

quatrième série - tome 42 fascicule 6 novembre-décembre 2009

*ANNALES
SCIENTIFIQUES
de
L'ÉCOLE
NORMALE
SUPÉRIEURE*

Emmanuel DELSINNE

Le problème de Lehmer relatif en dimension supérieure

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

LE PROBLÈME DE LEHMER RELATIF EN DIMENSION SUPÉRIEURE

PAR EMMANUEL DELSINNE

RÉSUMÉ. – Nous généralisons en dimension supérieure un théorème d’Amoroso et Zannier concernant le problème de Lehmer relatif. Nous minorons la hauteur d’un point d’un tore en fonction de son indice d’obstruction sur \mathbb{Q}^{ab} , l’extension abélienne maximale de \mathbb{Q} , à condition qu’il ne soit pas contenu dans une sous-variété de torsion de petit degré. Nous en déduisons une minoration du minimum essentiel d’une sous-variété non contenue dans un sous-groupe algébrique propre en fonction de son indice d’obstruction sur \mathbb{Q}^{ab} . Nous montrons ainsi, à un epsilon près, les conjectures les plus fines qui peuvent être formulées dans ce cadre.

ABSTRACT. – We generalize in higher dimension a theorem of Amoroso and Zannier concerning the relative Lehmer problem. We obtain a lower bound for the height of a point in a torus in terms of its obstruction index over \mathbb{Q}^{ab} , the maximal abelian extension of \mathbb{Q} , provided that this point does not lie in a torsion subvariety of small degree. We deduce a lower bound for the essential minimum of a subvariety not contained in a proper algebraic subgroup in terms of its obstruction index over \mathbb{Q}^{ab} . We prove up to an epsilon the sharpest conjectures that can be formulated.

1. Introduction

Nous nous proposons dans cet article de poursuivre l’étude du problème de Lehmer dans un tore, amorcée par F. Amoroso et S. David dans [2] et [4]. Soit n un entier naturel non nul. Nous considérons le plongement « naturel » de \mathbb{G}_m^n dans \mathbb{P}^n . La hauteur (normalisée) d’un point $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ est donc la hauteur de Weil logarithmique $h(\alpha)$ du point projectif $(1 : \alpha_1 : \dots : \alpha_n)$. Cette hauteur est nulle si et seulement si α 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 $h(\alpha)$ si α n’est pas de torsion.

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

CONJECTURE 1.1. – *Il existe un nombre réel c strictement positif tel que, pour tout $\alpha \in \mathbb{G}_m(\overline{\mathbb{Q}})$ 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 [12] :

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

où c est un réel strictement positif. Par la suite, F. Amoroso et U. Zannier montrent dans [6] 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 $[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]$, où \mathbb{Q}^{ab} désigne l'extension abélienne maximale de \mathbb{Q} : c'est le problème de Lehmer « relatif ».

Par ailleurs, dans [2], 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 1.2. – Soient $\alpha \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$ et K un sous-corps de $\overline{\mathbb{Q}}$. On appelle *indice d'obstruction* de α relativement à K (ou sur K) et on note $\omega_K(\alpha)$ le plus petit degré ⁽¹⁾ d'une hypersurface de \mathbb{G}_m^n définie sur K contenant α .

La conjecture peut alors se formuler ainsi :

CONJECTURE 1.3. – *Soit n un entier naturel non nul. Il existe un nombre réel $c(n)$ tel que pour tout $\alpha \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$ à coordonnées multiplicativement indépendantes, on a*

