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_{\mathrm{m}}^n$ est donc la hauteur de Weil logarithmique et absolue (avec la norme du sup aux places archimédiennes) $h(\boldsymbol{\alpha})$ du point projectif $(1 : \alpha_1 : \ldots : \alpha_n)$. Cette hauteur est nulle si seulement si $\boldsymbol{\alpha}$ est un point de torsion, c'est-à-dire un point dont les coordonnées sont des racines de l'unité. Le *problème de Lehmer* consiste à déterminer la minoration optimale de la hauteur $h(\boldsymbol{\alpha})$ si $\boldsymbol{\alpha}$ n'est pas de torsion.

Dans le cas $n = 1$, le problème de Lehmer « classique » est le suivant :

Conjecture 4.1. — *Il existe un nombre réel c strictement positif tel que pour tout $\alpha \in \mathbb{G}_{\mathrm{m}}(\bar{\mathbb{Q}})$ qui n'est pas une racine de l'unité, on a*

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

Si l'on ne suppose rien de plus sur α, c'est la meilleure minoration possible étant donné que $h(2^{1/d}) = (\log 2)/d$. Dans cette direction, le meilleur résultat à ce jour est la minoration de E. Dobrowolski :

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \left(\frac{\log(3[\mathbb{Q}(\alpha) : \mathbb{Q}])}{\log\log(3[\mathbb{Q}(\alpha) : \mathbb{Q}])} \right)^3,$$

où c est un réel strictement positif. Par la suite F. Amoroso et U. Zannier montrent dans [**AmZa00**] que l'on a le même type de minoration en remplaçant le degré total $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ de α par le degré « non abélien » de α, c'est-à-dire

$[\mathbb{Q}^{ab}(\alpha) : \mathbb{Q}^{ab}]$, où $\mathbb{Q}^{ab}$ désigne l'extension abélienne maximale de $\mathbb{Q}$: c'est le problème de Lehmer « relatif ».

Par ailleurs, dans [**AmDa99**], F. Amoroso et S. David énoncent une conjecture qui est l'analogue en dimension supérieure du problème de Lehmer. L'invariant à considérer en dimension supérieure n'est plus le degré, mais une notion plus géométrique : l'indice d'obstruction.

Définition 4.2. — Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ et K un sous-corps de $\bar{\mathbb{Q}}$. On appelle *indice d'obstruction* de $\boldsymbol{\alpha}$ relativement à K (ou sur K) et on note $\omega_K(\boldsymbol{\alpha})$ le plus petit degré[(1)] d'une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie sur K contenant $\boldsymbol{\alpha}$.

La conjecture peut alors se formuler ainsi :

Conjecture 4.3. — *Soit n un entier naturel non nul. Il existe un nombre réel $c(n)$ tel que pour tout $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

$$h(\boldsymbol{\alpha}) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(\boldsymbol{\alpha})}.$$

La version « relative » de cette conjecture correspond à celle où l'on remplace $\omega_{\mathbb{Q}}(\boldsymbol{\alpha})$ par $\omega_{\mathbb{Q}^{\mathrm{ab}}}(\boldsymbol{\alpha})$. Notons que l'on ne peut, dans cette conjecture, faire l'économie de l'hypothèse d'indépendance multiplicative des coordonnées de $\boldsymbol{\alpha}$: il suffit de considérer le point $\boldsymbol{\alpha}_d = (2^{1/d}, \ldots, 2^{1/d})$, $d \in \mathbb{N}^*$, dont la hauteur peut être arbitrairement petite et qui vérifie $\omega_{\mathbb{Q}}(\boldsymbol{\alpha}_d) = \omega_{\mathbb{Q}^{\mathrm{ab}}}(\boldsymbol{\alpha}_d) = 1$. Rappelons également que faire cette hypothèse équivaut à supposer que $\boldsymbol{\alpha}$ n'appartient à aucune *sous-variété de torsion*, c'est-à-dire une réunion de translatés de sous-tores par des points de torsion. Dans [**AmDa99**], F. Amoroso et S. David montrent l'analogue du résultat de E. Dobrowolski, puis dans [**AmDa04**], une version « semi-relative » :

Théorème 4.4. — *Pour tout entier naturel non nul, il existe des nombres réels strictement positifs $c(n)$, $\kappa(n)$ et $\mu(n)$ ne dépendant que de n et effectivement calculables tels que la propriété suivante soit vraie.*

Soient $\mathbb{L}$ une extension cyclotomique de $\mathbb{Q}$ et $\boldsymbol{\alpha}$ un point de $\mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$. Si

$$h(\boldsymbol{\alpha}) \leq c(n)^{-1}\omega_{\mathbb{L}}(\boldsymbol{\alpha})^{-1}(\log(3[\mathbb{L} : \mathbb{Q}]\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{-\kappa(n)},$$

(1) Le plongement de $\mathbb{G}_{\mathrm{m}}^n$ dans $\mathbb{P}_n$ ayant été fixé, on entend par degré d'une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ le degré de son adhérence de Zariski dans $\mathbb{P}_n$.

alors il existe une sous-variété de torsion B définie sur $\mathbb{L}$ et contenant $\boldsymbol{\alpha}$ telle que

$$(\deg B)^{1/\mathrm{codim}(B)} \leq c(n)\omega_{\mathbb{L}}(\boldsymbol{\alpha})(\log(3[\mathbb{L}:\mathbb{Q}]\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{\mu(n)}.$$

Le but de ce qui suit est d'obtenir une minoration similaire en supprimant la dépendance en le degré $\mathbb{L}$, qui n'est pas satisfaisante si le degré $[\mathbb{L}:\mathbb{Q}]$ est pathologiquement grand par rapport à $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$ (c'est-à-dire si $[\mathbb{L}:\mathbb{Q}]$ n'est pas polynomial en $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$). Pour obtenir un tel théorème, nous sommes contraints de faire une hypothèse technique sur $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et $\mathbb{L}$ extension abélienne de $\mathbb{Q}$, dont voici l'énoncé :

Hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$ **:** *Pour tout sous-tore H de $\mathbb{G}_{\mathrm{m}}^n$, pour tout entier naturel l, pour tout nombre premier p ramifié dans $\mathbb{L}$ et pour tout conjugué*[(2)] $\tilde{\boldsymbol{\alpha}}$ *de $\boldsymbol{\alpha}$, on a*

$$(\tilde{\boldsymbol{\alpha}}\boldsymbol{\alpha}^{-1})^l \notin H \Longrightarrow (\tilde{\boldsymbol{\alpha}}\boldsymbol{\alpha}^{-1})^{lp} \notin H. \tag{4.1}$$

En d'autres termes, cette hypothèse affirme que si $\boldsymbol{\alpha}^l$ et $\tilde{\boldsymbol{\alpha}}^l$ sont indépendants modulo H alors il en va de même pour leurs puissances p-ièmes. En réalité, nous utilisons une version plus faible de cette hypothèse. En particulier, l'assertion (4.1) n'est requise que pour des sous-tores H, des entiers l et des premiers p dont nous contrôlons degrés et valeurs (en fonction de $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$). Nous avons énoncé ici une version plus forte dans un souci de concision et de clarté. La version plus faible que nous utiliserons sera donnée au paragraphe 5. Nous pouvons maintenant énoncer notre résultat :

Théorème 4.5. — *Soit n un entier naturel non nul. Posons*

$$\kappa(n) = \left(2(n+1)^2(n+1)!\right)^n \quad \textit{et} \quad \mu(n) = 2\kappa(n).$$

Il existe un nombre réel strictement positif $c(n)$ ne dépendant que de n et effectivement calculable tel que la propriété suivante soit vraie.

Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Supposons que l'hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$ soit satisfaite. Si

$$h(\boldsymbol{\alpha}) \leq c(n)^{-1}\omega_{\mathbb{L}}(\boldsymbol{\alpha})^{-1}(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{-\kappa(n)},$$

(2) On dit que $\tilde{\boldsymbol{\alpha}} = (\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$ est un conjugué de $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ s'il existe $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que pour tout $i \in [\![1, n]\!]$, on a $\tau\alpha_i = \tilde{\alpha}_i$.

alors il existe une sous-variété de torsion B définie sur $\mathbb{L}$ et contenant $\boldsymbol{\alpha}$ telle que

$$(\deg B)^{1/\mathrm{codim}(B)} \leq c(n)\omega_{\mathbb{L}}(\boldsymbol{\alpha})(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{\mu(n)}.$$

Les constantes $\kappa(n)$ et $\mu(n)$ sont en fait légèrement meilleures mais leur expression a été simplifiée, à nouveau dans un but de clarté.

Le plan de ce chapitre est le suivant. Dans le paragraphe 2, nous précisons tout d'abord les notations que nous utiliserons et montrons quelques lemmes préliminaires. Puis nous passons, dans le paragraphe 3, à la preuve du théorème 4.5, dont le schéma s'inspire naturellement de celle du théorème 4.4 (schéma classique d'une preuve de transcendance), avec cependant des différences notoires. À la différence de [**AmDa04**], nous devons prendre en compte les premiers qui sont ramifiés dans $\mathbb{L}$, ce qui nous oblige à effectuer une dichotomie entre les premiers « peu » et « très » ramifiés, à la manière de [**AmZa00**]. Pour les premiers peu ramifiés, la transcendance est semblable à celle de [**AmDa04**], mis à part le fait que nous devrons utiliser un théorème de Siegel « absolu », afin d'éviter toute dépendance en $\mathbb{L}$. La suite de la transcendance s'en trouve alors modifiée. En ce qui concerne les premiers très ramifiés, nous utiliserons un argument de déterminant, qui s'inspire de [**AmDe07**] et de [**Amo07**] et qui a l'avantage d'éviter l'utilisation d'un lemme de Siegel. Nous combinons alors ces deux résultats pour montrer que si la hauteur de $\boldsymbol{\alpha}$ est petite (en fonction de $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$), il existe soit un multiple $\boldsymbol{\alpha}^l$ de $\boldsymbol{\alpha}$ pour lequel l'indice d'obstruction $\omega_{\mathbb{L}}(\boldsymbol{\alpha}^l)$ sur $\mathbb{L}$ est pathologiquement petit, soit un multiple $\boldsymbol{\alpha}^{l'}$ de $\boldsymbol{\alpha}$ pour lequel l'indice d'obstruction $\omega_{\mathbb{L}_{(l')}}(\boldsymbol{\alpha}^{l'})$ sur un sous-corps strict $\mathbb{L}_{(l')}$ de $\mathbb{L}$ est du même ordre de grandeur que $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$. Comme dans [**AmDa99**] et [**AmDa04**], cette proposition ne suffit pas pour conclure ; il nous faut utiliser un argument de descente, que cette dichotomie rend particulièrement technique (paragraphe 4). Enfin, en supposant l'hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$, nous démontrons le théorème 4.5 dans le paragraphe 5.

4.2. Notations et préliminaires

Nous fixons $\bar{\mathbb{Q}}$, une clôture algébrique de $\mathbb{Q}$, que nous plongeons dans $\mathbb{C}$.

4.2.1. Géométrie

Soit n un entier naturel non nul. Dans toute la suite nous fixons le plongement naturel

$$\begin{array}{rccc} \iota : & \mathbb{G}_{\mathrm{m}}^n & \hookrightarrow & \mathbb{P}_n \\ & \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) & \mapsto & (1 : \alpha_1 : \ldots : \alpha_n). \end{array}$$

Ainsi, les sous-ensembles algébriques de $\mathbb{G}_{\mathrm{m}}^n$ peuvent être vus comme des ensembles algébriques de $\mathbb{P}_n$ en considérant leur adhérence de Zariski dans $\mathbb{P}_n$. Nous dirons qu'un ensemble algébrique (ou fermé de Zariski) est *défini* sur un corps $K \subseteq \bar{\mathbb{Q}}$ s'il est stable sous l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$. En d'autres termes, cela signifie que son idéal de définition peut être engendré par des polynômes à coefficients dans le corps K. Le *corps de définition* d'un ensemble algébrique sera le plus petit sous-corps de $\bar{\mathbb{Q}}$ sur lequel il est défini. Une *variété* désignera un ensemble algébrique irréductible sur son corps de définition. Nous dirons qu'une variété est *géométriquement irréductible* si elle est irréductible sur $\bar{\mathbb{Q}}$. Nous rappelons la définition de l'*indice d'obstruction* d'un ensemble algébrique :

Définition 4.6. — Soient $Z \subset \mathbb{G}_{\mathrm{m}}^n$ un ensemble algébrique et K un sous-corps de $\bar{\mathbb{Q}}$. On appelle *indice d'obstruction* de Z relativement à K (ou sur K) et on note $\omega_K(Z)$ le plus petit degré d'une hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie sur K contenant Z.

Soient K un sous-corps de $\bar{\mathbb{Q}}$ et Z un ensemble algébrique. Nous noterons Z_K l'ensemble algébrique constitué des conjugués de Z au-dessus du corps K :

$$Z_K = \bigcup_{\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)} \sigma Z.$$

Il est clair que $\omega_K(Z) = \omega_K(Z_K)$.

Si Z est un ensemble algébrique de $\mathbb{G}_{\mathrm{m}}^n$ plongé dans $\mathbb{P}_n$ alors $Z \not\subset \{X_0 = 0\}$. Nous travaillerons donc dans la carte affine correspondante pour définir la *multiplicité d'annulation* d'un polynôme sur Z. Pour $\boldsymbol{\lambda} \in \mathbb{N}^n$, nous noterons $\partial_{\boldsymbol{\lambda}}$ l'opérateur différentiel

$$\partial_{\boldsymbol{\lambda}} = \frac{1}{\boldsymbol{\lambda}!} \left(\frac{\partial^{\lambda_1}}{\partial X_1^{\lambda_1}} \right) \circ \cdots \circ \left(\frac{\partial^{\lambda_n}}{\partial X_n^{\lambda_n}} \right),$$

où $\boldsymbol{\lambda}! = \lambda_1! \cdots \lambda_n!$. On dit que $P \in \bar{\mathbb{Q}}[\boldsymbol{X}]$ s'annule avec *multiplicité* T sur Z si $\partial_{\boldsymbol{\lambda}}(P)$ est identiquement nul sur Z pour tout $\boldsymbol{\lambda}$ tel que $|\boldsymbol{\lambda}| \leq T - 1$.

Soient L et T deux entiers naturels non nuls. Nous désignerons par $\mathcal{E}_K(Z,T,L)$ le sous-espace vectoriel de $K[\boldsymbol{X}]$ constitué des polynômes s'annulant sur Z avec multiplicité supérieure ou égale à T et de degré inférieur ou égal à L. Il est clair que $\mathcal{E}_K(Z,T,L) = \mathcal{E}_K(Z_K,T,L)$.

Nous noterons

$$H_K(Z,T,L) = \binom{L+n}{n} - \dim_K\left(\mathcal{E}_K(Z,T,L)\right)$$

la valeur en L de la fonction de Hilbert de Z avec multiplicité T sur K.

Soit V une variété. Nous noterons G_V son *stabilisateur*, c'est-à-dire le sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$ défini par

$$G_V = \{\boldsymbol{x} \in \mathbb{G}_{\mathrm{m}}^n,\ \boldsymbol{x}V = V\} = \bigcap_{\boldsymbol{x}\in V} \boldsymbol{x}^{-1}V$$

et G_V^0 la composante neutre de celui-ci (c'est-à-dire la composante géométriquement irréductible contenant $(1,\dots,1)$). Nous disposons des propriétés suivantes :

- pour toute composante géométriquement irréductible W de V on a
$$G_W^0 = G_V^0 \text{ et } G_W \subseteq G_V\ ;$$
- toutes les composantes géométriquement irréductibles de V ont le même stabilisateur ;
- la dimension du stabilisateur satisfait l'inégalité

$$\dim(G_V) \leq \dim(V)\ ; \tag{4.2}$$

- si V est géométriquement irréductible, alors

$$V \text{ est un translaté de sous-tore } \iff \dim(G_V) = \dim(V). \tag{4.3}$$

Soient V une variété et K son corps de définition. Nous aurons besoin par la suite de travailler avec de « bons » entiers associés à V, c'est-à-dire des entiers l pour lesquels le degré de V a « un bon comportement » lorsqu'on applique à V le morphisme de multiplication par l. Soit W une composante géométriquement irréductible de V. Nous définissons un ensemble d'*entiers exceptionnels* associés à V :

$$\begin{aligned} E_{\mathrm{exc}}(V) \quad &= \quad \{l \in \mathbb{Z},\ \exists \tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/K), W \neq \tau W \text{ et } [l]W = \tau[l]W\} \\ &\quad \cup \{l \in \mathbb{Z},\ l \text{ premier à } |G_W/G_W^0|\}. \end{aligned}$$

Étant donné que le groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ agit transitivement sur l'ensemble des composantes géométriquement irréductibles de V et que toutes ces

composantes ont le même stabilisateur, on vérifie aisément que cette définition ne dépend pas du choix de W ; son intérêt réside dans la proposition suivante :

Proposition 4.7. — *Soient V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ et l, l' deux entiers.*

1. *Si $l \notin E_{\mathrm{exc}}(V)$ alors on a*
$$\deg([l]V) \geq \deg(V).$$
2. *Si $l \notin E_{\mathrm{exc}}(V)$ et V n'est pas une réunion de translatés de sous-tores alors on a*
$$\deg([l]V) \geq l \deg(V).$$
3. *Si $l \notin E_{\mathrm{exc}}(V)$ et $l' \notin E_{\mathrm{exc}}([l]V)$ alors $ll' \notin E_{\mathrm{exc}}(V)$.*
4. *Nous disposons de la majoration*
$$|E_{\mathrm{exc}}(V) \cap \{p \text{ premier}\}| \leq \frac{\dim V + 1}{\log 2} \log \deg(V).$$

Démonstration. — Il est clair que, par la définition de $E_{\mathrm{exc}}(V)$, si $l \notin E_{\mathrm{exc}}(V)$ alors la variété $[l]V$ possède autant de composantes géométriquement irréductibles que V. De plus, pour chacune de ces composantes W, on dispose, grâce au lemme 6 de [**Hin88**], de l'égalité
$$\deg([l]W) = \frac{l^{\dim(W)}}{|\ker[l] \cap G_W|} \deg(W) = \frac{l^{\dim(W)-\dim(G_W)}}{|\ker[l] \cap (G_W/G_W^0)|} \deg(W),$$
où l'on a encore noté $[l]$ le morphisme de multiplication dans le tore quotient $\mathbb{G}_{\mathrm{m}}^n/G_W^0$. Or, si $l \notin E_{\mathrm{exc}}(V)$ alors l est premier à $|(G_W/G_W^0)|$ et $\ker[l] \cap (G_W/G_W^0)$ est trivial. Ainsi, on a
$$\deg([l]W) = l^{\dim(W)-\dim(G_W)} \deg(W).$$
On obtient alors facilement 1 et 2 à l'aide des propriétés (4.2) et (4.3). Pour les points 3 et 4, on procède comme dans la proposition 2.4 de [**AmDa99**] en remplaçant $\mathbb{Q}$ par le corps de définition de la variété V. □

Voici maintenant deux lemmes concernant les indices d'obstruction d'une variété.

Lemme 4.8. — *Soit K un sous-corps de $\bar{\mathbb{Q}}$ et Z un ensemble algébrique. Supposons qu'il existe un polynôme f non nul tel que*
$$f \in \mathcal{E}_{\bar{\mathbb{Q}}}(Z_K, T, L).$$
Alors il existe un polynôme g non nul tel que
$$g \in \mathcal{E}_K(Z_K, T, L).$$

En particulier $\omega_K(Z) = \omega_{\bar{\mathbb{Q}}}(Z_K)$.

