Une minoration relative explicite pour la hauteur dans une extension d'une extension abélienne

Francesco Amoroso & Emmanuel Delsinne *

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 montrer qu'il existe un 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 (*cf.* [Do]) 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 (*cf.* [Am-Dv]) que si α appartient 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 $\mathbb{K}$, *i. e.* le degré de α sur une extension abélienne de $\mathbb{K}$. Ils ont ainsi montré dans [Am-Za] un analogue du théorème de Dobrowolski dans le cas relatif :

Théorème 1.1 *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*

*Laboratoire de Mathématiques « N. Oresme », U.M.R. 6139 (C.N.R.S.), Université de Caen, Campus II, BP 5186, F–14032 Caen Cedex. e-mail: delsinne@math.unicaen.fr

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 :

$$h(\alpha) \geq \frac{c(\mathbb{K})}{D} \left(\frac{\log\log 5D}{\log 2D} \right)^{13} \tag{1.1}$$

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 $\ll \log \gg$, 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 Δ du corps $\mathbb{K}$. Si l'on a assume l'hypothèse de Riemann généralisée (GRH), un résultat de Odlyzko et Lagarias (*cf.* [La-Od], théorème 1.1) fournit une très bonne estimation de ce reste et permet de montrer le résultat suivant :

Théorème 1.2 *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 $\lambda = (\log|\Delta|)^2 \max((\log\log|\Delta|)^2, (\log d)^4)$. En particulier :

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

où $\delta = \log|\Delta|$.

Sans GRH, les estimations du reste dans le théorème des idéaux premiers sont nettement moins bonnes (voir nouveau [La-Od], théorèmes 1.3 et 1.4) et ne permettent pas de trouver une dépendance polynomiale en Δ. Nous utiliserons alors une estimation dû Friedlander (*cf.* [Fr]), qui donne une version moins précise du théorème des idéaux premiers, avec en contrepartie une meilleure dépendance en Δ.

Théorème 1.3 *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 :*

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

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 $\mathbb{K}_i/\mathbb{K}_{i-1}$ normale 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 suivante le montre. Soit $x > 1$ et soit $n = n(x)$ le produit de tout 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 $D = 1$. Alors :

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

La démonstration du théorème 1.1 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 « beaucoup » ramifiée dans l'extension abélienne $\mathbb{L}$ de $\mathbb{K}$ (tout ceci étant clairement quantifié l'aide de paramètres). Ici, nous traitons le cas de « grande ramification » part, en montrant qu'il ne peut y avoir de premier « beaucoup » 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 1.1 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 eut été possible d'utiliser les mmes 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 [Am-Za]. Puis nous montrons les résultats préliminaires qui nous servirons à minorer la hauteur de α dans la dernière partie.

2 Notations

Dans toute la suite nous fixons $\overline{\mathbb{Q}}$ 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. Δ) le degré (resp. le discriminant) de $\mathbb{K}$ sur $\mathbb{Q}$; rappelons qu'on a l'inégalité $\log|\Delta| \geq c_0 d$. 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, *i. e.* 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 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 $h(\alpha) \geq f(d, \Delta, D)$ où $D \mapsto f(d, \Delta, D)$ est décroissante. Par invariance de la hauteur de Weil par multiplication par des racines de l'unité, nous pouvons faire exactement les mmes hypothèses de minimalité et réductions que dans [Am-Za] (*cf.* (2.3),(2.4),...,(2.8) de *op. cit.*). Ainsi, nous pourrons utiliser le lemme 3.2 de [Am-Za] (*cf.* Proposition 3.1) 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 $\mathbb{L} \hookrightarrow \overline{\mathbb{Q}}$ 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

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

est de cardinal $D|S|$. Enfin nous désignerons par F la clotûre 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 P.