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

La version « relative » de cette conjecture correspond à celle où l'on remplace $\omega_{\mathbb{Q}}(\alpha)$ par $\omega_{\mathbb{Q}^{\text{ab}}}(\alpha)$. Notons que l'on ne peut, dans cette conjecture, faire l'économie de l'hypothèse d'indépendance multiplicative des coordonnées de α : il suffit de considérer le point $\alpha_d = (2^{1/d}, \dots, 2^{1/d})$, $d \in \mathbb{N}^*$, dont la hauteur peut être arbitrairement petite et qui vérifie, dès que $n \geq 2$, $\omega_{\mathbb{Q}}(\alpha_d) = \omega_{\mathbb{Q}^{\text{ab}}}(\alpha_d) = 1$. Rappelons également que faire cette hypothèse équivaut à supposer que α n'appartient à aucune *sous-variété de torsion*, c'est-à-dire une réunion de translatés de sous-tors stricts par des points de torsion. Dans [2], F. Amoroso et S. David montrent l'analogue du résultat de E. Dobrowolski, puis dans [4], une version « semi-relative » :

THÉORÈME 1.4. – *Pour tout entier naturel n 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.*

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

Soient \mathbb{L} une extension cyclotomique de \mathbb{Q} et α un point de $\mathbb{G}_m^n(\bar{\mathbb{Q}})$. Si

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

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

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

Dans ce résultat, la dépendance en le corps \mathbb{L} n'est pas satisfaisante car le degré $[\mathbb{L} : \mathbb{Q}]$ peut être pathologiquement grand par rapport à $\omega_{\mathbb{L}}(\alpha)$ (en particulier lorsque $[\mathbb{L} : \mathbb{Q}]$ n'est pas polynomial en $\omega_{\mathbb{L}}(\alpha)$). Nous montrons ici que l'on peut se défaire de cette dépendance. Avant d'énoncer les résultats principaux, nous posons, pour tout $n \in \mathbb{N}^*$,

$$\begin{aligned} \kappa_1(n) &= 3(2(n+1)^2(n+1)!)^n, \quad \kappa_2(n) = n\kappa_1(n), \\ \eta_1(n) &= (n-1)! \left(\sum_{i=0}^{n-3} \frac{1}{i!} + 1 \right), \quad \eta_2(n) = \eta_1(n) + n - 1 \end{aligned}$$

et

$$\mu(n) = 8n!(2(n+1)^2(n+1)!)^n.$$

THÉORÈME 1.5. – *Pour tout entier naturel n non nul, il existe un réel strictement positif $c_1(n)$ ne dépendant que de n et effectivement calculable tel que la propriété suivante soit vraie. Soit $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$. Si*

$$h(\alpha) \leq \left(c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(\alpha)(\log(3\omega_{\mathbb{Q}^{\text{ab}}}(\alpha)))^{\kappa_1(n)} \right)^{-1}$$

alors α est contenu dans une sous-variété de torsion B telle que

$$(\deg B)^{1/\text{codim}(B)} \leq c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(\alpha)^{\eta_1(n)}(\log(3\omega_{\mathbb{Q}^{\text{ab}}}(\alpha)))^{\mu(n)}.$$

Il semble raisonnable de conjecturer que l'on peut obtenir le même résultat en remplaçant $\eta_1(n)$ par 1, quel que soit n (ici, $\eta_1(n)$ est majoré par $4(n-1)!$ et on a $\eta_1(1) = \eta_2(1) = 1$). Malheureusement, le schéma de la preuve que nous utilisons (une récurrence sur n) ne nous permet pas d'obtenir un tel exposant.

Par un simple argument d'algèbre linéaire, on montre que pour tout sous-corps K de $\bar{\mathbb{Q}}$ on a l'inégalité

$$\omega_K(\alpha) \leq n[K(\alpha) : K]^{1/n}.$$

Par conséquent, il devient possible d'obtenir une forme « faible » du théorème 1.5 (comme corollaire immédiat de celui-ci) en remplaçant l'indice d'obstruction par une racine n -ième du degré. On peut en fait en déduire un résultat plus précis concernant le produit des hauteurs des coordonnées de α en fonction du degré :

THÉORÈME 1.6. – *Pour tout entier naturel n non nul, il existe un réel strictement positif $c_2(n)$ ne dépendant que de n et effectivement calculable tel que la propriété suivante soit vraie. Soit $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$. Si*

$$\prod_{i=1}^n h(\alpha_i) \leq \left(c_2(n)[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}](\log(3[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]))^{\kappa_2(n)} \right)^{-1}$$

alors α est contenu dans une sous-variété de torsion B telle que

$$(\deg B)^{1/\text{codim}(B)} \leq c_2(n)[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]^{\eta_2(n)}(\log(3[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]))^{\mu(n)}.$$