Démonstration. — Comme f n'est pas nul, nous pouvons supposer que l'un de ses coefficients est égal à 1. Soit $\mathbb{F}$ une extension galoisienne de $\mathbb{Q}$ contenant K et les coefficients de f. Le polynôme f étant identiquement nul avec multiplicité T sur tous les conjugués de Z au-dessus de K, il en est de même pour les polynômes f^σ, où $\sigma \in \mathrm{Gal}(\mathbb{F}/K)$. Donc le polynôme

$$g = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}/K)} f^\sigma$$

est lui aussi identiquement nul avec multiplicité T sur Z_K. De plus son degré est inférieur ou égal à celui de f et il n'est pas nul car l'un de ses coefficients est égal à $[\mathbb{F} : K]$. Enfin, par construction, il est à coefficients dans K, d'où

$$g \in \mathcal{E}_K(Z_K, T, L).$$

Remarquons que l'on a

$$\omega_K(Z) = \omega_K(Z_K) \geq \omega_{\bar{\mathbb{Q}}}(Z_K).$$

Soit $f \in \bar{\mathbb{Q}}[X]$ un polynôme identiquement nul sur Z_K de degré $\omega_{\bar{\mathbb{Q}}}(Z_K)$. Par ce qui précède, il existe un polynôme non nul $g \in \mathcal{E}_K(Z_K, 1, \omega_{\bar{\mathbb{Q}}}(Z_K))$, donc $\omega_K(Z_K) \leq \omega_{\bar{\mathbb{Q}}}(Z_K)$ et finalement

$$\omega_K(Z) = \omega_{\bar{\mathbb{Q}}}(Z_K).$$

□

Lemme 4.9. — *Soient K un sous-corps de $\bar{\mathbb{Q}}$, W un ensemble algébrique et Z une variété de $\mathbb{G}_{\mathrm{m}}^n$. On suppose que Z contient tous les conjugués de W au-dessus de K. Alors*

$$\omega_K(W) \leq n(\deg Z)^{1/\mathrm{codim} Z}.$$

Démonstration. — Par hypothèse Z contient W_K donc $\omega_{\bar{\mathbb{Q}}}(W_K) \leq \omega_{\bar{\mathbb{Q}}}(Z)$ et par le lemme 4.8 on a $\omega_K(W) = \omega_{\bar{\mathbb{Q}}}(W_K)$. Or par un résultat de M. Chardin (voir le corollaire 2 du chapitre 1 et l'exemple 1 de [**Cha88**]), on a $\omega_{\bar{\mathbb{Q}}}(Z) \leq n(\deg Z)^{1/\mathrm{codim} Z}$. □

Enfin, nous noterons $\ker[p]$ l'ensemble des points de p-torsion, c'est-à-dire l'ensemble des points dont les coordonnées sont des racines p-ièmes de l'unité, ce qui correspond au noyau du morphisme d'élévation à la puissance p dans $\mathbb{G}_{\mathrm{m}}^n$. Si V est une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$, nous noterons

$$\ker[p] \cdot V = \bigcup_{\zeta \in \ker[p]} \zeta V.$$

4.2.2. Arithmétique

Soit $\mathbb{F}$ un corps de nombres ; nous noterons $\mathcal{O}_{\mathbb{F}}$ (resp. $\mathcal{M}_{\mathbb{F}}$) son anneau d'entiers (resp. l'ensemble de ses places).

Soient p un nombre premier et A un anneau ; nous désignerons par $\sqrt[p]{pA}$ l'idéal de A constitué des éléments dont la puissance p-ième appartient à l'idéal engendré par p :

$$\sqrt[p]{pA} = \{\gamma \in A \mid \gamma^p \in pA\}.$$

Soient $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et p un nombre premier. Nous noterons $e_p(\mathbb{L})$ l'indice de ramification de p dans $\mathbb{L}$ et $\phi_p \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ le morphisme de Frobenius défini dans le lemme suivant :

Lemme 4.10. — *Soit $(\pi_1 \cdots \pi_r)^{e_p(\mathbb{L})}$ la décomposition de p dans $\mathcal{O}_{\mathbb{L}}$. Alors il existe un élément ϕ_p du groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ tel que pour tout entier algébrique $\gamma \in \mathbb{L}$, on a*

$$\phi_p \gamma \equiv \gamma^p \mod \pi_1 \cdots \pi_r. \tag{4.4}$$

Démonstration. — Voir le lemme 3.1 de [**AmZa00**]. □

Par abus de notation, nous poserons $\phi_1 = \mathrm{Id}$ et $e_1(\mathbb{L}) = 1$.

Supposons maintenant que le premier p est ramifié dans $\mathbb{L}$. Par le théorème de Kronecker-Weber, le corps $\mathbb{L}$ est inclus dans une extension cyclotomique ; soit $m \in \mathbb{N}^*$ minimal tel que $\mathbb{L} \subset \mathbb{Q}(\zeta_m)$, où ζ_m désigne une racine primitive m-ième de l'unité. Alors p est ramifié dans $\mathbb{Q}(\zeta_m)$ donc p divise m. Nous posons

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

Si p^2 divise m, alors $[\mathbb{L} : \mathbb{L}_{(p)}] = p$ par minimalité de m. Sinon $[\mathbb{L} : \mathbb{L}_{(p)}] \geq e_p(\mathbb{L})$ car p n'est pas ramifié dans $\mathbb{L}_{(p)}$. Nous avons ainsi

$$[\mathbb{L} : \mathbb{L}_{(p)}] \geq \min\left(p, e_p(\mathbb{L})\right). \tag{4.5}$$

Par ailleurs nous avons la congruence suivante :

Lemme 4.11. — *Soient $\mathbb{L}$ une extension abélienne et p un nombre premier ramifié dans $\mathbb{L}$. Alors pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{L}_{(p)})$ et tout $\gamma \in \mathcal{O}_{\mathbb{L}}$ on a*

$$\sigma\gamma \equiv \gamma \mod \sqrt[p]{p\mathcal{O}_{\mathbb{L}}}. \tag{4.6}$$

Démonstration. — Soit m le plus petit entier tel que $\mathbb{L} \subset \mathbb{Q}(\zeta_m)$, où ζ_m est une racine primitive m-ième de l'unité. Alors $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ et pour tout $\gamma \in \mathcal{O}_{\mathbb{L}}$, il existe $P \in \mathbb{Z}[X]$ tel que $\gamma = P(\zeta_m)$. Par définition, $\mathbb{L}_{(p)} =$

$\mathbb{Q}(\zeta_{m/p}) \cap \mathbb{L}$, donc tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{L}_{(p)})$ est la restriction à $\mathbb{L}$ d'un élément $\tilde{\sigma}$ de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p}))$. Ainsi, par le petit théorème de Fermat,

$$\sigma\gamma^p = \tilde{\sigma}\gamma^p = \tilde{\sigma}(P(\zeta_m))^p \equiv P(\tilde{\sigma}\zeta_m^p) = P(\zeta_m^p) \equiv (P(\zeta_m))^p = \gamma^p \mod p\mathbb{Z}[\zeta_m].$$

et finalement

$$\sigma\gamma \equiv \gamma \mod \sqrt[p]{p\mathcal{O}_{\mathbb{L}}}.$$

□

Nous utiliserons à plusieurs reprises le lemme d'approximation suivant :

Lemme 4.12. — *Soient K un corps de nombres, v_0 une place ultramétrique de K et $\gamma_1, \ldots, \gamma_n$ des éléments de K. Alors il existe un élément $\beta \in \mathcal{O}_K$ tel que $\beta\gamma_1, \ldots, \beta\gamma_n \in \mathcal{O}_K$ et $|\beta|_{v_0} = \max\{1, |\gamma_1|_{v_0}, \ldots, |\gamma_n|_{v_0}\}^{-1}$.*

Démonstration. — Fixons une place archimédienne quelconque $\tilde{v}$ et notons Σ l'ensemble fini :

$$\Sigma = \{v \in \mathcal{M}_k \mid v \nmid \infty \text{ et } \max\{1, |\gamma_1|_v, \ldots, |\gamma_n|_v\} > 1\} \cup \{v_0\}.$$

Pour toute place $v \in \Sigma$, notons θ_v^{-1} celui des éléments de $\gamma_1, \ldots, \gamma_n$ de valeur absolue maximale en v (si $v = v_0$ et si $\max\{|\gamma_1|_{v_0}, \ldots, |\gamma_n|_{v_0}\} < 1$, on pose $\theta_{v_0} = 1$). D'après le théorème de [**CF67**, chap II, 15, p. 67] il existe un élément $\beta \in K$ tel que

$$\begin{cases} |\beta - \theta_v|_v < \max\{1, |\gamma_1|_v, \ldots, |\gamma_n|_v\}^{-1} & \text{pour tout } v \in \Sigma, \\ |\beta|_v \leq 1 & \text{si } v \notin \Sigma \cup \{\tilde{v}\}. \end{cases}$$

En utilisant l'inégalité ultramétrique, on en déduit

$$\begin{cases} |\beta|_v = \max\{1, |\gamma_1|_v, \ldots, |\gamma_n|_v\}^{-1} & \text{pour tout } v \in \Sigma, \\ |\beta|_v \leq 1 & \text{si } v \notin \Sigma \cup \{\tilde{v}\}. \end{cases}$$

En particulier, pour toute place finie v de K on a $|\beta|_v \leq 1$ (donc $\beta \in \mathcal{O}_K$) et pour tout $i \in [\![1, n]\!]$, $|\beta\gamma_i|_v \leq 1$ (donc $\beta\gamma_i \in \mathcal{O}_K$). Enfin, on a bien $|\beta|_{v_0} = \max\{1, |\gamma_1|_{v_0}, \ldots, |\gamma_n|_{v_0}\}^{-1}$ car $v_0 \in \Sigma$. Le lemme est donc établi. □

4.2.3. Hauteur

La hauteur considérée est la hauteur de Weil logarithmique et absolue, dont nous rappelons rapidement la définition. Soient $\boldsymbol{x} \in \mathbb{P}^n$, $(x_0 : x_1 : \cdots : x_n)$ un choix de coordonnées homogènes pour $\boldsymbol{x}$, $\mathbb{F}$ un corps de nombres contenant

$x_0, x_1, \ldots, x_n$ et v une place de $\mathbb{F}$ normalisée de façon usuelle (à savoir : si $v|p$ alors $|p|_v = p^{-1}$ et $|2|_v = 2$ si $v|\infty$). On pose

$$\|\boldsymbol{x}\|_v = \max\{|x_0|_v, \ldots, |x_n|_v\}.$$

Alors la hauteur de $\boldsymbol{x}$ est le réel positif défini par

$$h(\boldsymbol{x}) = \sum_{v \in \mathcal{M}_{\mathbb{F}}} \frac{[\mathbb{F}_v : \mathbb{Q}_v]}{[\mathbb{F} : \mathbb{Q}]} \log \|\boldsymbol{x}\|_v.$$

La hauteur d'un point $\boldsymbol{\alpha}$ de $\mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$ est alors la hauteur du point projectif correspondant :

$$h(\boldsymbol{\alpha}) = h(\iota(\boldsymbol{\alpha})).$$

Enfin, si F est un polynôme, on note $h(F)$ (resp. $\|F\|_v$) la hauteur (resp. la norme v) de la famille ses coefficients.

4.3. Transcendance

Afin d'obtenir une minoration indépendante du degré de l'extension abélienne $\mathbb{L}$ sur $\mathbb{Q}$, nous devons considérer pour la transcendance tous les premiers de $\mathbb{L}$, ramifiés ou non, à la différence de [**AmDa04**]. Nous allons donc effectuer une dichotomie, selon qu'un premier sera « peu » ou « très » ramifié dans $\mathbb{L}$ (cela sera clairement quantifié par des paramètres dans la suite). La transcendance est alors très distincte dans les deux cas. Nous traitons d'abord le cas de grande ramification, puis celui de petite ramification et énonçons dans un troisième temps un théorème qui synthétise les deux cas et permet d'aborder la descente au paragraphe suivant.

4.3.1. Transcendance dans le cas de grande ramification

Nous allons montrer que si la hauteur de $\boldsymbol{\alpha}$ est suffisamment petite et s'il existe un premier p ramifié dans une extension abélienne $\mathbb{L}$ alors l'indice d'obstruction $\omega_{\mathbb{L}_{(p)}}(\boldsymbol{\alpha}^p)$ de $\boldsymbol{\alpha}^p$ sur le sous-corps $\mathbb{L}_{(p)}$ de $\mathbb{L}$ est du même ordre que celui de $\boldsymbol{\alpha}$ sur $\mathbb{L}$. Pour cela, nous utiliserons la congruence donnée dans le lemme 4.11 et le fait que si $\boldsymbol{\zeta}$ est un point de p-torsion alors $\boldsymbol{\zeta\alpha}$ et $\boldsymbol{\alpha}$ sont proches v-adiquement pour toute valuation v divisant p. Puis nous exploiterons ces propriétés métriques dans un déterminant bien choisi afin de minorer la hauteur de $\boldsymbol{\alpha}$ en fonction de certaines valeurs de fonctions de Hilbert. Enfin, en supposant que la hauteur de $\boldsymbol{\alpha}$ est petite, nous en déduirons la non-nullité

des espaces vectoriels correspondants, ce qui nous permettra de construire une variété dont le degré réalise $\omega_{\mathbb{L}_{(p)}}(\boldsymbol{\alpha}^p)$.

Nous utilisons tout d'abord la congruence établie dans le lemme 4.11 pour établir le lemme suivant, qui va permettre d'extrapoler par la suite.

Lemme 4.13. — *Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$, $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et p un premier ramifié dans $\mathbb{L}$. Soient $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$ et v une place de $\bar{\mathbb{Q}}$ divisant p. Alors pour tout conjugué $\tilde{\boldsymbol{\alpha}}$ de $\boldsymbol{\alpha}$ au-dessus de $\mathbb{L}$, pour tout $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$ et pour tout $\boldsymbol{\zeta} \in \ker[p]$ on a*

$$|F^\tau(\boldsymbol{\zeta}\tilde{\boldsymbol{\alpha}})|_v \leq p^{-T/p}\|F^\tau\|_v \|\iota(\tilde{\boldsymbol{\alpha}})\|_v^L.$$

La démonstration de ce lemme s'inspire de la preuve alternative de U. Zannier ([**Zan01**]) pour généraliser le lemme clé de E. Dobrowolski en dimension supérieure (théorème 3.1 de [**AmDa99**]), et contourner le fait que dans ce cas les anneaux de polynômes ne sont plus principaux.

Démonstration. — Remarquons tout d'abord que, grâce au lemme 4.12, quitte à diviser le polynôme F par $\|F^\tau\|_v$ puis à le multiplier par un entier algébrique, on peut supposer que F est à coefficients entiers algébriques et $\|F^\tau\|_v = 1$. Par symétrie, il suffit d'effectuer la démonstration pour $\tilde{\boldsymbol{\alpha}} = \boldsymbol{\alpha}$. Nous supposerons de plus, dans un premier temps, que $\boldsymbol{\alpha}$ est à coordonnées entières.

Soit $\mathbb{F}$ une extension galoisienne de $\mathbb{Q}$ contenant le corps $\mathbb{L}$, les coefficients de F, les coordonnées de $\boldsymbol{\alpha}$ et les racines p-ièmes de l'unité. Soit $\mathcal{O}_{\mathbb{F}_v}$ (resp. $\mathcal{O}_{\mathbb{L}_v}$) l'anneau des entiers du complété de $\mathbb{F}$ (resp. $\mathbb{L}$) par rapport à v. D'après [**Ser68**, Prop. 12, p. 66], $\mathcal{O}_{\mathbb{F}_v}$ est monogène sur $\mathcal{O}_{\mathbb{L}_v}$: il existe $\delta \in \mathcal{O}_{\mathbb{F}_v}$ tel que $\mathcal{O}_{\mathbb{F}_v} = \mathcal{O}_{\mathbb{L}_v}[\delta]$. En particulier, pour tout $i \in [\![1, n]\!]$, il existe $a_i \in \mathcal{O}_{\mathbb{L}_v}[X]$ tel que

$$\alpha_i = a_i(\delta).$$

Considérons maintenant $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$; il induit un élément de $\mathrm{Gal}(\mathbb{F}_v/\mathbb{L}_{(p)_v})$ que nous noterons encore τ. La congruence (4.6) se prolonge à $\mathcal{O}_{\mathbb{L}_v}$:

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}_v}, \quad \tau\gamma \equiv \gamma \mod \sqrt[p]{p\mathcal{O}_{\mathbb{L}_v}}. \tag{4.7}$$

Pour tout $i \in [\![1, n]\!]$, posons

$$\beta_i = a_i^\tau(\delta)$$

de sorte que

$$\beta_i \equiv \alpha_i \mod \sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}. \tag{4.8}$$

Remarquons que $\partial_{\boldsymbol{\lambda}}(F) \in \mathcal{O}_{\mathbb{F}}[\boldsymbol{X}]$. Nous allons montrer que pour tout polynôme $H \in \mathcal{O}_{\mathbb{F}}[\boldsymbol{X}]$ nul en $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ avec multiplicité au moins t, on a

$$H^{\tau}(\boldsymbol{\beta}) \equiv 0 \mod \left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^t. \tag{4.9}$$

Soit $\Delta \in \mathcal{O}_{\mathbb{L}_v}[X]$ le polynôme minimal de δ sur $\mathbb{L}_v$ et soit s la plus grande puissance de Δ divisant $G = H(a_1, \ldots, a_n)$; montrons que $s \geq t$. La dérivée $G^{(s)}$ n'est pas divisible par Δ. Or le polynôme $G^{(s)}$ appartient à l'idéal engendré par

$$\left\{\partial_{\boldsymbol{\lambda}}(H)(a_1, \ldots, a_n)\ ,\ |\boldsymbol{\lambda}| \leq s\right\}$$

donc il existe un n-uplet $\boldsymbol{\lambda} \in \mathbb{N}^n$ avec $|\boldsymbol{\lambda}| \leq s$ tel que $\partial_{\boldsymbol{\lambda}}(H)(a_1, \ldots, a_n)$ ne soit pas divisible par Δ. Cela signifie qu'il existe $\sigma \in \mathrm{Gal}(\mathbb{F}_v/\mathbb{L}_v)$ tel que

$$\partial_{\boldsymbol{\lambda}}(H)(\alpha_1^{\sigma}, \ldots, \alpha_n^{\sigma}) = \partial_{\boldsymbol{\lambda}}(H)(a_1(\delta^{\sigma}), \ldots, a_n(\delta^{\sigma})) \neq 0.$$

Puisque H est nul en $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ avec multiplicité au moins t, on en déduit $|\boldsymbol{\lambda}| \geq t$ donc $s \geq t$. Ainsi, on vient de montrer que Δ^t divise $H(a_1, \ldots, a_n)$ dans $\mathbb{F}_v[X]$ donc dans $\mathcal{O}_{\mathbb{F}_v}[X]$. On peut alors écrire

$$H^{\tau}(a_1^{\tau}(X), \ldots, a_n^{\tau}(X)) = R^{\tau}(X)(\Delta^{\tau}(X))^t, \quad R \in \mathcal{O}_{\mathbb{F}_v}[X].$$

En évaluant en δ dans cette équation et en tenant compte du fait que, par (4.7),

$$\Delta^{\tau}(\delta) \equiv \Delta(\delta) \equiv 0 \mod \sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}},$$

on obtient (4.9).

Si l'on applique (4.9) à $H = \partial_{\boldsymbol{\lambda}}(F)$ et $t = T - |\boldsymbol{\lambda}|$, pour un n-uplet quelconque $\boldsymbol{\lambda}$ vérifiant $|\boldsymbol{\lambda}| \leq T$, on obtient

$$\partial_{\boldsymbol{\lambda}}(F)^{\tau}(\boldsymbol{\beta}) \equiv 0 \mod \left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^{T-|\boldsymbol{\lambda}|}. \tag{4.10}$$

Enfin, par la formule de Taylor, on a

$$F^{\tau}(\boldsymbol{\zeta\alpha}) = \sum_{|\boldsymbol{\lambda}| \geq 0} (\boldsymbol{\zeta\alpha} - \boldsymbol{\beta})^{\boldsymbol{\lambda}} \partial_{\boldsymbol{\lambda}}(F)^{\tau}(\boldsymbol{\beta}),$$

où $(\boldsymbol{\zeta\alpha} - \boldsymbol{\beta})^{\boldsymbol{\lambda}} = \prod_{i=1}^{n} (\zeta_i \alpha_i - \beta_i)^{\lambda_i}$. Or, pour tout ξ racine p-ième de l'unité, on a $\xi \equiv 1 \mod \sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}$. D'où, avec (4.8), $(\boldsymbol{\zeta\alpha} - \boldsymbol{\beta})^{\boldsymbol{\lambda}} \equiv 0 \mod \left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^{|\boldsymbol{\lambda}|}$. On en déduit avec (4.10)

$$F^{\tau}(\boldsymbol{\zeta\alpha}) \equiv 0 \mod \left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^{T}$$

et le lemme est ainsi démontré sous l'hypothèse que $\alpha_1, \ldots, \alpha_n$ soient des entiers algébriques.