3 Résultats préliminaires

3.1 Congruences

Nous rappelons tout d'abord le lemme 3.2 de [Am-Za] :

Proposition 3.1 *Soit $P \in \mathcal{P}$. Il existe un sous-groupe H_P de G_P d'ordre*

$$|H_P| \geq \min\{e_P, p\}$$

tel que :

$$|\gamma^p - \sigma\gamma^p|_v \leq p^{-1} \tag{3.2}$$

pour tout entier $\gamma \in \mathbb{L}$, pour tout $\sigma \in H_P$ et pour tout valuation v de $\overline{\mathbb{Q}}$ au dessus de P.

De plus, soit $\sigma \in H_P \backslash \{\mathrm{Id}\}$ et soit τ un prolongement de σ $\mathbb{L}(\alpha)$. Alors, $\tau\alpha^p \neq \alpha^p$.

Nous aurons besoin du lemme d'approximation suivant :

Lemme 3.2 *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 :

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

D'après le théorème de [Ca–Fr], chapitre II, 15, page 67, il existe un élément $\beta \in k$ tel que

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

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 3.3 *Soit $\tau : \mathbb{L}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$. 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 3.2 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 $\overline{\mathbb{Q}}$ qui prolongent l'inclusion $\mathbb{L} \hookrightarrow \overline{\mathbb{Q}}$ 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 :

$$(bf(X))^p \equiv b^p g(X^p) \mod p\mathcal{O}_{\mathbb{L}}[X] \tag{3.3}$$

Examinons maintenant les différents cas.

Si $\tau_{|\mathbb{L}} \in H_P$, on a pour tout $\sigma \in H_P$, d'après la proposition 3.1 et le petit théorème de Fermat :

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

En combinant ceci avec la congruence (3.3) on obtient :

$$(b^\sigma)^p g^\sigma(X^p) \equiv (b^\tau)^p f^\tau(X)^p \mod P\mathcal{O}_F[X], \tag{3.4}$$

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 $\mathcal{O}_\mathbb{L}$ définit 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 (3.3), 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, avec la caractérisation de l'automorphisme de Frobenius et le petit théorème de Fermat :

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

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

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

et

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

□

3.2 Déterminant de Vandermonde généralisé

Pour montrer les théorèmes 1.2 et 1.3 nous utiliserons des déterminants de Vandermonde généralisés :

Lemme 3.4 *Soient $T_1, \dots, T_r$ des entiers positifs et $L = T_1 + \cdots + T_r$. Soit $\Delta((X_i, T_i)_{1 \leq i \leq r}) \in \mathbb{Z}[X_1, \dots, X_r]$ le déterminant de la matrice $L \times L$:*

$$M = (M_1 \ M_2 \ \dots \ M_r)$$

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

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

Alors

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

Démonstration. Voir [Me]

□

Lemme 3.5 *Soient $\gamma_1, \dots, \gamma_r$ des nombres algébriques, $T_1, \dots, T_r$ des entiers positifs et $\Delta := \Delta((\gamma_i, T_i)_{1 \leq i \leq r})$. Si k est un corps contenant $\gamma_1, \dots, \gamma_r$ et v une place de k, alors*

- *si v est archimédienne,*

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

- *si v est ultramétrique,*

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

où $L = T_1 + \cdots + T_r$.

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

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

Soit v est une place ultramétrique ; en utilisant le lemme 3.4 et l'inégalité

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

on obtient directement la deuxième majoration du lemme.

□

4 Preuve du théorème 1.2

Nous fixons deux paramètres :

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

où $C>0$ est une constante absolue que l'on supposera « assez grande » (en d'autres termes, les inégalités que nous serons amenés 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 la proposition 3.1 soit de cardinal supérieur 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 4.1 *On a les inégalités :*

$$\log N \geq \log\log(5D) \tag{4.5}$$

et

$$\frac{\log\log(5D)^2}{d^3\log(2D)}N \geq C^{5/2}\log(ND)^2 \ . \tag{4.6}$$

Démonstration. L'inégalité (4.5) est claire. Montrons (4.6) ; compte tenu du choix de N et de la majoration

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

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 4.2 *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 [La-Od] montre que :