Comme le signale le rapporteur de l'article, en effectuant en détail les calculs dans les démonstrations, le lecteur est quasiment amené à calculer les valeurs des constantes $c_1(n)$ et $c_2(n)$. Nous regroupons en annexe des valeurs indicatives pour les constantes utilisées au cours du texte et celles-ci nous permettent d'affirmer que l'on peut prendre

$$c_1(n) = \exp\left(64nn! \left(2(n+1)^2(n+1)!\right)^{2n}\right) \text{ et } c_2(n) = (2n^2)^n \exp\left(64n^2n! \left(2(n+1)^2(n+1)!\right)^{2n}\right).$$

Enfin, nous pouvons déduire du théorème 1.5 un résultat concernant le *minimum essentiel* $\hat{\mu}^{\text{ess}}(V)$ d'une sous-variété V , défini comme étant la borne inférieure des réels $\theta > 0$ tels que l'ensemble des points de V de hauteur majorée par θ est Zariski dense dans V . Nous obtenons ainsi :

COROLLAIRE 1.7. – *Soit V une sous-variété de \mathbb{G}_m^n qui n'est contenue dans aucun sous-groupe algébrique propre de \mathbb{G}_m^n . Alors*

$$\hat{\mu}^{\text{ess}}(V) \geq \left(c_3(n)\omega_{\mathbb{Q}^{\text{ab}}}(V)(\log(3\omega_{\mathbb{Q}^{\text{ab}}}(V)))^{\kappa_1(n)}\right)^{-1}$$

où $c_3(n) = c_1(n)(\dim(V) + 1)$.

Ce corollaire généralise le théorème principal de [11], où un tel résultat est démontré pour les sous-variétés de codimension 1.

REMARQUE 1.8. – Il est possible d'énoncer les mêmes résultats que précédemment en remplaçant \mathbb{Q}^{ab} par K^{ab} où K^{ab} désigne l'extension abélienne maximale d'un corps de nombres K quelconque. Dans ce cas, les constantes dépendent alors de n et de K . Il suffit pour cela de procéder à la manière de [6], en substituant à l'ensemble des nombres premiers un ensemble d'idéaux premiers (voir le début du paragraphe 2 de [6]). Afin de ne pas alourdir les notations, nous démontrons les résultats pour \mathbb{Q}^{ab} , mais les démonstrations sont exactement les mêmes dans le cas de K^{ab} .

Le plan de cet article 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 1.5, dont le schéma s'inspire naturellement de celle du théorème 1.4 (schéma classique d'une preuve de transcendance), avec cependant des différences notoires. À la différence de [4], nous devons prendre en compte les premiers qui sont ramifiés dans l'extension abélienne \mathbb{L} , ce qui nous oblige à effectuer une dichotomie entre les premiers « peu » et « très » ramifiés, à la manière de [6]. Pour les premiers peu ramifiés, la transcendance est semblable à celle de [4], mis à part le fait que nous devons 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 [5] et de [1] 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 α est petite (en fonction de $\omega_{\mathbb{L}}(\alpha)$), il existe soit un multiple α^l de α pour lequel l'indice d'obstruction $\omega_{\mathbb{L}}(\alpha^l)$ sur \mathbb{L} est pathologiquement petit, soit un multiple $\alpha^{l'}$ de α pour lequel l'indice d'obstruction $\omega_{\mathbb{L}(U)}(\alpha^{l'})$ sur un sous-corps strict $\mathbb{L}(U)$ de \mathbb{L} est du même ordre de grandeur que $\omega_{\mathbb{L}}(\alpha)$. Comme dans [2] et [4], cette proposition ne suffit pas pour conclure ; il nous faut utiliser un argument de descente, que cette dichotomie rend particulièrement technique (paragraphe 4). Enfin, dans le paragraphe 5, nous démontrons le

théorème 1.5 en procédant par récurrence sur n , la dimension du tore ambiant, et en déduisons les théorème 1.6 et corollaire 1.7. De plus, nous donnons en annexe des valeurs (non nécessairement optimales) pour toutes les constantes rencontrées dans le texte, desquelles nous déduisons les valeurs citées précédemment pour $c_1(n)$ et $c_2(n)$.