Dans le cas géneral, on se ramène, comme dans [**AmDa99**] et [**AmDa04**] au cas précédent en utilisant le lemme 4.12. Ce dernier affirme qu'il existe $\theta \in \mathcal{O}_{\mathbb{F}}$ tel que

$$\begin{cases} \theta\alpha_1, \dots, \theta\alpha_n \in \mathcal{O}_{\mathbb{F}} \\ \text{et} \\ |\theta|_v = \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{-1}. \end{cases}$$

Le polynôme

$$\tilde{F}(X_0, \dots, X_n) = X_0^L F\Big(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\Big) \in \mathcal{O}_{\mathbb{F}}[\boldsymbol{X}]$$

est nul à un ordre supérieur ou égal à T en $(\theta, \theta\alpha_1, \dots, \theta\alpha_n) \in \mathcal{O}_{\mathbb{F}}^{n+1}$ et ses conjugués au-dessus de $\mathbb{L}$. On en déduit

$$|\tilde{F}^\tau(\theta, \zeta_1\theta\alpha_1, \dots, \zeta_n\theta\alpha_n)|_v \leq p^{-T/p},$$

par la première partie de la preuve. De plus, on a

$$\begin{aligned} |\tilde{F}^\tau(\theta, \zeta_1\theta\alpha_1, \dots, \zeta_n\theta\alpha_n)|_v &= |\theta|_v^L |F^\tau(\boldsymbol{\zeta\alpha})|_v \\ &= |F^\tau(\boldsymbol{\zeta\alpha})|_v \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{-L}. \end{aligned}$$

Le lemme est ainsi complètement démontré. □

Nous pouvons maintenant minorer la hauteur de $\boldsymbol{\alpha}$.

Proposition 4.14. — *Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Soient L, T deux entiers naturels non nuls et p un premier ramifié dans $\mathbb{L}$. Alors*

$$h(\boldsymbol{\alpha}) \geq \left(1 - \frac{H_{\bar{\mathbb{Q}}}\left(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L\right)}{H_{\bar{\mathbb{Q}}}\left(\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}, 1, L\right)}\right) \frac{T \log p}{pL} - \frac{n}{2L} \log(L+1).$$

Démonstration. — Considérons la matrice de terme général $\boldsymbol{\beta}_k^{\boldsymbol{\lambda}_l}$ où $\boldsymbol{\beta}_k$ parcourt l'ensemble des points de $\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}$ et $\boldsymbol{\lambda}_l$ l'ensemble des multi-indices de longueur inférieure ou égale à L. Le rang de cette matrice est $r = H_{\bar{\mathbb{Q}}}\left(\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}, 1, L\right)$. Nous pouvons donc en extraire une matrice de taille $r \times r$ inversible : choisissons $\boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_r$ et $\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_r$ tels que

$$M = (\boldsymbol{\beta}_i^{\boldsymbol{\lambda}_j})_{1 \leq i,j \leq r}$$

soit de déterminant non nul. Alors l'espace vectoriel

$$\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L) \cap \mathrm{Vect}\left\{\boldsymbol{X}^{\boldsymbol{\lambda}_1}, \cdots, \boldsymbol{X}^{\boldsymbol{\lambda}_r}\right\}$$

est de dimension supérieure ou égale à $r_0 = r - H_{\bar{\mathbb{Q}}}\left(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L\right)$. Si $r_0 \leq 0$, alors la proposition est triviale, par positivité de la hauteur. Sinon, il existe

r_0 polynômes linéairement indépendants $G_k = \sum_{j=1}^{r} g_{k,j} \boldsymbol{X}^{\boldsymbol{\lambda}_j}$ $(1 \leq k \leq r_0)$ s'annulant sur $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ avec multiplicité supérieure ou égale à T. Soit v une place de $\bar{\mathbb{Q}}$ divisant p. Alors, quitte à faire des combinaisons linéaires et à réordonner $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_r$, on peut supposer de plus (grâce au lemme 4.12) que, pour $k = 1, \ldots, r_0$, les polynômes

$$G_k = \sum_{j=k}^{r} g_{k,j} \boldsymbol{X}^{\boldsymbol{\lambda}_j}$$

sont à coefficients entiers algébriques et

$$|g_{k,j}|_v \begin{cases} = 1 & \text{si } j = k; \\ \leq 1 & \text{si } j \in [\![k+1, r]\!]. \end{cases} \tag{4.11}$$

Par des opérations élémentaires sur les colonnes de M, on peut se ramener à une matrice $\tilde{M}$ dont les r_0 premières colonnes sont de la forme $(G_k(\boldsymbol{\beta}_1), \ldots, G_k(\boldsymbol{\beta}_r))^t$, $k \in [\![1, r_0]\!]$. Par la condition (4.11), on a $|\det(M)|_v = |\det(\tilde{M})|_v$. Comme $G_k \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$, le lemme 4.13 implique

$$|G_k^{\tau}(\boldsymbol{\zeta}\boldsymbol{\alpha})|_{v'} \leq p^{-T/p} \max\{1, |\alpha_1|_{v'}, \ldots, |\alpha_n|_{v'}\}^L$$

pour tout $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$, tout $\boldsymbol{\zeta} \in \ker[p]$ et toute place v' divisant p. Pour tout $i \in [\![1, r]\!]$ nous fixons $\tau_i \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$ et $\boldsymbol{\zeta}_i \in \ker[p]$ tel que $\boldsymbol{\beta}_i = \tau_i(\boldsymbol{\zeta}_i \boldsymbol{\alpha})$. Alors

$$\begin{aligned} |G_k(\boldsymbol{\beta}_i)|_v &= |G_k(\tau_i(\boldsymbol{\zeta}_i\boldsymbol{\alpha}))|_v \\ &= |G_k^{\tau_i^{-1}}(\boldsymbol{\zeta}\boldsymbol{\alpha})|_{\tau_i^{-1}v} \\ &\leq p^{-T/p} \max\{1, |\alpha_1|_{\tau_i^{-1}v}, \ldots, |\alpha_n|_{\tau_i^{-1}v}\}^L \\ &\leq p^{-T/p} \max\{1, |\beta_{i,1}|_v, \ldots, |\beta_{i,n}|_v\}^L. \end{aligned}$$

En développant $\det(\tilde{M})$ suivant les r_0 premières colonnes, on a finalement

$$|\det(M)|_v = |\det(\tilde{M})|_v \leq p^{-r_0 T/p} \prod_{i=1}^{r} \max\{1, |\beta_{i,1}|_v \ldots, |\beta_{i,n}|_v\}^L.$$

La formule précédente est valable pour toute place v divisant p. Si v est une autre place finie, l'inégalité ultramétrique donne

$$|\det(M)|_v \leq \prod_{i=1}^{r} \max\{1, |\beta_{i,1}|_v, \ldots, |\beta_{i,n}|_v\}^L.$$

Enfin, si v est une place archimédienne, l'inégalité de Hadamard fournit la majoration

$$\begin{aligned} |\det(M)|_v &\leq \prod_{i=1}^{r}\left(\sum_{j=1}^{r}|\boldsymbol{\beta}_i^{\boldsymbol{\lambda}_j}|_v^2\right)^{1/2} \\ &\leq \prod_{i=1}^{r}\left(r\max\{1,|\beta_{i,1}|_v\ldots,|\beta_{i,n}|_v\}^{2L}\right)^{1/2} \\ &\leq r^{r/2}\prod_{i=1}^{r}\max\{1,|\beta_{i,1}|_v\ldots,|\beta_{i,n}|_v\}^{L}. \end{aligned}$$

En appliquant la formule du produit à $\det(M)$ (qui n'est pas nul), on obtient

$$\begin{aligned} 1 &\leq p^{-r_0T/p}r^{r/2}\prod_{i=1}^{r}\exp(Lh(\boldsymbol{\beta}_i)) \\ &\leq p^{-r_0T/p}r^{r/2}\exp(Lrh(\boldsymbol{\alpha})) \end{aligned}$$

et finalement, en utilisant l'inégalité $r \leq \binom{L+n}{n} \leq (L+1)^n$,

$$h(\boldsymbol{\alpha}) \geq \frac{r_0}{r}\frac{T\log p}{pL} - \frac{n}{2L}\log(L+1),$$

ce qui achève la preuve de la proposition. □

Proposition 4.15. — *Il existe un nombre réel strictement positif c_0 ne dépendant que de n tel que la propriété suivante soit vraie. Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$, $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et p un premier ramifié dans $\mathbb{L}$. Si*

$$h(\boldsymbol{\alpha}) \leq {c_0}^{-1}\frac{\log p}{p\omega_{\mathbb{L}}(\boldsymbol{\alpha})},$$

alors

$$\omega_{\mathbb{L}_{(p)}}(\boldsymbol{\alpha}^p) \leq c_0\omega_{\mathbb{L}}(\boldsymbol{\alpha})\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})).$$

Démonstration. — Afin d'alléger les notations, nous posons $\omega = \omega_{\mathbb{L}}(\boldsymbol{\alpha})$. Nous noterons C un réel strictement positif ne dépendant que de n que nous supposerons suffisamment grand pour que les inégalités suivantes soient vérifiées. Nous noterons également c_1', c_2' et c_3' des réels strictement positifs ne dépendant que de n.

Nous fixons deux paramètres :

$$T = [Cp\log(3\omega)] \quad \text{et} \quad L = (2n+1)\omega T.$$

On a alors

$$\log(L+1) \leq c_1'(\log C)(\log p)(\log(3\omega))$$

et

$$\frac{\log(L+1)}{L} \leq c_2' \frac{\log C}{C} \frac{\log p}{p\omega}.$$

Supposons

$$h(\boldsymbol{\alpha}) \leq \frac{1}{C} \frac{\log p}{p\omega}.$$

Alors la proposition 4.14 implique

$$\begin{aligned} 1 - \frac{H_{\bar{\mathbb{Q}}}\left(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L\right)}{H_{\bar{\mathbb{Q}}}\left(\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}, 1, L\right)} &\leq \left(h(\boldsymbol{\alpha}) + \frac{n}{2L}\log(L+1)\right) \frac{pL}{T \log p} \\ &\leq c_3' \frac{\log C}{C} \\ &< \frac{1}{2}. \end{aligned}$$

Ainsi,

$$H_{\bar{\mathbb{Q}}}\left(\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}, 1, L\right) < 2 H_{\bar{\mathbb{Q}}}\left(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L\right).$$

Or, si P_0 est un polynôme non nul s'annulant sur $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ de degré minimal ω, alors $P \cdot P_0^T$ appartient à $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$ pour tout $P \in \bar{\mathbb{Q}}[\boldsymbol{X}]$ de degré inférieur ou égal à $L - \omega T$; donc

$$H_{\bar{\mathbb{Q}}}\left(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L\right) \leq \binom{L+n}{n} - \binom{L-\omega T+n}{n}.$$

En remarquant

$$\begin{aligned} \binom{L+n}{n}\binom{L-\omega T+n}{n}^{-1} &= \prod_{j=1}^{n} \frac{L+j}{L-\omega T+j} \\ &\leq \left(1 + \frac{\omega T}{L-\omega T}\right)^n \\ &\leq \left(1 + \frac{1}{2n}\right)^n \leq \sqrt{e} < 2, \end{aligned}$$

on a ainsi

$$H_{\bar{\mathbb{Q}}}\left(\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}, 1, L\right) < \binom{L+n}{n},$$

ce qui signifie qu'il existe un polynôme F non nul tel que

$$F \in \mathcal{E}_{\bar{\mathbb{Q}}}\left(\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}, 1, L\right).$$

Par le lemme 4.8, on peut supposer que F est à coefficients dans $\mathbb{L}_{(p)}$.

Soit X l'ensemble algébrique défini dans $\mathbb{G}_{\mathrm{m}}^n$ par les équations $F(\boldsymbol{\zeta}\boldsymbol{X}) = 0$ où $\boldsymbol{\zeta}$ parcourt $\ker[p]$. Le polynôme F étant identiquement nul sur $\ker[p] \cdot \{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}$, il

existe une composante $\mathbb{L}_{(p)}$-irréductible V de X qui contient $\{\boldsymbol{\alpha}\}_{\mathbb{L}_{(p)}}$. De plus, X est stable sous l'action de $\ker[p]$, donc $\ker[p] \cdot V \subset X$. Ainsi $\ker[p] \cdot V$ est incomplètement défini par des polynômes de degré L et la proposition 3.3 de [**Phi86**] implique

$$\deg(\ker[p]V) \leq L^{\operatorname{codim} V}.$$

Or, par le lemme 2.1 de [**DP99**], si W est une variété géométriquement irréductible, on a

$$\deg([p]^{-1}W) = p^{\operatorname{codim} W} \deg(W).$$

Étant donné qu'une variété géométriquement irréductible ne peut pas être composante de l'image réciproque par $[p]$ de deux variétés géométriquement irréductibles distinctes, on a la même égalité pour les variétés. En appliquant ceci à $[p]V$, on a finalement

$$\deg(\ker[p]V) = \deg([p]^{-1}[p]V) = p^{\operatorname{codim} V} \deg([p]V).$$

D'où

$$\deg([p]V) \leq \left(\frac{L}{p}\right)^{\operatorname{codim} V} \leq ((2n+1)C\omega \log(3\omega))^{\operatorname{codim} V}$$

et, par le lemme 4.9 appliqué à $\mathbb{L}_{(p)}$, $\boldsymbol{\alpha}^p$ et $[p]V$,

$$\omega_{\mathbb{L}_{(p)}}(\boldsymbol{\alpha}^p) \leq n(2n+1)C\omega \log(3\omega).$$

On pose alors $c_0 = n(2n+1)C$ et la proposition est démontrée. □

4.3.2. Transcendance dans le cas de petite ramification

La transcendance dans le cas de petite ramification est plus classique : utilisation d'un lemme de Siegel pour la construction d'une fonction auxiliaire, extrapolation et lemme de zéros.

4.3.2.1. Construction de la fonction auxiliaire. — Nous allons maintenant construire une fonction auxiliaire, c'est-à-dire un polynôme dont on contrôle la hauteur et le degré et qui s'annule avec forte multiplicité en $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$. Dans [**AmDa04**], les auteurs utilisent pour cela un lemme de Siegel dû à E. Bombieri et J. D. Vaaler, qui fournit un polynôme à coefficients dans $\mathbb{L}$. Cependant, un tel lemme fait apparaître le discriminant du corps $\mathbb{L}$ dans la borne sur la hauteur du polynôme, ce que nous souhaitons éviter ici. Afin de contourner ce problème, il nous faut utiliser un lemme de Siegel « absolu ». Nous utiliserons une version due à S. David et P. Philippon (voir [**DP99**]) obtenue à l'aide du théorème plus général de S. Zhang sur les minima successifs d'une variété algébrique (voir [**Zha95b**]). Cette version est un raffinement du lemme de Siegel

absolu de D. Roy et J. Thunder (voir [**RT96**]). Si le polynôme obtenu a une hauteur majorée indépendamment du corps $\mathbb{L}$, nous perdons cependant tout contrôle sur le corps contenant ses coefficients. Un argument similaire à celui de la preuve du lemme 4.8 permet néanmoins de surmonter cet inconvénient. Rappelons, pour commencer, les notations.

Soit $S \subset \bar{\mathbb{Q}}^{N+1}$ un $\bar{\mathbb{Q}}$-espace vectoriel de dimension d. On définit la hauteur L_2 de S comme le fait Schmidt au paragraphe 8 du chapitre 1 de [**Sch96**] par la formule

$$h_{L_2}(S) = \sum_{v \in \mathcal{M}_{\mathbb{F}}} \frac{[\mathbb{F}_v : \mathbb{Q}_v]}{[\mathbb{F} : \mathbb{Q}]} \log \|\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_d\|_v,$$

où $(\boldsymbol{x}_1, \cdots, \boldsymbol{x}_d)$ est une base de S, $\mathbb{F}$ un corps de nombres contenant les coordonnées des $\boldsymbol{x}_i$ et $\|\cdot\|_v$ est la norme du sup si v est ultramétrique et la norme euclidienne sinon. Si S est la droite vectorielle engendrée par $\boldsymbol{x} \in \bar{\mathbb{Q}}^{N+1}$, on notera $h_{L_2}(\boldsymbol{x}) = h_{L_2}(S)$.

Énonçons maintenant le lemme.

Lemme 4.16. — *Soient $S \subset \bar{\mathbb{Q}}^{N+1}$ un $\bar{\mathbb{Q}}$-espace vectoriel et ε un nombre réel strictement positif. Alors, il existe un vecteur non nul $\boldsymbol{x} \in S$ tel que*

$$h_{L_2}(\boldsymbol{x}) \leq \frac{h_{L_2}(S)}{\dim S} + \frac{1}{2}\log(\dim(S)) + \varepsilon.$$

Démonstration. — Voir le lemme 4.7 de [**DP99**] ainsi que la remarque qui le suit. □

Nous pouvons maintenant construire la fonction auxiliaire dont nous aurons besoin.

Théorème 4.17. — *Soient $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$, $\boldsymbol{\alpha}$ un point de $\mathbb{G}_{\mathrm{m}}^n$ et L, T deux entiers naturels non nuls tels que*

$$2n\omega_{\mathbb{L}}(\boldsymbol{\alpha})T \leq L \quad \textit{et} \quad h(\boldsymbol{\alpha}) \leq \frac{T\log(L+1)}{L}.$$

Alors il existe $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$ tel que

$$h(F) \leq \frac{18n^2\omega_{\mathbb{L}}(\boldsymbol{\alpha})T^2\log(L+1)}{L} + \frac{1}{2}\log\binom{L+n}{n}.$$

Démonstration. — Notons $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d$ les conjugués de $\boldsymbol{\alpha}$ au-dessus de $\mathbb{L}$. Pour $i \in [\![1, d]\!]$ et $\boldsymbol{\lambda} \in \mathbb{N}^n$, $|\boldsymbol{\lambda}| \leq T$, on pose

$$\boldsymbol{y}_{\boldsymbol{\alpha}_i,\boldsymbol{\lambda}} = \left(\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}}\boldsymbol{\alpha}_i^{\boldsymbol{\mu}-\boldsymbol{\lambda}}\right)_{\boldsymbol{\mu}\in\mathbb{N}^n, |\boldsymbol{\mu}|\leq L} \in \bar{\mathbb{Q}}^{\binom{L+n}{n}}, \text{ où } \binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} = \prod_{j=1}^{n}\binom{\mu_j}{\lambda_j}.$$

En identifiant $\bar{\mathbb{Q}}[\boldsymbol{X}]_{\leq L}$ à $\bar{\mathbb{Q}}^{\binom{L+n}{n}}$, les $\boldsymbol{y}_{\boldsymbol{\alpha_i},\boldsymbol{\lambda}}$ sont des générateurs du sous-espace vectoriel $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)^{\perp}$, dont la dimension est $H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$. En utilisant l'inégalité

$$\begin{aligned}\left(\sum_{|\boldsymbol{\mu}|\leq L}\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}}^2\right)^{1/2} &\leq \sum_{|\boldsymbol{\mu}|\leq L}\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}}\\ &\leq \sum_{\mu_1=0}^{L}\cdots\sum_{\mu_n=0}^{L}\binom{\mu_1}{\lambda_1}\cdots\binom{\mu_n}{\lambda_n}\\ &\leq \prod_{i=1}^{n}\binom{L+1}{\lambda_i+1}\\ &\leq (L+1)^{T+n},\end{aligned}$$

on a la majoration

$$\|\boldsymbol{y}_{\boldsymbol{\alpha}_i,\boldsymbol{\lambda}}\|_{v,L_2} \leq (L+1)^{T+n}\|\iota(\boldsymbol{\alpha}_i)\|_v^L,$$

où v est une place archimédienne et $\|\cdot\|_{v,L_2}$ désigne la norme euclidienne associée à v. Ainsi, la hauteur L_2 des $\boldsymbol{y}_{\boldsymbol{\alpha}_i,\boldsymbol{\lambda}}$ est majorée :

$$h_{L_2}(\boldsymbol{y}_{\boldsymbol{\alpha}_i,\boldsymbol{\lambda}}) \leq (T+n)\log(L+1) + Lh(\boldsymbol{\alpha}).$$