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

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 $\leq x$. Soit P un idéal premier de $\mathcal{O}_{\mathbb{K}}$; si $e(P|p) > 1$, alors p divise Δ. Comme il y a au plus d premiers au-dessus de p, on a

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

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 $N \geq Cd^3$,

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

□

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

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

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 la proposition 3.1 est alors de cardinal supérieur 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 $\overline{\mathbb{Q}}$ 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 3.1

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

Lemme 4.3 *Soit v une place de F. Alors*

- *si $v|\infty$,*
$$|\Delta|_v \leq L^{L/2} \prod_{\tau\in\overline{S}} \max\{1, |\tau\alpha|_v\}^{p(L-1)},$$
- *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 3.5. Supposons que $v|P$. 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 3.4,

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

Fixons $\tau \in \overline{S}$; d'après la proposition 3.3, 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 Δ nous donne alors :

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

d'où

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

Or,

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

On en déduit :

$$h(\alpha) \geq \frac{\log(2D)}{2DNE} \geq \frac{c_3}{D}\min\left(\frac{\log\log(5D)^3}{d^4\log(2dD)^2\log(2D)}, \frac{\log\log(5D)}{\lambda d}\right) \ . \quad (4.7)$$

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 dans deux cas, suivant qu'une majorité de premiers est ramifiée ou non.

4.2.1 Une majorité est ramifiée

Soit $\Lambda_1 := \{P \in \Lambda \mid 2 \leq e_P \leq E\}$. Supposons dans un premier temps que :

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

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 2 $\not\equiv$ 2 distincts. Remarquons aussi que

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

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

Lemme 4.4 *Soit v une place de F. Alors*

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

Démonstration. Les deux premières inégalités sont encore données par le lemme 3.5. Soit $P \in \Lambda_1$ et supposons que $v|P$. 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 que $\tau_{|\mathbb{L}} = \sigma \in G_P \setminus \{\mathrm{Id}\}$, 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 3.3 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 :

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

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

$$\begin{aligned} &\frac{\log N}{2d} \sum_{P\in\Lambda_1} \sum_{\sigma\in G_P\setminus\{\mathrm{Id}\}} \frac{\lambda_\sigma}{e_P} \\ &\qquad\qquad \leq \left(\sum_{\sigma\in S} \lambda_\sigma^2\right) \log L + 2\left(\sum_{\sigma\in S} \lambda_\sigma\right)^2 Dh(\alpha) \ . \quad (4.8) \end{aligned}$$

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 (4.8) :

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\lambda_\sigma A_\sigma\Big)-c_4\log(ND)\le 2\Big(\sum_{\sigma\in S}\lambda_\sigma\Big)^2 Dh(\alpha) \tag{4.9}$$

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 :

$$\lambda_\sigma\le\frac{2C^2d^2\log(ND)\log(2D)}{N\log\log(5D)}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P} \tag{4.10}$$

valable pour $\sigma\neq\mathrm{Id}$ et les inégalités (4.5) et (4.6) du lemme 4.1, on a :

$$\begin{aligned}A_\sigma&\ge\left(\frac{\log N}{2d}-\frac{2c_4C^2d^2\log(ND)^2\log(2D)}{N\log\log(5D)}\right)\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\\&\ge\frac{\log N}{4d}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\,,\end{aligned}$$

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

$$A_\sigma\ge\frac{\log N}{4dE}\ge\frac{\log\log(5D)\log N}{8Cd^2\log(2D)}\,. \tag{4.11}$$

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

$$\frac{1}{2}|\Lambda_1|\le\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P}\le|\Lambda_1|\,. \tag{4.12}$$

En utilisant la minoration :

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

et (4.12) on obtient :

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

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

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

Ainsi, (4.11) donne :

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\lambda_\sigma A_\sigma\Big) - c_4\log(ND) \geq \log(ND)\ . \tag{4.13}$$

Enfin, en utilisant encore (4.10) et (4.12), on obtient :