On en déduit (voir le paragraphe 8 du chapitre 1 de [**Sch96**])

$$\begin{aligned}h_{L_2}(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)) &= h_{L_2}(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)^{\perp})\\ &\leq \dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)^{\perp})\max h_{L_2}(\boldsymbol{y}_{\boldsymbol{\alpha}_i,\boldsymbol{\lambda}})\\ &\leq H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)\left((T+n)\log(L+1) + Lh(\boldsymbol{\alpha})\right).\end{aligned}$$

Remarquons que $\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))$ est strictement positif. En effet, si $P_0 \in \mathbb{L}[\boldsymbol{X}]$ est un polynôme non nul s'annulant en $\boldsymbol{\alpha}$ de degré minimal $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$, alors pour tout $P \in \bar{\mathbb{Q}}[\boldsymbol{X}]$ de degré inférieur ou égal à $L - \omega_{\mathbb{L}}(\boldsymbol{\alpha})T$, le polynôme $P \cdot P_0^T$ appartient à $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$. Donc, en utilisant l'hypothèse $2nT\omega_{\mathbb{L}}(\boldsymbol{\alpha}) \leq L$,

$$\begin{aligned}\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)) &\geq \binom{L-\omega_{\mathbb{L}}(\boldsymbol{\alpha})T+n}{n}\\ &\geq \binom{(2n-1)\omega_{\mathbb{L}}(\boldsymbol{\alpha})T+n}{n}\\ &> 0.\end{aligned} \tag{4.12}$$

Nous appliquons maintenant le lemme de Siegel absolu (lemme 4.16) avec

$$\varepsilon = \frac{1}{2}\log\frac{\binom{L+n}{n}}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))}.$$

Ce dernier assure alors l'existence d'un élément non nul $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$ de hauteur

$$\begin{aligned} h_{L_2}(F) &\leq \frac{H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)\left((T+n)\log(L+1) + Lh(\boldsymbol{\alpha})\right)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))} \\ &\qquad + \frac{1}{2}\log(\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))) + \varepsilon \\ &\leq \frac{H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))}\left((T+n)\log(L+1) + Lh(\boldsymbol{\alpha})\right) \\ &\qquad + \frac{1}{2}\log\binom{L+n}{n}. \end{aligned}$$

Nous allons maintenant majorer la quantité

$$\frac{H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)}.$$

En utilisant l'hypothèse $2nT\omega_{\mathbb{L}}(\boldsymbol{\alpha}) \leq L$ et la première inégalité de (4.12), on a

$$\begin{aligned} \frac{H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))} &= \frac{\binom{L+n}{n} - \dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))} \\ &\leq \frac{\binom{L+n}{n} - \binom{L-\omega_{\mathbb{L}}(\boldsymbol{\alpha})T+n}{n}}{\binom{L-\omega_{\mathbb{L}}(\boldsymbol{\alpha})T+n}{n}} \\ &\leq \prod_{j=1}^{n}\left(1 + \frac{T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L - T\omega_{\mathbb{L}}(\boldsymbol{\alpha}) + j}\right) - 1 \\ &\leq \left(1 + \frac{2T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L}\right)^{n} - 1. \end{aligned}$$

En appliquant l'inégalité des accroissements finis à $x \mapsto (x+1)^n - 1$ entre 0 et $\frac{2T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L}$, on obtient finalement

$$\begin{aligned} \frac{H_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L))} &\leq n\left(1 + \frac{2T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L}\right)^{n-1}\frac{2T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L} \\ &\leq n\left(1 + \frac{1}{n}\right)^{n-1}\frac{2T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L} \\ &\leq ne\frac{2T\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{L}. \end{aligned}$$

L'hypothèse sur $h(\boldsymbol{\alpha})$, le fait que $2T + n \leq 3nT$ et l'inégalité $h(F) \leq h_{L_2}(F)$ permettent alors de conclure. □

4.3.2.2. Extrapolation. —

Lemme 4.18. — *Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$, $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et p un nombre premier. Soient $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$ et v une place de $\bar{\mathbb{Q}}$ divisant p. Alors pour tout morphisme $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{|\mathbb{L}} = \phi_p$ et tout conjugué $\tilde{\boldsymbol{\alpha}}$ de $\boldsymbol{\alpha}$ au-dessus de $\mathbb{L}$, on a*

$$|F^\tau(\tilde{\boldsymbol{\alpha}}^p)|_v \leq p^{-T/e_p(\mathbb{L})} \|F^\tau\|_v \|\iota(\tilde{\boldsymbol{\alpha}})\|_v^{pL}.$$

La démonstration de ce lemme est semblable à celle du lemme 4.13 :

Démonstration. — Comme dans la preuve du lemme 4.13, nous pouvons supposer que F est à coefficients entiers algébriques, que l'on a $\|F^\tau\|_v = 1$ et que $\boldsymbol{\alpha}$ est à coordonnées entières.

Soit $\mathbb{F}$ une extension galoisienne de $\mathbb{Q}$ contenant le corps $\mathbb{L}$, les coefficients de F, les coordonnées de $\boldsymbol{\alpha}$ et les racines p-ièmes de l'unité. Soit $\mathcal{O}_{\mathbb{F}_v}$ (resp. $\mathcal{O}_{\mathbb{L}_v}$) l'anneau des entiers du complété de $\mathbb{F}$ (resp. $\mathbb{L}$) par rapport à v. D'après [**Ser68**, Prop. 12, p. 66], $\mathcal{O}_{\mathbb{F}_v}$ est monogène sur $\mathcal{O}_{\mathbb{L}_v}$: il existe $\delta \in \mathcal{O}_{\mathbb{F}_v}$ tel que $\mathcal{O}_{\mathbb{F}_v} = \mathcal{O}_{\mathbb{L}_v}[\delta]$. En particulier, pour tout $i \in [\![1, n]\!]$, il existe $a_i \in \mathcal{O}_{\mathbb{L}_v}[X]$ tel que

$$\alpha_i = a_i(\delta).$$

Considérons maintenant $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{|\mathbb{L}} = \phi_p$; il induit un élément de $\mathrm{Gal}(\mathbb{F}_v/\mathbb{Q}_v)$ que nous noterons encore τ. La congruence (4.4) se prolonge à $\mathcal{O}_{\mathbb{L}_v}$:

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}_v}, \quad \tau\gamma \equiv \gamma^p \mod \mathcal{Q}\mathcal{O}_{\mathbb{L}_v}, \tag{4.13}$$

où $\mathcal{Q}$ est l'idéal de $\mathcal{O}_{\mathbb{L}}$ tel que $\mathcal{Q}^{e_p(\mathbb{L})} = p\mathcal{O}_{\mathbb{L}}$. Pour tout $i \in [\![1, n]\!]$, posons

$$\beta_i = a_i^\tau(\delta^p)$$

de sorte que

$$\beta_i \equiv \alpha_i^p \mod \mathcal{Q}\mathcal{O}_{\mathbb{F}_v}. \tag{4.14}$$

Remarquons que $\partial_{\boldsymbol{\lambda}}(F) \in \mathcal{O}_{\mathbb{F}}[\boldsymbol{X}]$. Nous allons montrer que pour tout polynôme $H \in \mathcal{O}_{\mathbb{F}}[\boldsymbol{X}]$ nul en $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ avec multiplicité au moins t, on a

$$H^\tau(\boldsymbol{\beta}) \equiv 0 \mod (\mathcal{Q}\mathcal{O}_{\mathbb{F}_v})^t. \tag{4.15}$$

Soit $\Delta \in \mathcal{O}_{\mathbb{L}_v}[X]$ le polynôme minimal de δ sur $\mathbb{L}_v$ et soit s la plus grande puissance de Δ divisant $G = H(a_1, \ldots, a_n)$; montrons que $s \geq t$. La dérivée $G^{(s)}$ n'est pas divisible par Δ. Or le polynôme $G^{(s)}$ appartient à l'idéal engendré par

$$\left\{ \partial_{\boldsymbol{\lambda}}(H)(a_1, \ldots, a_n) \ , \ |\boldsymbol{\lambda}| \leq s \right\}$$

donc il existe un n-uplet $\boldsymbol{\lambda} \in \mathbb{N}^n$ avec $|\boldsymbol{\lambda}| \leq s$ tel que $\partial_{\boldsymbol{\lambda}}(H)(a_1, \ldots, a_n)$ ne soit pas divisible par Δ. Cela signifie qu'il existe $\sigma \in \mathrm{Gal}(\mathbb{F}_v/\mathbb{L}_v)$ tel que

$$\partial_{\boldsymbol{\lambda}}(H)(\alpha_1^\sigma, \ldots, \alpha_n^\sigma) = \partial_{\boldsymbol{\lambda}}(H)(a_1(\delta^\sigma), \ldots, a_n(\delta^\sigma)) \neq 0.$$

Puisque H est nul en $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ avec multiplicité au moins t, on en déduit $|\boldsymbol{\lambda}| \geq t$ donc $s \geq t$. Ainsi, on vient de montrer que Δ^t divise $H(a_1, \ldots, a_n)$ dans $\mathbb{F}_v[X]$ donc dans $\mathcal{O}_{\mathbb{F}_v}[X]$. On peut alors écrire

$$H^\tau(a_1^\tau(X), \ldots, a_n^\tau(X)) = R^\tau(X)(\Delta^\tau(X))^t, \quad R \in \mathcal{O}_{\mathbb{F}_v}[X].$$

En évaluant en δ^p dans cette équation et en tenant compte du fait que, par (4.13),

$$\Delta^\tau(\delta^p) \equiv (\Delta(\delta))^p \equiv 0 \mod \mathcal{Q}\mathcal{O}_{\mathbb{F}_v},$$

on obtient (4.15).

Si l'on applique (4.15) à $H = \partial_{\boldsymbol{\lambda}}(F)$ et $t = T - |\boldsymbol{\lambda}|$, pour un n-uplet quelconque $\boldsymbol{\lambda}$ vérifiant $|\boldsymbol{\lambda}| \leq T$, on obtient

$$\partial_{\boldsymbol{\lambda}}(F)^\tau(\boldsymbol{\beta}) \equiv 0 \mod (\mathcal{Q}\mathcal{O}_{\mathbb{F}_v})^{T-|\boldsymbol{\lambda}|}. \tag{4.16}$$

Enfin, par la formule de Taylor, on a

$$F^\tau(\boldsymbol{\alpha}^p) = \sum_{|\boldsymbol{\lambda}| \geq 0} (\boldsymbol{\alpha}^p - \boldsymbol{\beta})^{\boldsymbol{\lambda}} \partial_{\boldsymbol{\lambda}}(F)^\tau(\boldsymbol{\beta}),$$

où $(\boldsymbol{\alpha}^p - \boldsymbol{\beta})^{\boldsymbol{\lambda}} = \prod_{i=1}^n (\alpha_i^p - \beta_i)^{\lambda_i}$. D'où, avec (4.14), $(\boldsymbol{\alpha}^p - \boldsymbol{\beta})^{\boldsymbol{\lambda}} \equiv 0 \mod (\mathcal{Q}\mathcal{O}_{\mathbb{F}_v})^{|\boldsymbol{\lambda}|}$. On en déduit avec (4.16)

$$F^\tau(\boldsymbol{\alpha}^p) \equiv 0 \mod (\mathcal{Q}\mathcal{O}_{\mathbb{F}_v})^T$$

et le lemme est ainsi démontré. □

Lemme 4.19. — *Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$, $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$, L, T deux entiers naturels non nuls, E un réel strictement positif et p un nombre premier dont l'indice de ramification dans $\mathbb{L}$ est inférieur à E. Soit $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$. Supposons*

$$h(\boldsymbol{\alpha}) \leq \frac{1}{4}\frac{T \log p}{EpL} \quad \textit{et} \quad h(F) \leq \frac{1}{4}\frac{T \log p}{E}. \tag{4.17}$$

On pose

$$T_1 = 2^{-1}\left(1 + \frac{(n+1)E\log(L+1)}{\log p}\right)^{-1} \times T$$

et on suppose $T_1 \geq 1$. Alors pour tout prolongement τ_p de ϕ_p à $\bar{\mathbb{Q}}$, le polynôme F^{τ_p} appartient à $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}^p\}_{\mathbb{L}}, \lceil T_1 \rceil^{(3)}, L)$.

(3) Si x est un réel, nous notons $\lceil x \rceil$ l'entier qui lui est immédiatement supérieur.

Démonstration. — Soit $\mathbb{F}$ une extension galoisienne de $\mathbb{Q}$ contenant $\mathbb{L}$, les coefficients de F et les coordonnées de $\boldsymbol{\alpha}$. Soient $\boldsymbol{\lambda} \in \mathbb{N}^n$ tel que $|\boldsymbol{\lambda}| = T^* < T$ et v une place de $\mathbb{F}$. Comme $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$, on a $\partial_{\boldsymbol{\lambda}}(F) \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T-T^*, L)$. Le lemme 4.18 affirme que pour tout prolongement τ_p de ϕ_p à $\bar{\mathbb{Q}}$, on a

$$\begin{aligned} |\partial_{\boldsymbol{\lambda}}(F)^{\tau_p}(\boldsymbol{\alpha}^p)|_v &\leq p^{-(T-T^*)/e_p(\mathbb{L})} \|\partial_{\boldsymbol{\lambda}}(F)^{\tau_p}\|_v \|\iota(\boldsymbol{\alpha})\|_v^{pL} \\ &\leq p^{-(T-T^*)/e_p(\mathbb{L})} \|F^{\tau_p}\|_v \|\iota(\boldsymbol{\alpha})\|_v^{pL} \end{aligned}$$

si v est une place divisant p. D'autre part, on déduit de l'inégalité

$$\sum_{|\boldsymbol{\mu}| \leq L} \binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} \leq \binom{L+1}{\lambda_1+1} \cdots \binom{L+1}{\lambda_n+1} \leq (L+1)^{|\boldsymbol{\lambda}|+n}$$

et de l'inégalité ultramétrique les majorations

$$|\partial_{\boldsymbol{\lambda}}(F)^{\tau_p}(\boldsymbol{\alpha}^p)|_v \leq \begin{cases} \|F^{\tau_p}\|_v \|\iota(\boldsymbol{\alpha})\|_v^{pL} & \text{si } v \nmid \infty, \\ (L+1)^{T^*+n} \|F^{\tau_p}\|_v \|\iota(\boldsymbol{\alpha})\|_v^{pL} & \text{si } v \mid \infty. \end{cases}$$

Ainsi, si $\partial_{\boldsymbol{\lambda}}(F)^{\tau_p}(\boldsymbol{\alpha}^p) \neq 0$, les inégalités ci-dessus et la formule du produit donnent

$$0 \leq (T^*+n)\log(L+1) + h(F) + pLh(\boldsymbol{\alpha}) - \frac{T-T^*}{e_p(\mathbb{L})} \log p.$$

Avec les hypothèses (4.17) et l'inégalité $T^* + n \leq (n+1)T^*$, on obtient la minoration

$$T^* \geq 2^{-1} \left(1 + \frac{(n+1)E\log(L+1)}{\log p}\right)^{-1} \times T = T_1.$$

On procède de même pour les conjugués de $\boldsymbol{\alpha}$ au-dessus de $\mathbb{L}$, ce qui achève la preuve. □

En utilisant r fois le lemme 4.19, on obtient :

Lemme 4.20. — *Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Soient L, T et r trois entiers naturels non nuls, E un réel strictement positif et $p_1, \ldots, p_r$ des nombres premiers dont l'indice de ramification dans $\mathbb{L}$ est inférieur à E. Pour $s \in [\![0, r]\!]$, on pose*

$$T_s = 2^{-s} T \prod_{j=1}^{s} \left(1 + \frac{(n+1)E\log(L+1)}{\log p_j}\right)^{-1}$$

et on suppose $T_r \geq 1$. Soit $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$. Supposons

$$h(\boldsymbol{\alpha}) \leq \frac{1}{4} \frac{T_{r-1} \min \log p_i}{EL\, p_1 \cdots p_r} \quad \textit{et} \quad h(F) \leq \frac{1}{4} \frac{T_{r-1} \min \log p_i}{E}. \tag{4.18}$$

Alors pour tous $\tau_{p_1},\dots,\tau_{p_r}$, respectivement prolongements à $\bar{\mathbb{Q}}$ de $\phi_{p_1},\dots,\phi_{p_r}$, le polynôme $F^{\tau_{p_1}\cdots\tau_{p_r}}$ appartient à $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}^{p_1\cdots p_r}\}_{\mathbb{L}},\lceil T_r\rceil,L)$.

Démonstration. — On montre ce lemme par récurrence sur r. Le cas $r=1$ correspond au lemme 4.19. Supposons donc $r\geq 2$. Soient L et T deux entiers naturels non nuls, E un réel strictement positif, $p_1,\dots,p_r$ des nombres premiers dont l'indice de ramication dans $\mathbb{L}$ est inférieur à E et $F\in\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}},T,L)$ tels que les conditions (4.18) soient satisfaites. En particulier, on a

$$h(\boldsymbol{\alpha})\leq\frac{1}{4}\frac{T_{r-2}\min\log p_i}{EL\ p_1\cdots p_{r-1}}\quad\text{et}\quad h(F)\leq\frac{1}{4}\frac{T_{r-2}\min\log p_i}{E}.$$

Par hypothèse de récurrence, pour tous $\tau_{p_1},\dots,\tau_{p_{r-1}}$, respectivement prolongements à $\bar{\mathbb{Q}}$ de $\phi_{p_1},\dots,\phi_{p_{r-1}}$ le polynôme F est tel que

$$F^{\tau_{p_1}\cdots\tau_{p_{r-1}}}\in\mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}^{p_1\cdots p_{r-1}}\}_{\mathbb{L}},\lceil T_{r-1}\rceil,L).$$

Or $h(F^{\tau_{p_1}\cdots\tau_{p_{r-1}}})=h(F)$ et $h(\boldsymbol{\alpha}^{p_1\cdots p_{r-1}})=p_1\cdots p_{r-1}h(\boldsymbol{\alpha})$, d'où

$$h(\boldsymbol{\alpha}^{p_1\cdots p_{r-1}})\leq\frac{T_{r-1}\log p_r}{Ep_rL}\leq\frac{\lceil T_{r-1}\rceil\log p_r}{Ep_rL}.$$

On applique alors le lemme 4.19 en remplaçant respectivement $T,p,\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ et F par $\lceil T_{r-1}\rceil,p_r,\{\boldsymbol{\alpha}^{p_1\cdots p_{r-1}}\}_{\mathbb{L}}$ et $F^{\tau_{p_1}\cdots\tau_{p_{r-1}}}$ pour conclure. □

4.3.2.3. Lemme de zéros. — Soient $\boldsymbol{\alpha}\in\mathbb{G}_{\mathrm{m}}^n$, $\mathbb{L}$ une extension abélienne et L, N_j, $j\in[\![1,n]\!]$, des entiers naturels non nuls. Pour tout $j\in[\![1,n]\!]$, on note $\mathcal{P}_j$ un ensemble contenant 1 et des nombres premiers inférieurs à N_j et pour tout entier p dans l'un des $\mathcal{P}_j$, on fixe $\sigma_p\in\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.

Théorème 4.21. — *Soit G un polynôme non nul tel que $G^{\sigma_{p_1}\cdots\sigma_{p_n}}$ appartient à $\mathcal{E}_{\mathbb{L}}(\{\boldsymbol{\alpha}^{p_1\cdots p_n}\}_{\mathbb{L}},1,L)$ pour tout $(p_1,\dots,p_n)\in\mathcal{P}_1\times\cdots\times\mathcal{P}_n$. Alors il existe un entier $r\in[\![1,n]\!]$, une sous-variété algébrique propre V de $\mathbb{G}_{\mathrm{m}}^n$ définie sur $\mathbb{L}$ de codimension inférieure ou égale à r et $(p_{r+1},\dots,p_n)\in\mathcal{P}_{r+1}\times\cdots\times\mathcal{P}_n$ tels que*

$$\boldsymbol{\alpha}^{p_{r+1}\cdots p_n}\in\sigma_{p_n}\cdots\sigma_{p_{r+1}}V$$

et

$$\deg\left(\bigcup_{p\in\mathcal{P}_r}\sigma_p^{-1}[p]V\right)\leq(N_1\cdots N_{r-1}L)^{\mathrm{codim}(V)}.\tag{4.19}$$

Démonstration. — À la manière de [**AmDa99**], on définit une suite d'idéaux $\mathcal{J}_1, \ldots, \mathcal{J}_{n+1}$ de $\bar{\mathbb{Q}}[\boldsymbol{X}]$ en posant

$$\begin{aligned}
\mathcal{J}_1 &= (G(\boldsymbol{X})),\\
\mathcal{J}_2 &= (G^{\sigma_{p_1}}(\boldsymbol{X}^{p_1}),\ p_1 \in \mathcal{P}_1),\\
\mathcal{J}_3 &= (G^{\sigma_{p_1}\sigma_{p_2}}(\boldsymbol{X}^{p_1p_2}),\ (p_1,p_2) \in \mathcal{P}_1 \times \mathcal{P}_2),\\
&\vdots\\
\mathcal{J}_{n+1} &= (G^{\sigma_{p_1}\cdots\sigma_{p_n}}(\boldsymbol{X}^{p_1\cdots p_n}),\ (p_1,\ldots,p_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n).
\end{aligned}$$

Pour tout $r \in [\![1, n+1]\!]$, on note X_r l'ensemble algébrique défini par $\mathcal{J}_r$. On a $[p]X_{r+1} \subset \sigma_p X_r$ pour tout $p \in \mathcal{P}_r$. Notons Y_r la réunion des composantes $\mathbb{L}$-irréductibles V de X_r pour lesquelles il existe $(p_r, \ldots, p_n) \in \mathcal{P}_r \times \cdots \times \mathcal{P}_n$ tel que

$$\boldsymbol{\alpha}^{p_r\cdots p_n} \in \sigma_{p_n} \cdots \sigma_{p_r} V.$$

Par hypothèse sur G, on a $Y_r \neq \emptyset$. De plus, pour tout $r \in [\![1, n]\!]$ et pour tout $p \in \mathcal{P}_r$,

$$[p]Y_{r+1} \subset \sigma_p Y_r. \tag{4.20}$$

En particulier, comme $1 \in \mathcal{P}_r$, on a les inclusions $Y_{n+1} \subset \sigma_1 Y_n \subset \cdots \subset \sigma_1^n Y_1$; par le principe des tiroirs, il existe alors un indice $l \in [\![1, n]\!]$ pour lequel Y_l et Y_{l+1} ont la même dimension. Soient r le plus grand indice pour lequel cette propriété est vérifiée et d la dimension correspondante ; ainsi $n - d \leq r$. Soit V une composante $\mathbb{L}$-irréductible de dimension d de Y_{r+1}. Posons

$$W = \bigcup_{p \in \mathcal{P}_r} \sigma_p^{-1}[p]V.$$

Par la propriété (4.20), on a

$$W \subset Y_r.$$

Ainsi, l'ensemble algébrique équidimensionnel W est incomplètement défini par des polynômes de degré au plus $N_1 \cdots N_{r-1} L$; la proposition 3.3 de [**Phi86**] implique alors

$$\deg(W) \leq (N_1 \cdots N_{r-1} L)^{\operatorname{codim}(V)},$$

ce qui achève la démonstration du théorème. □

4.3.3. Théorème clé

Le but de cette dernière partie est d'établir un théorème qui résume l'étape de transcendance. Soient $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Pour alléger les notations, nous posons $\omega = \omega_{\mathbb{L}}(\boldsymbol{\alpha})$. Nous désignerons par C_0 un réel

strictement positif, ne dépendant que de n et suffisamment grand pour que les inégalités que nous considérerons soient vraies. Nous noterons également $c_1, c_2, \ldots$, des réels strictement positifs (effectivement calculables) ne dépendant que de n. Soient ρ et δ des nombres réels positifs tels que

$$(1+\delta)(1+\rho) \leq (1+n)\big(((n+1)!-1)(1+2n^2)+1\big)^n.$$

Nous fixons les paramètres suivants[(4)] :

$$T = \left[C_0^{\delta n+1/2} \frac{(\log(3\omega))^{n(\delta+1)}}{(\log\log(16\omega))^n}\right], \quad L = \omega T^2 \quad \text{et} \quad E = (C_0 \log(3\omega))^\delta.$$

Pour tout $j \in [\![1, n]\!]$, nous posons

$$N_j = (C_0 \log(3\omega))^{2n(1+\rho)(1+\delta)j.j!}$$

et définissons l'ensemble suivant :

$$\mathcal{P}_j = \{1\} \cup \{p \text{ premier}, N_j/2 \leq p \leq N_j\}.$$

Remarquons que $\sum_{i=1}^{j} i \cdot i! = (j+1)! - 1$ et que cela implique

$$N_1 \cdots N_j = (C_0 \log(3\omega))^{2n(1+\rho)(1+\delta)((j+1)!-1)}. \tag{4.21}$$

Par ailleurs,

$$\log(3\omega) \leq \log(L+1) \leq c_1(\log C_0)\log(3\omega).$$

La proposition qui suit résume l'étape de transcendance dans le cas de petite ramification.

Proposition 4.22. — *Supposons*

$$h(\boldsymbol{\alpha}) \leq \Big(\omega(C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)((n+1)!-1)+2n(\delta+1)-1}\Big)^{-1} \tag{4.22}$$

et

$$\forall p \in \bigcup_{j=1}^{n} \mathcal{P}_j, \quad e_p(\mathbb{L}) \leq E.$$

Il existe alors un polynôme non nul $F \in \bar{\mathbb{Q}}[\boldsymbol{X}]$ de degré inférieur ou égal à L tel que pour tout $(p_1, \ldots, p_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ et pour tous $\tau_{p_1}, \ldots, \tau_{p_n}$ prolongeant à $\bar{\mathbb{Q}}$ les morphismes $\phi_{p_1}, \ldots, \phi_{p_n}$, le polynôme $F^{\tau_{p_1}\cdots\tau_{p_n}}$ est nul sur $\{\boldsymbol{\alpha}^{p_1\cdots p_n}\}_{\mathbb{L}}$.

(4) Nous posons « $\log\log(16\omega)$ » afin d'assurer que cette quantité est toujours plus grande que 1, quelle que soit la valeur de ω.

Démonstration. — On a

$$\frac{2n\omega T}{L} = \frac{2n}{T} < 1$$

et, avec l'hypothèse (4.22),

$$\frac{L}{T\log(L+1)}h(\boldsymbol{\alpha}) \leq \omega T h(\boldsymbol{\alpha}) \leq \omega C_0^{\delta n+1/2}(\log(3\omega))^{n(\delta+1)}h(\boldsymbol{\alpha}) < 1,$$

de sorte que les hypothèses du théorème 4.17 sont vérifiées. On en déduit l'existence de $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\boldsymbol{\alpha}\}_{\mathbb{L}}, T, L)$ tel que

$$\begin{aligned} h(F) &\leq \frac{18n^2\omega T^2\log(L+1)}{L} + \frac{1}{2}\log\binom{L+n}{n} \\ &\leq c_2(\log C_0)\log(3\omega). \end{aligned}$$

Nous allons montrer, grâce au lemme 4.20, que ce polynôme F convient. Pour cela, vérifions que les hypothèses de ce lemme sont satisfaites. Soit $(q_1,\dots,q_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ et supposons $q_{j_1},\dots,q_{j_r}$ premiers et $q_j = 1$ pour $j \notin \{j_1,\dots,j_r\}$. Pour $i \in [\![1,r]\!]$, notons $p_i = q_{j_i}$; on a

$$\log p_i \geq c_3 \log\log(16\omega).$$

Considérons la quantité T_{r-1} définie dans le lemme 4.20 ; on a

$$\begin{aligned} T_{r-1}^{-1} &= 2^{r-1}T^{-1}\prod_{j=1}^{r-1}\left(1+\frac{(n+1)E\log(L+1)}{\log p_j}\right) \\ &\leq c_4 T^{-1}\prod_{j=1}^{r-1}\left(\frac{E\log(L+1)}{\log\log(16\omega)}\right) \\ &\leq c_5 C_0^{-(\delta n+1/2)}\frac{(\log\log(16\omega))^n}{(\log(3\omega))^{n(\delta+1)}}\left(\frac{C_0^{\delta}(\log C_0)(\log(3\omega))^{\delta+1}}{\log\log(16\omega)}\right)^{n-1} \\ &\leq c_5\frac{(\log C_0)^{n-1}}{C_0^{(\delta+1/2)}}\frac{\log\log(16\omega)}{(\log(3\omega))^{(\delta+1)}}. \end{aligned}$$

Ainsi,

$$\begin{aligned} \frac{4Eh(F)}{T_{r-1}\min\log p_i} &\leq c_6\frac{(C_0\log(3\omega))^{\delta}(\log C_0)(\log(3\omega))}{\log\log(16\omega)} \\ &\qquad \times\frac{(\log C_0)^{n-1}}{C_0^{(\delta+1/2)}}\frac{\log\log(16\omega)}{(\log(3\omega))^{(\delta+1)}} \\ &\leq c_6\frac{(\log C_0)^n}{C_0^{1/2}} \\ &< 1. \end{aligned}$$

Par ailleurs, par hypothèse sur $h(\boldsymbol{\alpha})$ et en utilisant (4.21) avec $j = n$, on a

$$N_1 \cdots N_n h(\boldsymbol{\alpha}) \leq \omega^{-1}(C_0 \log(3\omega))^{-(2n(\delta+1)-1)}.$$

D'où

$$\begin{aligned}
\frac{4ELp_1 \cdots p_r}{T_{r-1} \min \log p_i} h(\boldsymbol{\alpha}) &\leq \frac{4\omega E T^2 N_{j_1} \cdots N_{j_r}}{T_{r-1}(\log\log(16\omega))} h(\boldsymbol{\alpha}) \\
&\leq c_7 \omega \frac{C_0^{2\delta n+\delta+1}(\log(3\omega))^{2n(\delta+1)+\delta}}{(\log\log(16\omega))^{2n+1}} T_{r-1}^{-1} N_1 \cdots N_n h(\boldsymbol{\alpha}) \\
&\leq c_8 \frac{C_0^{2\delta n+1/2}(\log C_0)^{n-1}(\log(3\omega))^{2n(\delta+1)-1}}{(\log\log(16\omega))^{2n}} \\
&\qquad \times (C_0 \log(3\omega))^{-(2n(\delta+1)-1)} \\
&\leq c_8 \frac{(\log C_0)^{n-1}}{C_0^{2n-3/2}} \\
&< 1.
\end{aligned}$$

Le lemme 4.20 assure alors que pour tous $\tau_{p_1}, \ldots, \tau_{p_r}$ prolongeant respectivement $\phi_{p_1}, \ldots, \phi_{p_r}$, le polynôme $F^{\tau_{p_1} \cdots \tau_{p_r}}$ est nul sur $\{\boldsymbol{\alpha}^{p_1 \cdots p_r}\}_{\mathbb{L}}$ à un ordre supérieur ou égal à T_r, avec

$$\begin{aligned}
T_r &\geq c_9 T \prod_{j=1}^{r} \left(\frac{\log\log(16\omega)}{E \log(L+1)} \right) \\
&\geq c_{10} C_0^{(\delta n+1/2)} \frac{(\log(3\omega))^{n(\delta+1)}}{(\log\log(16\omega))^n} \left(\frac{\log\log(16\omega)}{C_0^{\delta}(\log C_0)(\log(3\omega))^{\delta+1}} \right)^n \\
&\geq c_{10} \frac{C_0^{1/2}}{(\log C_0)^n} \\
&\geq 1.
\end{aligned}$$

Ainsi, nous avons montré que pour tout $(q_1, \ldots, q_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ et pour tous $\tau_{q_1}, \ldots, \tau_{q_n}$ prolongeant respectivement $\phi_{q_1}, \ldots, \phi_{q_n}$, le polynôme $F^{\tau_{q_1} \cdots \tau_{q_n}}$ est nul sur $\{\boldsymbol{\alpha}^{q_1 \cdots q_n}\}_{\mathbb{L}}$. □

Afin de pouvoir maintenant tirer parti du lemme de zéros, nous devons exclure des ensembles $\mathcal{P}_j$ les premiers exceptionnels associés à une variété V. Nous remarquons que leur quantité est négligeable, au vu du choix des paramètres.

Lemme 4.23. — *Soient $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et V une variété définie sur $\mathbb{L}$ telle que*

$$\log \deg(V) \leq (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)-1}. \tag{4.23}$$

Pour tout $j \in [\![1,n]\!]$, il existe alors un sous-ensemble $\mathcal{P}_j(V) \subset \mathcal{P}_j$ dont le cardinal satisfait l'inégalité

$$|\mathcal{P}_j(V)| \geq c_{11}\frac{(C_0\log(3\omega))^{2n(\rho+1)(\delta+1)j\cdot j!}}{(\log C_0)\log\log(16\omega)}.$$

et tel que $1 \in \mathcal{P}_j(V)$ et $p_1\cdots p_n \notin E_{\mathrm{exc}}(V)$ pour tout $(p_1,\ldots,p_n) \in \mathcal{P}_1(V)\times\cdots\times\mathcal{P}_n(V)$.

Démonstration. — La démonstration est en tout point identique à celle du lemme 5.2 de [**AmDa99**] en remplaçant $\mathbb{Q}$ par $\mathbb{L}$. □

Nous pouvons maintenant énoncer et montrer le théorème clé.

Théorème 4.24. — *Soit V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie sur $\mathbb{L}$ et $\mathbb{L}$-irréductible telle que*

$$\log(\deg V) \leq (C_0\log(3\omega))^{2n(\delta+1)(\rho+1)-1}.$$

Supposons

$$h(\boldsymbol{\alpha}) \leq \left(\omega(C_0\log(3\omega))^{2n(\delta+1)(\rho+1)((n+1)!-1)+2n(\delta+1)-1}\right)^{-1}. \tag{4.24}$$

Supposons de plus qu'il n'existe pas de sous-variété de torsion B définie sur $\mathbb{L}$ et contenant un conjugué de $\boldsymbol{\alpha}$ telle que

$$(\deg B)^{1/\mathrm{codim}(B)} \leq \omega(C_0\log(3\omega))^{2n(\delta+1)(\rho+1)(n+1)!}. \tag{4.25}$$

Alors l'une des deux propriétés suivantes est vraie :

1. *Il existe un premier $p \notin E_{\mathrm{exc}}(V)$ tel que*

$$E \leq p \leq N_n$$

qui est ramifié dans $\mathbb{L}$ avec

$$e_p(\mathbb{L}) \geq E$$

et tel que

$$\omega_{\mathbb{L}_{(p)}}(\boldsymbol{\alpha}^p) \leq c_0\omega_{\mathbb{L}}(\boldsymbol{\alpha})\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})). \tag{4.26}$$

2. *Il existe un entier $l \notin E_{\mathrm{exc}}(V)$ tel que*

$$l \leq (C_0\log(3\omega))^{2n(1+\delta)(\rho+1)((n+1)!-1)}$$

et

$$\omega_{\mathbb{L}}(\boldsymbol{\alpha}^l) \leq \frac{\omega_{\mathbb{L}}(\boldsymbol{\alpha})}{C_0^{1/2}(C_0\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n(1+\delta)\rho}}. \tag{4.27}$$

Démonstration. — Considérons la réunion

$$\mathcal{P}(V) = \bigcup_{j=1}^{n} \mathcal{P}_j(V).$$

Nous allons distinguer deux cas. Supposons dans un premier temps qu'il existe un premier $p \in \mathcal{P}(V)$ tel que $e_p(\mathbb{L}) \geq E$. Soit c_0 le réel strictement positif de la proposition 4.15 ; on a

$$c_0 \frac{p\omega}{\log p} h(\boldsymbol{\alpha}) \leq c_0 (C_0 \log(3\omega))^{-e},$$

avec

$$\begin{aligned} e &= 2n(\delta+1)(\rho+1)((n+1)!-1) + 2n(\delta+1) - 1 - 2n(\rho+1)(\delta+1)n.n! \\ &= 2n(\rho+1)(\delta+1)(n!-1) + 2n(\delta+1) - 1 \\ &> 0. \end{aligned}$$

D'où

$$c_0 \frac{p\omega}{\log p} h(\boldsymbol{\alpha}) < 1.$$

Ainsi, la proposition 4.15 s'applique et nous obtenons la première assertion de la conclusion alternative (en remarquant que $N_n \geq p \geq N_1/2 \geq E$).

Supposons maintenant que pour tout $p \in \mathcal{P}(V)$, $e_p(\mathbb{L}) \leq E$. Soit F le polynôme de degré inférieur ou égal à L fourni par la proposition 4.22. On a $F^{\tau_{p_1} \cdots \tau_{p_n} \sigma}$ qui est nul sur $\{\boldsymbol{\alpha}^{p_1 \cdots p_n}\}_{\mathbb{L}}$ pour tout $(p_1, \ldots, p_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ et pour tous $\tau_{p_1}, \ldots, \tau_{p_n}$ prolongeant à $\bar{\mathbb{Q}}$ les morphismes $\phi_{p_1}, \ldots, \phi_{p_n}$. Quitte à multiplier F par un nombre algébrique, on peut supposer qu'un de ses coefficients est égal à 1. Si $\mathbb{F}$ désigne une extension galoisienne de $\mathbb{L}$ contenant les coefficients de F, alors le polynôme

$$G = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{L})} F^{\sigma}$$

est non nul et satisfait les hypothèses du lemme de zéros (théorème 4.21) appliqué aux ensembles d'entiers $\mathcal{P}_j(V)$ définis dans le lemme précédent (lemme 4.23) et aux morphismes ϕ_p correspondants. Le lemme de zéros nous fournit donc un indice r et une sous-variété Z de $\mathbb{G}_{\mathrm{m}}^n$ définie sur $\mathbb{L}$, de codimension inférieure ou égale à r, contenant un conjugué d'une certaine puissance $\boldsymbol{\alpha}^l$, avec $l \notin E_{\mathrm{exc}}(V)$ (par le lemme 4.23) et

$$l \leq N_{r+1} \cdots N_n \leq N_1 \cdots N_n = (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)((n+1)!-1)},$$

pour laquelle l'inégalité (4.19) est satisfaite. Cette inégalité donne en particulier (car $1 \in \mathcal{P}_r(V)$) :

$$\begin{aligned}
\deg(Z)^{1/\operatorname{codim}(Z)} &\leq LN_1 \cdots N_{r-1} \\
&\leq LN_1 \cdots N_{n-1} \\
&\leq \omega C_0^{2\delta n+1} (\log(3\omega))^{2n(\delta+1)} \\
&\qquad \times (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(n!-1)} \\
&\leq \omega (C_0 \log(3\omega))^{2n(\delta+1)((\rho+1)(n!-1)+1)} \\
&\leq \omega (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)n!}.
\end{aligned} \tag{4.28}$$

Une composante $\mathbb{L}$-irréductible B de $[l]^{-1}Z$ contient un conjugué de $\{\boldsymbol{\alpha}\}_{\mathbb{L}}$ et son degré satisfait l'inégalité

$$\begin{aligned}
\deg(B)^{1/\operatorname{codim}(B)} &\leq l \deg(Z)^{1/\operatorname{codim}(Z)} \\
&\leq N_{r+1} \cdots N_n L N_1 \cdots N_{r-1} \\
&\leq \omega (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(n+1)!}.
\end{aligned}$$

Par hypothèse, la variété B (donc Z) n'est pas de torsion. Par ailleurs, l'inégalité (4.28) montre en particulier que

$$\log(\deg(Z)) \leq c_{13} \log(C_0) \log(3\omega).$$

Soit $\mathcal{Q} = \mathcal{P}_r(V) \setminus E_{\text{exc}}(Z)$; la proposition 4.7 et l'inégalité ci-dessus assurent que $|E_{\text{exc}}(Z)|$ est négligeable devant la minoration de $|\mathcal{P}_j(V)|$ fournie par le lemme 4.23, de sorte que

$$|\mathcal{Q}| \geq c_{14} \frac{(C_0 \log(3\omega))^{2n(\rho+1)(\delta+1)r \cdot r!}}{(\log C_0) \log\log(16\omega)}. \tag{4.29}$$

Comme Z n'est pas de torsion, le lemme 2.3, point (i) de [**AmDa99**] montre que les variétés $\tau_p^{-1}[p]Z$ et $\tau_q^{-1}[q]Z$ pour $(p,q) \in \mathcal{P}_r(V), p \neq q$, n'ont pas de composantes communes (ce qui revient à dire qu'elles sont distinctes). Par ailleurs, $\mathcal{Q} \cap E_{\text{exc}}(Z) = \emptyset$ donc pour $p \in \mathcal{Q}$, $\deg \tau_p^{-1}[p]Z \geq \deg Z$. On obtient alors, grâce à l'inégalité (4.19) du lemme de zéros (théorème 4.21),

$$|\mathcal{Q}| \deg(Z) \leq \deg\left(\bigcup_{p \in \mathcal{P}_r(V)} \tau_p^{-1}[p]Z \right) \leq (LN_1 \cdots N_{r-1})^{\operatorname{codim} Z}.$$