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

$$\leq 1+\frac{2C^2d^2\log(ND)\log(2D)}{N\log\log(5D)}\times\frac{N}{\log N} \tag{4.14}$$

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

En injectant (4.13) et (4.14) dans (4.9) et en utilisant (4.5), on a alors :

$$h(\alpha) \geq \frac{c_5(\log N)^2\log\log(5D)^2}{Dd^4\log(ND)\log(2D)^2} \geq \frac{c_6\log\log(5D)^4}{Dd^4\log(2D)^3}\ . \tag{4.15}$$

4.2.2 Une majorité n'est pas ramifiée

Soit $\Lambda_2 := \{P\in\Lambda\ |e_P = 1\}$. Supposons maintenant que :

$$|\Lambda_2| \geq \frac{N}{4\log N}$$

Pour tout $P\in\Lambda_2$, on note Φ_P le morphisme de Frobenius associé P, *i. e.* 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 $\Sigma_p = \{\Phi_P^{-1}\ |\ P\in\Lambda_2, P|p\}$. Notons également $\tau_1,\dots,\tau_D$ les D plongements distincts de $\mathbb{L}(\alpha)$ dans $\overline{\mathbb{Q}}$ qui prolongent l'inclusion $\mathbb{L}\hookrightarrow\overline{\mathbb{Q}}$. Considérons le déterminant

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

où

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

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

$$\log L \leq c_7 \log(ND) \, .$$

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

Lemme 4.5 *Soit v une place de F. Alors*

- *si $v|\infty$,*

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

- *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 3.5. Soient $Q \in \Lambda_2$ et $\tau_{Q,1}, \ldots, \tau_{Q,D}$ les D prolongements de Φ_Q^{-1} $\mathbb{L}(\alpha)$. Si $v|Q$, on a :

$$|\Delta|_v{}^2 \leq A_1 A_2 A_3 A_4$$

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 3.3 :

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

Il suffit alors de multiplier ces 4 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 2 à 2 distincts. On peut donc appliquer à Δ la formule du produit ; le lemme précédent donne alors :

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

soit

$$\frac{T}{d} \sum_{P\in\Lambda_2} \log p \leq (T^2+|\Lambda_2|)\log L + 2(T+|\Lambda_2|)(T+\sum_{P\in\Lambda_2} p)Dh(\alpha). \quad (4.16)$$

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 (4.6),

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

et

$$\begin{aligned}(T+|\Lambda_2|)(T+\sum_{P\in\Lambda_2}p) &\le \left(T+\frac{N}{\log N}\right)\left(T+\frac{N^2}{\log N}\right)\\ &\le \frac{4N^3}{(\log N)^2}\,.\end{aligned}$$

Finalement, en utilisant (4.5),

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

et donc, par le choix de N,

$$h(\alpha)\ge \frac{c_{10}}{D}\min\left(\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2},\frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right) \tag{4.17}$$

4.3 Conclusion de la preuve du théorème 1.2

Les inégalités (4.7), (4.15) et (4.17) donnent :

$$\begin{aligned}h(\alpha)&\ge \frac{c_{11}}{D}\min\left(\frac{\log\log(5D)^3}{d^4\log(2dD)^2\log(2D)},\frac{\log\log(5D)}{d\lambda},\frac{\log\log(5D)^4}{d^4\log(2D)^3},\right.\\ &\qquad\left.\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2},\frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right)\\ &\ge \frac{c_{12}}{D}\left(\frac{\log\log(5D)^4}{d^5\log(2dD)^2\log(2D)^2},\frac{\log\log(5D)^2}{\lambda d^2\log(2D)}\right).\end{aligned}$$

5 Preuve du théorème 1.3

La preuve du théorème 1.3 est très similaire celle du 1.2. 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 $A = g(d)|\Delta|$. On a l'encadrement :

$$\log\log(5D) \leq \log N \leq c_{13} C A \log\log(5D) \; . \tag{5.18}$$

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 [Fr] déj cité dans l'introduction montre que