Ainsi, en utilisant l'inégalité $\mathrm{codim} Z \leq r$, on obtient la majoration suivante pour le degré de Z :

$$\deg(Z)^{1/\mathrm{codim}(Z)} \leq L N_1 \cdots N_{r-1} |\mathcal{Q}|^{-1/r}.$$

En utilisant la relation (4.21) et la minoration (4.29) de $|\mathcal{Q}|$, on a

$$\begin{aligned}
\deg(Z)^{1/\mathrm{codim}(Z)} &\leq c_{15}\omega C_0^{2\delta n+1} \frac{(\log(3\omega))^{2n(\delta+1)}}{(\log\log(16\omega))^{2n}} \\
&\quad \times (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(r!-1)} \\
&\quad \times \frac{((\log C_0)\log\log(16\omega))^{1/r}}{(C_0\log(3\omega))^{2n(\delta+1)(\rho+1)r!}} \\
&\leq c_{15}\omega C_0^{-1} (\log C_0)\,(C_0\log(3\omega))^{-2n(\delta+1)\rho}\,.
\end{aligned}$$

Or il existe $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que τZ contienne $\{\boldsymbol{\alpha}^l\}_{\mathbb{L}}$. En appliquant le lemme 4.9 à $\mathbb{L}$, $\boldsymbol{\alpha}$ et τZ, on obtient

$$\omega_{\mathbb{L}}(\boldsymbol{\alpha}^l) \leq n \deg(\tau Z)^{1/\mathrm{codim}(\tau Z)} \leq \frac{\omega}{C_0^{1/2}(C_0\log(3\omega))^{2n(\delta+1)\rho}},$$

ce qui correspond à la deuxième assertion de la conclusion alternative du théorème. □

4.4. Descente

Nous fixons $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et $\mathbb{L}$ extension abélienne de $\mathbb{Q}$. Si nous pouvions assurer dans le théorème clé (théorème 4.24) que nous sommes dans la deuxième conclusion avec $l = 1$, le théorème 4.5 s'en déduirait immédiatement (même sans l'hypothèse $\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}}$). Plus généralement, si nous sommes dans la deuxième conclusion du 4.24, alors il existe un entier l n'appartenant pas à l'ensemble exceptionnel d'une certaine variété V tel que

$$\omega_{\mathbb{L}}(\boldsymbol{\alpha}^l) < \omega_{\mathbb{L}}(\boldsymbol{\alpha}).$$

Soient V_l une hypersurface $\mathbb{L}$-irréductible contenant $\boldsymbol{\alpha}^l$ telle que $\deg V_l = \omega_{\mathbb{L}}(\boldsymbol{\alpha}^l)$ et V_l' une composante $\mathbb{L}$-irréductible de $[l]^{-1}V_l$ contenant $\boldsymbol{\alpha}$. Alors

$$\begin{aligned}
\omega_{\mathbb{L}}(\boldsymbol{\alpha}) &\leq \deg V_l' \\
\text{et} \quad \deg([l]V_l') &= \deg V_l = \omega_{\mathbb{L}}(\boldsymbol{\alpha}^l).
\end{aligned}$$

Si nous pouvions assurer, *a priori*, que l n'est pas dans $E_{\mathrm{exc}}(V_l')$, le théorème 4.5 serait alors démontré dans la mesure où l'on aurait

$$\omega_{\mathbb{L}}(\boldsymbol{\alpha}) \leq \deg V_l' \leq \deg([l]V_l') \leq \omega_{\mathbb{L}}(\boldsymbol{\alpha}^l)$$

donc une contradiction. Malheureusement, cette condition est difficile à assurer car la variété V_l' est construite *après* la donnée de l.

Nous devons donc utiliser un argument de descente qui consiste à montrer, à l'aide d'un bon choix de paramètres, que l'on ne peut appliquer plus de n fois de suite le théorème 4.24 si la hauteur de $\boldsymbol{\alpha}$ est petite.

Nous commençons par introduire les paramètres suivants, pour $i \in [\![1, n]\!]$:

$$\begin{aligned}
\nu_i &= (1+n)(((n+1)!-1)(1+2n^2)+1)^{n-i};\\
P_i &= (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\nu_i nn!};\\
L_i &= (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\nu_i((n+1)!-1)};\\
\delta_i &= n\left(1+2n((n+1)!-1)\sum_{j=i+1}^{n}\nu_j\right);\\
E_i &= \left(\frac{C_0}{(\log C_0)^2}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))\right)^{\delta_i};\\
\varepsilon_i &= \frac{1}{C_0^{1/2}\left(C_0(\log C_0)^{-2}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))\right)^{2n((n+1)!-1)\sum_{j=i+1}^{n}\nu_j}}.
\end{aligned}$$

Remarquons que, pour tout $i \in [\![1, n]\!]$, un calcul simple donne

$$\nu_i = (\delta_i + 1) + ((n+1)!-1)\sum_{j=i+1}^{n}\nu_j. \tag{4.30}$$

En effet, en posant $\gamma = (((n+1)!-1)(1+2n^2)+1)$, on obtient

$$\begin{aligned}
&\nu_i - (\delta_i+1) - ((n+1)!-1)\sum_{j=i+1}^{n}\nu_j\\
&= \nu_i - n\left(1+2n((n+1)!-1)\sum_{j=i+1}^{n}\nu_j\right) - 1 - ((n+1)!-1)\sum_{j=i+1}^{n}\nu_j\\
&= \nu_i - n - 1 - \big(((n+1)!-1)(2n^2+1)\big)\sum_{j=i+1}^{n}\nu_j\\
&= (1+n)\left(\gamma^{n-i} - 1 - (\gamma-1)\sum_{j=i+1}^{n}\gamma^{n-j}\right)\\
&= 0.
\end{aligned}$$

Remarquons également les égalités suivantes que nous utiliserons plusieurs fois dans la suite :

$$L_1 \cdots L_k = (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n((n+1)!-1)\sum_{i=1}^{k}\nu_i} \tag{4.31}$$

et

$$L_{k+1} \cdots L_n = (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n((n+1)!-1)\sum_{i=k+1}^{n}\nu_i}. \tag{4.32}$$

Si nous appliquions plusieurs fois de suite le théorème 4.24, nous pourrions construire une suite de variétés possèdant des propriétés particulières, ce qui motive la définition suivante.

Définition 4.25. — On note $\mathcal{W}$ l'ensemble des quadruplets $(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L})$ où $k \in [\![0, n]\!]$, $\boldsymbol{l} = (l_1, \ldots, l_k)$ est un k-uplet d'entiers, $\boldsymbol{V} = (V_0, \ldots, V_k)$ est un $(k+1)$-uplet de sous-variétés propres de $\mathbb{G}_{\mathrm{m}}^n$ et $\boldsymbol{L} = (\mathbb{L}_0, \ldots, \mathbb{L}_k)$ est un $(k+1)$-uplet d'extensions abéliennes de $\mathbb{Q}$ tels que :

(a_0) $\mathbb{L}_0$ est un sous-corps de $\mathbb{L}$ tel que $\omega_{\mathbb{L}_0}(\boldsymbol{\alpha}) = \omega_{\mathbb{L}}(\boldsymbol{\alpha})$;

(b_0) V_0 est définie sur $\mathbb{L}_0$ et est $\mathbb{L}_0$-irréductible ;

(c_0) $\mathbb{L}_0$ est le plus petit sous-corps de $\mathbb{L}$ sur lequel V_0 est définie ;

(d_0) V_0 contient $\{\boldsymbol{\alpha}\}_{\mathbb{L}_0}$ et pour tout $K \subsetneq \mathbb{L}_0$ on a $\{\boldsymbol{\alpha}\}_K \not\subset V_0$;

(e_0) $\deg V_0 \leq (L_1 \cdots L_n \omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{\mathrm{codim} V_0}$;

puis pour tout i entre 1 et k :

1. Soit l'indice i est de type I :
   (a) l_i est un premier ramifié dans $\mathbb{L}_{i-1}$ tel que $e_{l_i}(\mathbb{L}_{i-1}) \geq E_i$;
   (b) $E_i \leq l_i \leq P_i$;
   (c) $l_i \notin E_{\mathrm{exc}}(V_{i-1})$;
   (d) V_i est définie sur $(\mathbb{L}_{i-1})_{(l_i)}$ et est $(\mathbb{L}_{i-1})_{(l_i)}$-irréductible ;
   (e) $\mathbb{L}_i$ est le plus petit sous-corps de $(\mathbb{L}_{i-1})_{(l_i)}$ sur lequel V_i est définie ;
   (f) V_i contient $\{\boldsymbol{\alpha}^{l_1 \cdots l_i}\}_{\mathbb{L}_i}$ et pour tout $K \subsetneq \mathbb{L}_i$ on a $\{\boldsymbol{\alpha}^{l_1 \cdots l_i}\}_K \not\subset V_i$;
   (g) $[l_i]V_{i-1} \subset V_i$;
   (h) $\deg V_i \leq \left(L_{i+1} \cdots L_n \omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1 \cdots l_i})\right)^{\mathrm{codim} V_i}$;
   (i) $\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1 \cdots l_i}) \leq c_0 \omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}) \log(3\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}))$.
2. Soit l'indice i est de type II :
   (a) l_i est un entier ;
   (b) $l_i \leq L_i$;

(c) $l_i \notin E_{\mathrm{exc}}(V_{i-1})$;

(d) V_i est définie sur $\mathbb{L}_{i-1}$ et est $\mathbb{L}_{i-1}$-irréductible ;

(e) $\mathbb{L}_i$ est le plus petit sous-corps de $\mathbb{L}_{i-1}$ sur lequel V_i est définie ;

(f) V_i contient $\{\boldsymbol{\alpha}^{l_1\cdots l_i}\}_{\mathbb{L}_i}$ et pour tout $K \subsetneq \mathbb{L}_i$ on a $\{\boldsymbol{\alpha}^{l_1\cdots l_i}\}_K \not\subset V_i$;

(g) $[l_i]V_{i-1} \subset V_i$;

(h) $\deg V_i \leq \left(L_{i+1}\cdots L_n \omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i})\right)^{\mathrm{codim} V_i}$;

(i) $\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i}) \leq \varepsilon_i \omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}})$.

Si un indice est à la fois de type I et II, nous dirons qu'il est de type II.

Si $(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L}) \in \mathcal{W}$, nous noterons r_{I} l'ensemble des indices de type I dans $(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L})$ et r_{II} l'ensemble des indices de type II (on a alors $|r_{\mathrm{I}}| + |r_{\mathrm{II}}| = k$).

Remarquons que cette définition implique en particulier que le n-uplet $\boldsymbol{L} = (\mathbb{L}_0, \ldots, \mathbb{L}_k)$ est en fait une tour descendante d'extensions abéliennes incluses dans $\mathbb{L}$:

$$\mathbb{L}_0 \supseteq \cdots \supseteq \mathbb{L}_k.$$

Dans la descente, nous appliquerons le théorème 4.24 à une certaine puissance $\boldsymbol{\alpha}^{l_1\cdots l_k}$ de $\boldsymbol{\alpha}$, issue d'un élément de $\mathcal{W}$. Pour vérifier les hypothèses du théorème 4.24, il nous faut des informations concernant l'indice d'obstruction de[(5)] $\boldsymbol{\alpha}^{l_1\cdots l_k}$. Or, le point $\boldsymbol{\alpha}^{l_1\cdots l_k}$ étant issu d'un élément de $\mathcal{W}$, nous pouvons comparer son indice d'obstruction à celui de $\boldsymbol{\alpha}$:

Lemme 4.26. — *Soit $(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L}) \in \mathcal{W}$. Alors, pour tout $j \in [\![0, k]\!]$, on a*

$$\omega_{\mathbb{L}_j}(\boldsymbol{\alpha}^{l_1\cdots l_j}) \leq c_{16}\omega_{\mathbb{L}}(\boldsymbol{\alpha})\left(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))\right)^{|r_{\mathrm{I}}\cap[\![1,j]\!]|} \tag{4.33}$$

et

$$\frac{1}{(\log C_0)^2}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})) \leq \log(3\omega_{\mathbb{L}_j}(\boldsymbol{\alpha}^{l_1\cdots l_j})) \leq c_{17}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})). \tag{4.34}$$

Démonstration. — L'inégalité (4.33) est immédiate, après avoir noté que pour tout $i \in [\![1, j]\!]$:

– si l'indice i est de type I alors

$$\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i}) \leq c_0\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}})\log(3\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}))\ ;$$

(5) Notons, à ce propos, qu'il y a une légère erreur dans **[AmDa99]** et **[AmDa04]** : les auteurs ne vérifient pas exactement les hypothèses de la proposition qui résume la transcendance (proposition 5.3 dans **[AmDa99]** et proposition 2.8 dans **[AmDa04]**) ; cependant, cela n'a pas de conséquence sur le résultat final, excepté au niveau de la constante $c(n)$. Voir les notes de bas de pages (6), (7) et (8) pour plus de précisions.

– si l'indice i est de type II alors

$$\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i}) \leq \varepsilon_i \omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) \leq \omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}).$$

On en déduit la deuxième inégalité de (4.34). De plus, comme $\mathbb{L}_j \subseteq \mathbb{L}_0$, on a

$$\omega_{\mathbb{L}}(\boldsymbol{\alpha}) = \omega_{\mathbb{L}_0}(\boldsymbol{\alpha}) \leq l_1 \cdots l_j \omega_{\mathbb{L}_0}(\boldsymbol{\alpha}^{l_1\cdots l_j}) \leq l_1 \cdots l_j \omega_{\mathbb{L}_j}(\boldsymbol{\alpha}^{l_1\cdots l_j})$$

et ainsi, par le choix des paramètres,

$$\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})) \leq c_{18}(\log C_0)\log(3\omega_{\mathbb{L}_j}(\boldsymbol{\alpha}^{l_1\cdots l_j})) \leq (\log C_0)^2 \log(3\omega_{\mathbb{L}_j}(\boldsymbol{\alpha}^{l_1\cdots l_j})).$$

□

Introduisons maintenant deux définitions :

Définition 4.27. — On note $\mathcal{W}_0$ le sous-ensemble de $\mathcal{W}$ défini de la façon suivante :

$$\mathcal{W}_0 = \{(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L}) \in \mathcal{W},\ \dim V_0 < \dim V_1 < \cdots < \dim V_k\}.$$

Définition 4.28. — On introduit un ordre total sur les suites finies d'entiers. Soient $(v) = (v_i)_{0\leq i\leq k}$ et $(v') = (v'_i)_{0\leq i\leq k'}$ deux telles suites. On pose $(v) \preceq (v')$ si $(v_i)_{0\leq i\leq \min(k,k')} < (v'_i)_{0\leq i\leq \min(k,k')}$ pour l'ordre lexicographique ou si $(v_i)_{0\leq i\leq \min(k,k')} = (v'_i)_{0\leq i\leq \min(k,k')}$ et $k \geq k'$.

La définition précédente permet de munir $\mathcal{W}$ d'un préordre total (relation réflexive, transitive et complète) en posant

$$(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L}) \preceq (k', \boldsymbol{l'}, \boldsymbol{V'}, \boldsymbol{L'}) \ \text{ si } \ (\dim V_i)_{0\leq i\leq k} \preceq (\dim V'_i)_{0\leq i\leq k'}. \tag{4.35}$$

Nous passons maintenant à la descente proprement dite : le théorème suivant permet de construire un élément de $\mathcal{W}$ qui n'est pas dans $\mathcal{W}_0$.

Théorème 4.29. — *Supposons qu'il n'existe pas de sous-variété de torsion B définie sur $\mathbb{L}$ contenant $\boldsymbol{\alpha}$ telle que*

(4.36)
$$\deg(B)^{1/\operatorname{codim}(B)} \leq \omega_{\mathbb{L}}(\boldsymbol{\alpha})\,(C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\cdot(n+1)!\sum_{j=1}^n \nu_j + n - 1}$$

et

$$h(\boldsymbol{\alpha}) < \omega_{\mathbb{L}}(\boldsymbol{\alpha})^{-1}\left((C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n((n+1)!-1)\sum_{j=1}^n \nu_j + 2n(\delta_1+1)-1}\right)^{-1}.$$

Alors il existe $(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L}) \in \mathcal{W} \setminus \mathcal{W}_0$.

Le schéma de la preuve est le suivant. Nous montrons dans un premier temps que l'ensemble $\mathcal{W}_0$ n'est pas vide et que l'on peut en extraire un élément minimal pour l'ordre introduit sur $\mathcal{W}$ (voir (4.35)). Puis à partir de cet élément, nous construisons une nouvelle suite de sous-variétés, à l'aide du théorème 4.24.

Nous montrons ensuite que cette suite de sous-variétés est en fait un élément de $\mathcal{W}$ qui est strictement inférieur (pour l'ordre (4.35)) à l'élément minimal initial. Nous en déduisons qu'il n'appartient pas à $\mathcal{W}_0$.

Démonstration. — Montrons tout d'abord que l'ensemble $\mathcal{W}_0$ n'est pas vide. Soit V_0 une hypersurface définie sur $\mathbb{L}$ contenant $\boldsymbol{\alpha}$ et de degré minimal $\omega_{\mathbb{L}}(\boldsymbol{\alpha})$. Soit $\mathbb{L}_0$ son corps de définition. Nous pouvons supposer, quitte à changer le couple $(V_0, \mathbb{L}_0)$, que pour tout sous-corps $K \subsetneq \mathbb{L}_0$, on a $\omega_K(\boldsymbol{\alpha}) > \omega_{\mathbb{L}}(\boldsymbol{\alpha})$. Alors le quadruplet $(0, \emptyset, V_0, \mathbb{L}_0)$ appartient à $\mathcal{W}_0$. En effet, les conditions (a_0), (b_0) et (c_0) sont vérifiées par construction. Supposons qu'il existe $K \subsetneq \mathbb{L}_0$ tel que $\{\boldsymbol{\alpha}\}_K \subset V_0$; soit $f \in \mathbb{L}_0[\boldsymbol{X}]$ une équation de V_0. Par le lemme 4.8, il existe un polynôme g non nul, à coefficients dans K, de degré inférieur ou égal à celui de f tel que $g(\boldsymbol{\alpha}) = 0$; donc $\omega_K(\boldsymbol{\alpha}) \leq \omega_{\mathbb{L}}(\boldsymbol{\alpha})$, contradiction. L'hypothèse (d_0) est donc vérifiée. Enfin l'hypothèse (e_0) est ici trivialement vérifiée. Donc $\mathcal{W}_0$ n'est pas vide.

Par ailleurs, l'ensemble des suites finies d'entiers compris entre 0 et $n-1$, de longueur au plus n et strictement croissantes (au sens usuel) est fini (de cardinal inférieur à $2^n - 1$). Ainsi, il existe un élément minimal $(k, \boldsymbol{l}, \boldsymbol{V}, \boldsymbol{L})$ dans $\mathcal{W}_0$ pour l'ordre introduit précédemment, c'est-à-dire satisfaisant

$$\forall (k', \boldsymbol{l'}, \boldsymbol{V'}, \boldsymbol{L'}) \in \mathcal{W}_0, \quad (\dim V_i)_{0 \leq i \leq k} \preceq (\dim V'_i)_{0 \leq i \leq k'}.$$

Nous allons appliquer le théorème 4.24 à $\boldsymbol{\alpha}^{l_1 \cdots l_k}$, à la sous-variété V_k et à $\mathbb{L}_k$ avec $\delta = \delta_{k+1}$ et ρ tel que $(\rho+1)(\delta+1) = \nu_{k+1}$. Remarquons que dans ce cas, le paramètre E qui apparaît dans ce théorème satisfait, grâce à l'inégalité (4.34),

$$\begin{aligned} E &\geq \left(C_0 \log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k}))\right)^{\delta} \\ &\geq \left(\frac{C_0}{(\log C_0)^2} \log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))\right)^{\delta_{k+1}} \\ &\geq E_{k+1}. \end{aligned} \tag{4.37}$$

Vérifions que les hypothèses du théorème 4.24 sont satisfaites. On a

$$h(\boldsymbol{\alpha}^{l_1 \cdots l_k}) = l_1 \cdots l_k h(\boldsymbol{\alpha})$$

et, par l'inégalité (4.33),

$$\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k}) \leq c_{16} \omega_{\mathbb{L}}(\boldsymbol{\alpha}) (\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{|r_{\mathrm{I}}|}.$$

Donc par l'hypothèse faite sur la hauteur de $\boldsymbol{\alpha}$,

$$\begin{aligned}
h(\boldsymbol{\alpha}^{l_1\cdots l_k})\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k}) &\leq l_1\cdots l_k h(\boldsymbol{\alpha})c_{16}\omega_{\mathbb{L}}(\boldsymbol{\alpha})(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{|r_{\mathrm{I}}|}\\
&\leq h(\boldsymbol{\alpha})\omega_{\mathbb{L}}(\boldsymbol{\alpha})\left(\prod_{i\in r_{\mathrm{I}}} l_i\,(c_{16}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))\right)\prod_{i\in r_{\mathrm{II}}} l_i\\
&\leq h(\boldsymbol{\alpha})\omega_{\mathbb{L}}(\boldsymbol{\alpha})\left(\prod_{i\in r_{\mathrm{I}}} P_i\,(c_{16}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))\right)\prod_{i\in r_{\mathrm{II}}} L_i\\
&\leq h(\boldsymbol{\alpha})\omega_{\mathbb{L}}(\boldsymbol{\alpha})\prod_{i=1}^{k} L_i\\
&\leq (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{-e}
\end{aligned}$$

avec

$$\begin{aligned}
e &= 2n((n+1)!-1)\sum_{j=1}^{n}\nu_j + 2n(\delta_1+1) - 1\\
&\qquad\qquad -2n((n+1)!-1)\sum_{j=1}^{k}\nu_j\\
&= 2n((n+1)!-1)\sum_{j=k+1}^{n}\nu_j + 2n(\delta_1+1) - 1\\
&\geq 2n((n+1)!-1)\nu_{k+1} + 2n(\delta_{k+1}+1) - 1\\
&\geq 2n((n+1)!-1)(\rho+1)(\delta_{k+1}+1) + 2n(\delta_{k+1}+1) - 1.
\end{aligned}$$

D'où[(6)], par l'inégalité (4.34),

$$h(\boldsymbol{\alpha}^{l_1\cdots l_k})\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k}) \leq (C_0\log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})))^{-e}.$$

De plus, il n'existe pas de sous-variété de torsion B définie sur $\mathbb{L}_k$ et contenant $\boldsymbol{\alpha}^{l_1\cdots l_k}$ qui satisfait la majoration (4.25). En effet, si tel était le cas, il existerait B', sous-variété de torsion, composante $\mathbb{L}_k$-irréductible de $[l_1\cdots l_k]^{-1}B$ contenant $\boldsymbol{\alpha}$ (en particulier B' serait définie sur $\mathbb{L}_0$). Mais dans ce cas, avec les

[(6)] C'est ici que s'est glissée l'erreur dans **[AmDa99]** (resp. **[AmDa04]**) : les auteurs ont une majoration en fonction de $\delta(\boldsymbol{\alpha})$ (resp. w_*) à la place de $\delta(\boldsymbol{\alpha}^{l_1\cdots l_k})$ (resp. $[K:\mathbb{Q}]w_K(\boldsymbol{\alpha}^{l_1\cdots l_k})$).

inégalités (4.33), (4.34) et (4.31), on aurait

$$\begin{aligned}
\deg(B')^{1/\mathrm{codim}(B')} &= \Big((l_1 \dots l_k)^{\mathrm{codim}(B)} \deg(B)\Big)^{1/\mathrm{codim}(B')} \\
&\leq L_1 \cdots L_k \deg(B)^{1/\mathrm{codim}(B)} \\
&\leq L_1 \cdots L_k \omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})(C_0 \log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})))^{2n\nu_{k+1}(n+1)!} \\
&\leq c_{16} L_1 \cdots L_k \omega_{\mathbb{L}}(\boldsymbol{\alpha})(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{n-1} \\
&\qquad \times (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\nu_{k+1}(n+1)!} \\
&\leq \omega_{\mathbb{L}}(\boldsymbol{\alpha})(C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\cdot(n+1)!\sum_{j=1}^{n}\nu_j + n - 1},
\end{aligned}$$

ce qui contredirait l'hypothèse (4.36).

Considérons la variété V_k. On a

$$\deg V_k \leq \Big(L_{k+1} \cdots L_n \omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})\Big)^{\mathrm{codim} V_k},$$

ce qui entraîne[7] par le choix des paramètres et l'inégalité (4.34)

$$\begin{aligned}
\log \deg V_k &\leq c_{19}(\log C_0)\log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})) \\
&\leq C_0 \log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})),
\end{aligned}$$

de sorte que toutes les hypothèses du théorème 4.24 sont maintenant vérifiées.

Dans les deux cas de sa conclusion alternative, ce théorème fournit un entier que l'on note l_{k+1}. Si nous sommes dans le premier cas (resp. deuxième cas) de la conclusion, nous notons Z une hypersurface définie sur $(\mathbb{L}_k)_{(l_{k+1})}$ (resp. $\mathbb{L}_k$) contenant $\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}$ de degré minimal : $\deg(Z) = \omega_{(\mathbb{L}_k)_{(l_{k+1})}}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}})$ (resp. $\deg Z = \omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}})$). On note $\mathbb{L}_{k+1}$ le plus petit sous-corps de $(\mathbb{L}_k)_{(l_{k+1})}$ (resp. $\mathbb{L}_k$) sur lequel Z est définie. Par définition, on a $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}\}_{\mathbb{L}_{k+1}} \subset Z$. Supposons maintenant qu'il existe $K \subsetneq \mathbb{L}_{k+1}$ tel que $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}\}_K \subset Z$; soit $f \in \mathbb{L}_{k+1}[\boldsymbol{X}]$ une équation de Z. Par le lemme 4.8, il existe un polynôme g non nul à coefficients dans K, de degré inférieur ou égal à celui de f et tel que $g(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) = 0$. Ainsi, quitte à remplacer Z par l'hypersurface définie par g et $\mathbb{L}_{k+1}$ par K, nous pouvons de plus supposer que si $K \subsetneq \mathbb{L}_{k+1}$ alors $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}\}_K \not\subset Z$.

[7] Même remarque que la note (6).

Nous allons maintenant montrer qu'il existe un entier $k' \in [\![0, k+1]\!]$ et une sous-variété $Z_{k'}$ définie sur $\mathbb{L}_{k'}$ et $\mathbb{L}_{k'}$-irréductible tels que :

1. $\deg(Z_{k'}) \leq l_{k'+1} \cdots l_{k+1} \omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \deg(V_{k'})$;
2. $[l_{k'}]V_{k'-1} \subset Z_{k'}$;
3. $\operatorname{codim}(Z_{k'}) = \operatorname{codim}(V_{k'}) + 1$;
4. $\mathbb{L}_{k'}$ est le corps de définition de $Z_{k'}$ (en d'autres termes $Z_{k'}$ n'est pas défini sur un sous-corps strict de $\mathbb{L}_{k'}$) ;
5. $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k'}}\}_{\mathbb{L}_{k'}} \subset Z_{k'}$ et si $K \subsetneq \mathbb{L}_{k'}$ alors $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k'}}\}_K \not\subset Z_{k'}$.

en posant les conventions $\operatorname{codim}(V_{k+1}) = 0$, $\deg(V_{k+1}) = 1$ et $V_{-1} = \{\boldsymbol{\alpha}\}_{\mathbb{L}_0}$.

Remarquons que cela impliquera notamment

$$(\dim(V_0), \ldots, \dim(V_{k'-1}), \dim(Z_{k'})) \prec (\dim(V_0), \ldots, \dim(V_k)). \tag{4.38}$$

Nous distinguons deux cas.

Supposons dans un premier temps qu'il existe $i \in [\![0, k]\!]$ tel que

$$[l_{i+1} \ldots l_{k+1}]V_i \not\subset Z.$$

Soit k' le plus petit entier vérifiant cette propriété. Considérons l'ensemble algébrique équidimensionnel $V_{k'} \cap [l_{k'+1} \ldots l_{k+1}]^{-1} Z$; la variété $V_{k'}$ et l'ensemble algébrique $[l_{k'+1} \ldots l_{k+1}]^{-1} Z$ étant définis respectivement sur $\mathbb{L}_{k'}$ et $\mathbb{L}_{k+1} \subset \mathbb{L}_{k'}$, leur intersection est elle aussi définie sur $\mathbb{L}_{k'}$. Soit $Z_{k'}$ une des composantes $\mathbb{L}_{k'}$-irréductibles de $V_{k'} \cap [l_{k'+1} \ldots l_{k+1}]^{-1} Z$ contenant $[l_{k'}]V_{k'-1}$. La propriété 1 est alors assurée par l'inégalité de Bézout :

$$\begin{aligned} \deg(Z_{k'}) &\leq \deg([l_{k'+1} \ldots l_{k+1}]^{-1} Z) \deg(V_{k'}) \\ &\leq l_{k'+1} \ldots l_{k+1} \omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \deg(V_{k'}). \end{aligned}$$

De plus on a $[l_{k'}]V_{k'-1} \subset V_{k'}$ par hypothèse et $[l_{k'}]V_{k'-1} \subset [l_{k'+1} \ldots l_{k+1}]^{-1} Z$ par minimalité de k', donc $[l_{k'}]V_{k'-1} \subset Z_{k'}$ (propriété 2). De plus, on a $\operatorname{codim}(Z_{k'}) = \operatorname{codim}(V_{k'}) + 1$ (propriété 3) par construction. Supposons maintenant que $Z_{k'}$ soit définie sur $K \subsetneq \mathbb{L}_{k'}$. Alors $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k'}}\}_K \subset Z_{k'}$ et par suite on avait nécessairement $\{\boldsymbol{\alpha}^{l_1 \cdots l_{k'}}\}_K \subset V_{k'}$, ce qui contredit l'hypothèse (f) dans la définition de $\mathcal{W}$. Donc $\mathbb{L}_{k'}$ est le corps de définition de $Z_{k'}$ (propriété 4). Enfin, la propriété 5 est assurée par le même argument.

Supposons dans un deuxième temps que $\forall i \in [\![0, k]\!]$, $[l_{i+1} \ldots l_{k+1}]V_i \subset Z$. Posons alors $k' = k+1$ et $Z_{k+1} = Z$. Les propriétés 1,2,3,4 et 5 sont alors trivialement vérifiées par la définition de Z_{k+1} et les remarques qui la suivent.

Nous allons maintenant montrer

$$(k', (l_1, \ldots, l_{k'}), (V_1, \ldots, V_{k'-1}, Z_{k'}), (\mathbb{L}_1, \ldots, \mathbb{L}_{k'})) \in \mathcal{W}$$

en distinguant 3 cas.

Cas 1. Si $k' = k+1$ et que nous sommes dans la conclusion 1 du théorème 4.24, nous allons montrer que $k+1$ est un indice de type I. En effet l_{k+1} est alors un premier ramifié dans $\mathbb{L}_k$ tel que $e_{l_{k+1}}(\mathbb{L}_k) \geq E_{k+1}$ (en utilisant (4.37)), ce qui assure la condition (a). De plus, $l_{k+1} \notin E_{\text{exc}}(V_k)$ et, en utilisant encore (4.34) et (4.37), on obtient

$$\begin{aligned} E_{k+1} \leq l_{k+1} &\leq (C_0 \log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})))^{2n(1+\delta)(\rho+1)n.n!} \\ &\leq (c_{17} C_0 \log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\nu_{k+1} n.n!} \\ &\leq P_{k+1}. \end{aligned}$$

Donc les conditions (b) et (c) sont satisfaites. De même, grâce à l'inégalité (4.26), la condition (i) est vérifiée :

$$\begin{aligned} \omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) &= \omega_{\mathbb{L}_{k(l_{k+1})}}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \\ &\leq c_0 \omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k}) \log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})). \end{aligned}$$

La variété Z_{k+1} est définie sur $\mathbb{L}_{k+1}$ (condition (d)) et vérifie les propriétés 2, 4 et 5 qui correspondent respectivement aux conditions (g), (e) et (f). Enfin, la condition (h) est assurée :

$$\deg(Z_{k+1}) = \omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}).$$

Donc l'indice $k+1$ est de type I et

$$(k+1, (l_1, \ldots, l_{k+1}), (V_1, \ldots, V_k, Z_{k+1}), (\mathbb{L}_1, \ldots, \mathbb{L}_{k+1})) \in \mathcal{W}.$$

Cas 2. Si $k' = k+1$ et que nous sommes dans la conclusion 2 du théorème 4.24, nous allons montrer que $k+1$ est un indice de type II. En effet, l_{k+1} est alors un entier tel que[8] (en utilisant (4.34)),

$$\begin{aligned} l_{k+1} &\leq (C_0 \log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1 \cdots l_k})))^{2n(1+\delta)(\rho+1)((n+1)!-1)} \\ &\leq (c_{17} C_0 \log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n\nu_{k+1}((n+1)!-1)} \\ &\leq L_{k+1} \end{aligned}$$

[8] Même remarque que la note (6).

et $l_{k+1} \notin E_{\mathrm{exc}}(V_k)$ de sorte que les conditions (a), (b) et (c) sont satisfaites. De même, à l'aide des inégalités (4.27) et (4.34), la condition (i) est vérifiée :

$$\begin{aligned}
\omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1\cdots l_{k+1}}) &= \omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_{k+1}}) \\
&\leq \frac{\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})}{C_0^{1/2}(C_0\log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})))^{2n(\delta_{k+1}+1)\rho}} \\
&\leq \frac{\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})}{C_0^{1/2}(C_0(\log C_0)^{-2}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n(\delta_{k+1}+1)\rho}} \\
&\leq \frac{\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})}{C_0^{1/2}(C_0(\log C_0)^{-2}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n((n+1)!-1)\sum_{j=k+2}^{n}\nu_j}} \\
&\leq \varepsilon_{k+1}\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k}).
\end{aligned}$$

En effet, grâce à l'égalité (4.30) on a

$$\begin{aligned}
((n+1)!-1)\sum_{j=k+2}^{n}\nu_j &= \nu_{k+1}-(\delta_{k+1}+1) \\
&= (\delta_{k+1}+1)\rho.
\end{aligned}$$

Enfin, les conditions (d), (e), (f), (g) et (h) sont assurées de la même façon que dans le cas précédent. Donc l'indice $k+1$ est de type II et

$$(k+1,(l_1,\dots,l_{k+1}),(V_1,\dots,V_k,Z_{k+1}),(\mathbb{L}_1,\dots,\mathbb{L}_{k+1}))\in\mathcal{W}.$$

Cas 3. Si $k'<k+1$, on vérifie aisément que, par hypothèse sur $(k,\boldsymbol{l},\boldsymbol{V},\boldsymbol{L})$ et grâce aux propriétés 2, 4 et 5 de $Z_{k'}$, nous sommes dans l'un des deux cas de la définition 4.25, sauf éventuellement pour les conditions (h). Posons $\theta=1$ si nous sommes dans la première conclusion du théorème 4.24 et $\theta=0$ sinon. On a alors

$$\omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1\cdots l_{k+1}})\leq\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})(c_0\log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})))^{\theta}.$$

Donc, en utilisant la relation sur le degré de $Z_{k'}$ (propriété 1) et l'inégalité (4.34)

$$\begin{aligned}
\deg(Z_{k'}) &\leq l_{k'+1}\dots l_{k+1}\omega_{\mathbb{L}_{k+1}}(\boldsymbol{\alpha}^{l_1\cdots l_{k+1}})\deg(V_{k'}) \\
&\leq l_{k'+1}\dots l_{k+1}\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})(c_0\log(3\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})))^{\theta}\deg(V_{k'}). \\
&\leq l_{k'+1}\dots l_{k+1}\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k})(c_0c_{17}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{\theta}\deg(V_{k'}).
\end{aligned}$$

De plus, par un argument similaire à celui de la démonstration du lemme 4.26, on montre

$$\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k}) \leq c_{20}\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})(\log(3\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})))^{|r_{\mathrm{I}}\cap[\![k'+1,k]\!]|}$$

et de nouveau avec l'inégalité (4.34)

$$\omega_{\mathbb{L}_k}(\boldsymbol{\alpha}^{l_1\cdots l_k}) \leq c_{21}\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{|r_{\mathrm{I}}\cap[\![k'+1,k]\!]|}.$$

D'où, en posant $A_{k'} = \deg(Z_{k'})\left(\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})\deg(V_{k'})\right)^{-1}$, on a

$$\begin{aligned}
A_{k'} &\leq c_{21}l_{k'+1}\dots l_{k+1}(\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{|r_{\mathrm{I}}\cap[\![k'+1,k]\!]|}(c_0c_{17}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{\theta} \\
&\leq l_{k+1}(c_0c_{17}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{\theta}\prod_{\substack{i=k'+1\\ i\in r_{\mathrm{I}}}}^{k} c_{21}l_i\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))\prod_{\substack{i=k'+1\\ i\in r_{\mathrm{II}}}}^{k} l_i \\
&\leq L_{k+1}\prod_{\substack{i=k'+1\\ i\in r_{\mathrm{I}}}}^{k} L_i\prod_{\substack{i=k'+1\\ i\in r_{\mathrm{II}}}}^{k} L_i \\
&\leq \prod_{i=k'+1}^{k+1} L_i.
\end{aligned}$$

Enfin, la relation sur la codimension de $Z_{k'}$ (propriété 3) et la majoration du degré de $V_{k'}$ (condition (h) de la définition 4.25) donnent

$$\begin{aligned}
\deg(Z_{k'}) &\leq L_{k'+1}\cdots L_{k+1}\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})\left(L_{k'+1}\cdots L_n\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})\right)^{\operatorname{codim}(V_{k'})} \\
&\leq \left(L_{k'+1}\cdots L_n\omega_{\mathbb{L}_{k'}}(\boldsymbol{\alpha}^{l_1\cdots l_{k'}})\right)^{\operatorname{codim}(Z_{k'})},
\end{aligned}$$

ce qui montre que la condition (h) est vérifiée. Nous avons donc montré de nouveau

$$(k',(l_1,\dots,l_{k'}),(V_1,\dots,V_{k'-1},Z_{k'}),(\mathbb{L}_1,\dots,\mathbb{L}_{k'}))\in\mathcal{W}.$$

Comme la suite des dimensions $(\dim(V_0),\dots,\dim(V_{k'-1}),\dim(Z_{k'}))$ est strictement inférieure à la suite $(\dim(V_0),\dots,\dim(V_k))$ (voir la remarque (4.38)) et comme cette dernière est minimale parmi les éléments de $\mathcal{W}_0$, on en déduit

$$(k',(l_1,\dots,l_{k'}),(V_1,\dots,V_{k'-1},Z_{k'}),(\mathbb{L}_1,\dots,\mathbb{L}_{k'}))\in\mathcal{W}\setminus\mathcal{W}_0,$$

ce qui achève la preuve du théorème.

□

4.5. Démonstration du théorème 4.5

Soient $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$ et $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\bar{\mathbb{Q}})$. On fait l'hypothèse suivante :

Hypothèse $(\tilde{\mathcal{H}}_{\boldsymbol{\alpha},\mathbb{L},C_0\log C_0})$: Soient H un sous-tore, l un entier, p un nombre premier ramifié dans $\mathbb{L}$ tels que

$$\begin{cases} (\deg H)^{1/\mathrm{codim} H} & \leq & \omega_{\mathbb{L}}(\boldsymbol{\alpha}) \\ & & \times (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n((n+1)!-1)\sum_{j=1}^{n}\nu_j+n-1}; \\ l & \leq & (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n((n+1)!-1)\sum_{j=1}^{n-1}\nu_j}; \\ p & \leq & (C_0(\log C_0)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})))^{2n^2\nu_1 n!}; \end{cases}$$

Si $\tilde{\boldsymbol{\alpha}}$ est un conjugué de $\boldsymbol{\alpha}$ tel que $((\tilde{\boldsymbol{\alpha}})\boldsymbol{\alpha}^{-1})^l \notin H$ alors $((\tilde{\boldsymbol{\alpha}})\boldsymbol{\alpha}^{-1})^{pl} \notin H$.