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

où ρ est une constante positive. D'où, en utilisant les mmes arguments que ceux du lemme 4.2,

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

Quitte 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 4.1 montre que s'il existe un premier $P \in \Lambda$ tel que $e_P \geq E$, alors :

$$h(\alpha) \geq \frac{\log(2D)}{2DNE} \geq \frac{A^{-c_{14}}}{D} \frac{\log\log(5D)^2}{\log(2D)^3} \; . \tag{5.19}$$

Supposons de maintenant que pour tout $P \in \Lambda$ on ait $e_P \leq E$. Soit, comme dans le sous paragraphe 4.2.1, $\Lambda_1 := \{P \in \Lambda \mid 2 \leq e_P \leq E\}$ 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 (4.9) :

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\lambda_\sigma A_\sigma\Big) - c_4\log(ND) \le 2\Big(\sum_{\sigma\in S}\lambda_\sigma\Big)^2 Dh(\alpha) \tag{5.20}$$

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 :

$$\lambda_\sigma \le \frac{2\log\log(5D)}{C^2Ad\log(2D)}\sum_{P\in\Lambda(\sigma)}\frac{1}{e_P} \tag{5.21}$$

valable pour $\sigma\neq\mathrm{Id}$, et l'encadrement (5.18), on a :

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

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

$$A_\sigma \ge \frac{\log\log(5D)^2}{8d^2\log(2D)}\ . \tag{5.22}$$

En utilisant la minoration :

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

l'inégalité (5.18) et la relation (4.12), on obtient :

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

Ainsi, (5.22) donne :

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

et, en utilisant (5.18),

$$\Big(\sum_{\sigma\in S\setminus\{\mathrm{Id}\}}\lambda_\sigma A_\sigma\Big) - c_4\log(ND) \geq \log(2D)\ . \tag{5.23}$$

Enfin, en utilisant encore (5.21), (4.12) et (5.18), on obtient :

$$\sum_{\sigma\in S}\lambda_\sigma \leq 1 + \frac{2\log\log(5D)}{\log(2D)} \times \frac{N}{(\log N)^2} \leq \frac{4A^C\log(2D)^2}{\log\log(5D)^2}\ . \tag{5.24}$$

En injectant (5.23) et (5.24) dans (4.9), on a alors :

$$h(\alpha) \geq \frac{A^{-c_{15}}\log\log(5D)^4}{D\log(2D)^3}\ . \tag{5.25}$$

Soit 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 4.2.2. Réécrivons, pour la commodité du lecteur, l'inégalité (4.16) :

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

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 :

$$h(\alpha) \geq \frac{A^{-c_{19}}\log\log(5D)^3}{\log(2D)^4}\ . \tag{5.26}$$

Le théorème 1.3 découle des inégalités (5.19), (5.25) et (5.26).

Références

[Am-Dv] F. Amoroso and R. Dvornicich – "A Lower Bound for the Height in Abelian Extensions." *J. Number Theory* **80** (2000), no 2, 260–272.

[Am-Za] F. Amoroso and U. Zannier – "A relative Dobrowolski's lower bound over abelian extensions." *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 3, 711–727.

[Ca–Fr] J. W. S. Cassels and A. Frlich. Algebraic number theory. Proceedings of an instructional conference organized by the London Mathematical Society, Academic Press, London–New-York, 1967.

[Do] E. Dobrowolski – "On a question of Lehmer and the number of irreducible factors of a polynomial", Acta Arith. **34** (1979), 391–401.

[Fr] J. B. Friedlander – "Estimates for Prime Ideals." *J. Number Theory* **12** (1980), 101–105.

[La-Od] J. C. Lagarias and A. M. Odlyzko – "Effective versions of the Čebotarev density theorem", Algebraic Number Fields, Durham Symposium, Academic Press, 1977.

[Me] C. Méray – "Sur un déterminant dont celui de Vandermonde n'est qu'un cas particulier", Revue de Mathématiques Spéciales, 9, (1899) p.217-219.