Sous $(\tilde{\mathcal{H}}_{\boldsymbol{\alpha},\mathbb{L},C_0\log C_0})$, nous allons montrer que si les hypothèses du théorème 4.29 sont satisfaites, nous aboutissons à une contradiction.

Appliquons donc le théorème 4.29 à $\boldsymbol{\alpha}$. Soient $(k,\boldsymbol{l},\boldsymbol{V},\boldsymbol{L}) \in \mathcal{W} \setminus \mathcal{W}_0$ et $i \in [\![1,k]\!]$ tel que V_i et V_{i-1} soient de même dimension. On a $[l_i]V_{i-1} \subset V_i$ avec $l_i \notin E_{\mathrm{exc}}(V_{i-1})$. Nous allons distinguer trois cas.

Par la proposition 4.7, si i est de type I et que V_{i-1} n'est pas une réunion de translatés de sous-tores, on a

$$\deg([l_i]V_{i-1}) \geq l_i \deg V_{i-1},$$

car $l_i \notin E_{\mathrm{exc}}(V_{i-1})$. Or $[l_i]V_{i-1} \subset V_i$ et ces deux variétés ont même dimension donc

$$\deg([l_i]V_{i-1}) \leq \deg(V_i).$$

Mais V_{i-1} contient $\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}$ d'où

$$\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) \leq n \deg(V_{i-1})^{1/\mathrm{codim}(V_{i-1})}.$$

En combinant ces inégalités avec celles de la définition 4.25 on obtient

$$\begin{aligned}
\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) &\leq n\left(l_i^{-1}\deg(V_i)\right)^{1/\mathrm{codim}(V_i)}\\
&\leq nE_i^{-1/n}L_{i+1}\cdots L_n\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i})\\
&\leq nE_i^{-1/n}L_{i+1}\cdots L_n\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}})\\
&\qquad\qquad\times c_0\log(3\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}))\\
&\leq c_0c_{17}nE_i^{-1/n}L_{i+1}\cdots L_n\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}})\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha})).
\end{aligned}$$

D'où

$$\begin{aligned}
1 &\leq c_0c_{17}n(C_0\log(3\omega))^{-\delta_i/n+2n((n+1)!-1)\sum_{j=i+1}^n\nu_j}\\
&\qquad\qquad\times(\log C_0)^{2\delta_i/n+2n((n+1)!-1)\sum_{j=i+1}^n\nu_j}\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))\\
&\leq c_0c_{17}n(C_0)^{-1}(\log C_0)^{2\delta_i/n+2n((n+1)!-1)\sum_{j=i+1}^n\nu_j}.
\end{aligned}$$

On aboutit alors à une contradiction.

Supposons maintenant que i est de type I et que V_{i-1} est une réunion de translatés de sous-tores ; écrivons

$$V_{i-1}=\bigcup_{\tau\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{L}_{i-1})}\tau\left(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}H\right)=\bigcup_{k=1}^r\boldsymbol{\alpha}_k^{l_1\cdots l_{i-1}}H,$$

où H est un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ et les $\boldsymbol{\alpha}_k$, $k\in[\![1,r]\!]$, sont des conjugués de $\boldsymbol{\alpha}$ au-dessus de $\mathbb{L}_{i-1}$ tels que $\boldsymbol{\alpha}_{k_1}^{l_1\cdots l_{i-1}}$ et $\boldsymbol{\alpha}_{k_2}^{l_1\cdots l_{i-1}}$ sont distincts modulo H dès que $k_1\neq k_2$ (en d'autres termes, $(\boldsymbol{\alpha}_{k_1}\boldsymbol{\alpha}_{k_2}^{-1})^{l_1\cdots l_{i-1}}\notin H$). Comme $l_i\notin E_{\mathrm{exc}}(V_{i-1})$, on a

$$\deg\left([l_i]V_{i-1}\right)\geq\deg V_{i-1}$$

qui est en fait une égalité ici car V_i est une réunion de translatés de sous-tores et

$$[l_i]V_{i-1}=\bigcup_{k=1}^r\boldsymbol{\alpha}_k^{l_1\cdots l_i}H,$$

où la réunion est disjointe (en particulier $[l_i]H=H$). De plus V_i étant définie sur $\mathbb{L}_i$ et V_{i-1} sur $\mathbb{L}_{i-1}$, on a $\sigma([l_i]V_{i-1})\subset V_i$ pour tout $\sigma\in\mathrm{Gal}(\mathbb{L}_{i-1}/\mathbb{L}_i)$.

Donc

$$\deg V_i \geq \deg\left(\bigcup_{\sigma\in\mathrm{Gal}(\mathbb{L}_{i-1}/\mathbb{L}_i)} \sigma([l_i]V_{i-1})\right).$$

Par ailleurs, pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}_{i-1}/\mathbb{L}_i) \setminus \{\mathrm{Id}\}$, les variétés $\sigma(V_{i-1})$ et V_{i-1} n'ont pas de composante (géométriquement irréductible) commune car $\mathbb{L}_{i-1}$ est le corps de définition de V_{i-1} (voir l'hypothèse (e) de la définition 4.25). Donc si on note

$$\sigma(V_{i-1}) = \bigcup_{k=1}^{r} \boldsymbol{\alpha}_{k,\sigma}^{l_1\cdots l_{i-1}} H,$$

on a $(\boldsymbol{\alpha}_{k_1,\sigma_1}\boldsymbol{\alpha}_{k_2,\sigma_2}^{-1})^{l_1\cdots l_{i-1}} \notin H$ dès que $(k_1,\sigma_1) \neq (k_2,\sigma_2)$. Les conditions (b) et (h) de la définition 4.25 nous placent alors dans le cadre de l'hypothèse $(\tilde{\mathcal{H}}_{\boldsymbol{\alpha},\mathbb{L},C_0\log C_0})$. Ainsi, nous avons

$$(\boldsymbol{\alpha}_{k_1,\sigma_1}\boldsymbol{\alpha}_{k_2,\sigma_2}^{-1})^{l_1\cdots l_i} \notin H \quad \text{dès que} \quad (k_1,\sigma_1) \neq (k_2,\sigma_2).$$

En d'autres termes : pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}_{i-1}/\mathbb{L}_i) \setminus \{\mathrm{Id}\}$, les variétés $\sigma([l_i]V_{i-1})$ et $[l_i]V_{i-1}$ n'ont pas de composante (géométriquement irréductible) commune. Ainsi, on a, avec (4.5),

$$\begin{aligned}\deg V_i &\geq [\mathbb{L}_{i-1}:\mathbb{L}_i]\deg([l_i]V_{i-1})\\ &\geq \min(e_{l_i}(\mathbb{L}_{i-1}), l_i)\deg(V_{i-1})\\ &\geq E_i \deg(V_{i-1}).\end{aligned}$$

Mais V_{i-1} contient $\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}$, d'où

$$\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) \leq n\deg(V_{i-1})^{1/\mathrm{codim}(V_{i-1})}.$$

En combinant ces inégalités avec celles de la définition 4.25 on obtient

$$\begin{aligned}\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) &\leq n\left(E_i^{-1}\deg(V_i)\right)^{1/\mathrm{codim}(V_i)}\\ &\leq nE_i^{-1/n}L_{i+1}\cdots L_n\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i})\end{aligned}$$

Comme dans le cas précédent, ceci constitue une contradiction.

Enfin, si i est de type II, on a

$$\deg([l_i]V_{i-1}) \geq \deg V_{i-1},$$

car $l_i \notin E_{\mathrm{exc}}(V_{i-1})$. Or $[l_i]V_{i-1} \subset V_i$ et ces deux variétés ont même dimension donc

$$\deg([l_i]V_{i-1}) \leq \deg(V_i).$$

Mais V_{i-1} contient $\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}$, d'où

$$\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) \leq n\deg(V_{i-1})^{1/\mathrm{codim}(V_{i-1})}.$$

En combinant ces inégalités avec celles de la définition 4.25 on obtient

$$\begin{aligned}\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}) &\leq n\left(\deg(V_i)\right)^{1/\mathrm{codim}(V_i)}\\ &\leq nL_{i+1}\cdots L_n\omega_{\mathbb{L}_i}(\boldsymbol{\alpha}^{l_1\cdots l_i})\\ &\leq nL_{i+1}\cdots L_n\varepsilon_i\omega_{\mathbb{L}_{i-1}}(\boldsymbol{\alpha}^{l_1\cdots l_{i-1}}).\end{aligned}$$

D'où

$$1 \leq n(\log C_0)^{6n((n+1)!-1)\sum_{j=i+1}^n \nu_j} C_0^{-1/2},$$

ce qui constitue une nouvelle contradiction.

Ainsi les hypothèses du théorème 4.29 ne sont jamais satisfaites (sous $(\tilde{\mathcal{H}}_{\boldsymbol{\alpha},\mathbb{L},C_0\log C_0})$). Nous avons donc montré le théorème suivant :

Théorème 4.30. — *Pour tout entier naturel n non nul, il existe un nombre réel strictement positif $\tilde{c}(n)$ ne dépendant que de n et effectivement calculable tel que la propriété suivante soit vraie. Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et soit $\mathbb{L}$ une extension abélienne de $\mathbb{Q}$. Supposons que l'hypothèse $(\tilde{\mathcal{H}}_{\boldsymbol{\alpha},\mathbb{L},\tilde{c}(n)})$ soit satisfaite. Si*

$$h(\boldsymbol{\alpha}) \leq \omega_{\mathbb{L}}(\boldsymbol{\alpha})^{-1}(\tilde{c}(n)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{-\tilde{\kappa}(n)},$$

alors il existe une sous-variété de torsion B contenant $\boldsymbol{\alpha}$ définie sur $\mathbb{L}$ telle que

$$(\deg B)^{1/\mathrm{codim}(B)} \leq \omega_{\mathbb{L}}(\boldsymbol{\alpha})(\tilde{c}(n)\log(3\omega_{\mathbb{L}}(\boldsymbol{\alpha}))^{\tilde{\mu}(n)},$$

avec

$$\begin{cases}\tilde{\kappa}(n) &= 2n((n+1)!-1)\displaystyle\sum_{j=1}^n \nu_j + 2n(\delta_1+1) - 1\ ;\\ \tilde{\mu}(n) &= 2n(n+1)!\displaystyle\sum_{j=1}^n \nu_j + n - 1.\end{cases}$$

D'une part, l'hypothèse $(\mathcal{H}_{\boldsymbol{\alpha},\mathbb{L}})$ implique l'hypothèse $(\tilde{\mathcal{H}}_{\boldsymbol{\alpha},\mathbb{L},\tilde{c}(n)})$. D'autre part, par (4.30),

$$\begin{aligned}
\tilde{\kappa}(n) &= 2n((n+1)!-1)\nu_1 + 2n\nu_1 - 1 \\
&= 2n(n+1)!(1+n)\left(((n+1)!-1)(1+2n^2)+1\right)^{n-1} - 1 \\
&\leq 2(n+1)^2(n+1)!\left((n+1)!2(n+1)^2\right)^{n-1} \\
&\leq \left(2(n+1)^2(n+1)!\right)^n
\end{aligned}$$

et

$$\begin{aligned}
\tilde{\mu}(n) &= 2n(n+1)!\sum_{j=1}^{n}\nu_j + n - 1 \\
&\leq 4n((n+1)!-1)\sum_{j=1}^{n}\nu_j \\
&\leq 2\left(2(n+1)^2(n+1)!\right)^n .
\end{aligned}$$

Ainsi, le théorème 4.5 est démontré.

BIBLIOGRAPHIE

[AmDa99] F. Amoroso & S. David – « Le problème de Lehmer en dimension supérieure », *J. Reine Angew. Math.* **513** (1999), p. 145–179.

[AmDa00] ———, « Minoration de la hauteur normalisée des hypersurfaces », *Acta Arithmetica* **92** (2000), no. 4, p. 339–366.

[AmDa01] ———, « Densité des points à coordonnées multiplicativement indépendantes », *The Ramanujan Journal* **5** (2001), p. 237–246.

[AmDa03] ———, « Minoration de la hauteur normalisée dans un tore », *Journal of the Inst. of Math. Jussieu* **2** (2003), no. 3, p. 335–381.

[AmDa04] ———, « Distribution des points de petite hauteur dans les groupes multiplicatifs », *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5)* **3** (2004), no. 2, p. 325–348.

[AmDe07] F. Amoroso & E. Delsinne – « Une minoration relative explicite pour la hauteur dans une extension d'une extension abélienne », *Diophantine Geometry* (U. Zannier, éd.), CRM, vol. 4, Scuola Norm. Sup. Pisa, 2007, p. 1–24.

[AmDv00] F. Amoroso & R. Dvornicich – « A lower bound for the height in abelian extensions », *Journal of Number Theory* **80** (2000), p. 260–272.

[Amo07] F. Amoroso – « Bogomolov revisited », Manuscrit, 2007.

[AmNu07] F. Amoroso & F. A. E. Nuccio – « Algebraic numbers of small Weil's height in CM-fields : on a theorem of Schinzel », *J. Number Theory* **122** (2007), no. 1, p. 247–260.

[AmZa00] F. AMOROSO & U. ZANNIER – « A relative Dobrowolski lower bound over abelian extensions », *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 3, p. 711–727.

[BG06] E. BOMBIERI & W. GUBLER – *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[CF67] J. W. S. CASSELS & A. FRÖHLICH – *Algebraic number theory, proceedings of an instructional conference organized by the London mathematical society*, Academic Press, London-New-York, 1967.

[Cha88] M. CHARDIN – « Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique », *Bull. Soc. Math. France* **117** (1988), p. 305–318.

[Del05] E. DELSINNE – « Problème de Lehmer relatif dans un tore : cas des hypersurfaces », Preprint disponible à `http ://arxiv.org/abs/math/0509196`, 2005.

[Dob79] E. DOBROWOLSKI – « On a question of Lehmer and the number of irreducible factors of a polynomial », *Acta Arith.* **34** (1979), p. 391–401.

[DP99] S. DAVID & P. PHILIPPON – « Minorations des hauteurs normalisées des sous-variétés des tores », *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **28** (1999), no. 3, p. 489–543.

[Fri80] J. B. FRIEDLANDER – « Estimates for prime ideals », *J. Number Theory* **12** (1980), no. 1, p. 101–105.

[Hin88] M. HINDRY – « Autour d'une conjecture de Serge Lang », *Invent. math.* **94** (1988), p. 575–603.

[Leh33] D. H. LEHMER – « Factorization of certain cyclotomic functions », *Ann. Math.* **34** (1933), no. 2, p. 461–479.

[LO77] J. C. LAGARIAS & A. M. ODLYZKO – « Effective versions of the Chebotarev density theorem », Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, p. 409–464.

[Mér99] C. MÉRAY – « Sur un déterminant dont celui de Vandermonde n'est qu'un cas particulier », *Revue de Mathématiques Spéciales* **9** (1899), p. 217–219.

[Phi86] P. PHILIPPON – « Lemmes de zéros dans les groupes algébriques commutatifs », *Bull. Soc. Math. France* **114** (1986), p. 355–383.

[Phi91] ———, « Sur des hauteurs alternatives I », *Math. Ann.* **289** (1991), p. 255–283.

[Phi94] ———, « Sur des hauteurs alternatives II », *Ann. Inst. Fourier (Grenoble)* **44** (1994), p. 1043–1065.

[Phi95] ———, « Sur des hauteurs alternatives III », *J. Math. Pures Appl.* **74** (1995), p. 345–365.

[Rat04] N. RATAZZI – « Minoration de la hauteur de Néron-Tate pour les points et les sous-variétés : variation sur le problème de Lehmer. », Thèse, Université de Paris 6, 2004.

[RT96] D. ROY & J. THUNDER – « An absolute Siegel's lemma », *J. Reine Angew. Math.* **476** (1996), p. 1–26.

[Sch73] A. SCHINZEL – « On the product of the conjugates outside the unit circle of an algebraic number », *Acta Arith.* **24** (1973), p. 385–399, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday. IV.

[Sch96] W. M. SCHMIDT – « Heights of points on subvarieties of $\mathbf{G}_m^n$ », *Number theory (Paris, 1993–1994)* (Cambridge), London Math. Soc. Lecture Note Ser., vol. 235, Cambridge Univ. Press, 1996, p. 157–187.

[Ser68] J. P. SERRE – *Corps locaux*, Hermann, 1968.

[Smy71] C. J. SMYTH – « On the product of the conjugates outside the unit circle of an algebraic integer », *Bull. London Math. Soc.* **3** (1971), p. 169–175.

[Zan01] U. ZANNIER – Communication personnelle, 2001.

[Zha92] S. ZHANG – « Positive line bundles on arithmetic surfaces », *Ann. of Math.* **136** (1992), p. 569–587.

[Zha95a] ———, « Positive line bundles on arithmetic varieties », *J. Amer. Math. Soc* **8** (1995), p. 187–221.

[Zha95b] ———, « Small points and adelic metrics », *J. Algebraic Geom.* **4** (1995), p. 281–300.

Titre : Autour du problème de Lehmer relatif dans un tore

Résumé de la thèse

Le problème de Lehmer consiste à minorer la hauteur de Weil d'un nombre algébrique en fonction de son degré sur $\mathbb{Q}$. Si la question originelle de Lehmer reste aujourd'hui sans réponse, la conjecture optimale correspondante a été démontrée à un epsilon près. Par ailleurs, ce problème admet plusieurs généralisations. D'une part, on peut formuler le même type de conjecture en remplaçant le corps des rationnels par une extension abélienne d'un corps de nombres. D'autre part, on peut généraliser ces énoncés en dimension supérieure. Il s'agit alors de minorer la hauteur normalisée d'un point ou d'une sous-variété d'un tore ; dans ce cas, on substitue au degré un invariant plus fin : l'indice d'obstruction. Il est ensuite naturel de chercher à combiner ces deux généralisations : c'est le problème de Lehmer relatif dans un tore.

Dans cette thèse, nous considérons tout d'abord le problème de Lehmer relatif unidimensionnel. Nous donnons une minoration pour la hauteur d'un nombre algébrique en fonction de son dégré sur une extension abélienne d'un corps de nombres. Il s'agit d'une amélioration d'un théorème d'Amoroso et Zannier, obtenue à l'aide d'une démonstration techniquement plus simple. De plus, nous explicitons la dépendance de la borne inférieure en le corps de base. Puis nous abordons le problème de Lehmer relatif en dimension supérieure et minorons la hauteur d'une hypersurface en fonction de son indice d'obstruction sur une extension abélienne de $\mathbb{Q}$. Enfin, nous obtenons un résultat analogue pour un point, sous réserve que celui-ci satisfasse une hypothèse technique. Nous montrons ainsi les conjectures les plus fines à un epsilon près.

Title : On the relative Lehmer problem

Thesis summary

Lehmer's problem consists in finding lower bounds for the Weil height of an algebraic number in terms of its degree over $\mathbb{Q}$. Even if there is still no answer to Lehmer's original question, the sharpest corresponding conjecture has been proved up to an epsilon. Besides, there are several generalizations of this problem. On one hand, one can formulate the same kind of conjecture replacing the field of rationals by an abelian extension of a number field. On the other hand, one can generalize these statements in higher dimension. The point is to find lower bounds for the normalized height of a point or a subvariety of a torus ; in this case, we substitute to the degree a more precise invariant : the obstruction index. It is then natural to try to combine these two generalizations : this is the relative Lehmer problem in a torus.

In this thesis, we first consider the one dimensional relative Lehmer problem. We give a lower bound for the height of an algebraic number in terms of its degree over an abelian extension of a number field. This is an improvement of a theorem of Amoroso and Zannier, obtained through a technically simpler proof. Furthermore, we precise the dependence of the lower bound on the ground field. Then, we focus on the relative Lehmer problem in higher dimension and find a lower bound for the normalized height of a hypersurface in terms of its obstruction index over an abelian extension of $\mathbb{Q}$. Finally, we obtain an analogous result for a point, provided a technical hypothesis is satisfied. Thus we show the sharpest conjectures up to an epsilon.

Discipline : Mathématiques et leurs applications

Mots clés :

-*indexation Rameau :* Nombres (théorie des) ; Approximation diophantienne ; Extensions abéliennes ; Géométrie algébrique arithmétique ; Tore (géométrie) ; Variétés (mathématiques).

-*indexation libre :* Hauteur, Problème de Lehmer.

Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139,
Université de Caen/Basse-Normandie BP 5186
14032 CAEN Cedex, FRANCE
delsinne@math.unicaen.fr