Remerciements. – Je remercie Francesco Amoroso pour m’avoir suggéré ce problème, ainsi que pour les nombreux conseils qu’il m’a prodigués tout au long de l’avancée de mes recherches. Je tiens également à remercier chaleureusement Gaël Rémond pour l’intérêt qu’il a porté à mon travail et pour ses indications qui ont contribué à finaliser celui-ci. Enfin, je souhaite exprimer ma gratitude envers le rapporteur anonyme pour sa relecture minutieuse de l’article, qui a permis de clarifier et de préciser certains points de ce texte.

2. Notations et préliminaires

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

2.1. Géométrie

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

$$\iota : \mathbb{G}_m^n \hookrightarrow \mathbb{P}^n \\ \alpha = (\alpha_1, \dots, \alpha_n) \mapsto (1 : \alpha_1 : \dots : \alpha_n).$$

Ainsi, les sous-ensembles algébriques de \mathbb{G}_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 $\text{Gal}(\bar{\mathbb{Q}}/K)$. 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 2.1. – Soient $Z \subset \mathbb{G}_m^n$ 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}_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 :

$$Z_K = \bigcup_{\sigma \in \text{Gal}(\bar{\mathbb{Q}}/K)} \sigma Z.$$

Il est clair que $\omega_K(Z) = \omega_K(Z_K)$.

Si Z est un ensemble algébrique de \mathbb{G}_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 $\lambda \in \mathbb{N}^n$, nous noterons ∂_λ l’opérateur différentiel

$$\partial_\lambda = \frac{1}{\lambda!} \left(\frac{\partial^{\lambda_1}}{\partial X_1^{\lambda_1}} \right) \circ \dots \circ \left(\frac{\partial^{\lambda_n}}{\partial X_n^{\lambda_n}} \right),$$

où $\lambda! = \lambda_1! \cdots \lambda_n!$. On dit que $P \in \bar{\mathbb{Q}}[\mathbf{X}]$ s'annule avec *multiplicité* T sur Z si $\partial_\lambda(P)$ est identiquement nul sur Z pour tout λ tel que $|\lambda| \leq T - 1$.

Soient L et T deux entiers naturels non nuls. Nous désignerons par $\mathcal{E}_K(Z, T, L)$ le sous-espace vectoriel de $K[\mathbf{X}]$ 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

$$H_K(Z, T, L) = \binom{L+n}{n} - \dim_K(\mathcal{E}_K(Z, T, L))$$

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}_m^n défini par

$$G_V = \{\mathbf{x} \in \mathbb{G}_m^n, \mathbf{x}V = V\} = \bigcap_{\mathbf{x} \in V} \mathbf{x}^{-1}V,$$

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

$$(2.1) \quad \dim(G_V) \leq \dim(V) ;$$

– si V est géométriquement irréductible, alors

$$(2.2) \quad V \text{ est un translaté de sous-tore } \iff \dim(G_V) = \dim(V).$$

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 :

$$E_{\text{exc}}(V) = \{l \in \mathbb{Z}, \exists \tau \in \text{Gal}(\bar{\mathbb{Q}}/K), W \neq \tau W \text{ et } [l]W = \tau[l]W\} \\ \cup \{l \in \mathbb{Z}, l \text{ n'est pas premier à } |G_W/G_W^0|\}.$$

Étant donné que le groupe de Galois $\text{Gal}(\bar{\mathbb{Q}}/K)$ 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 2.2. – *Soient V une sous-variété de \mathbb{G}_m^n et l, l' deux entiers.*

1. *Si $l \notin E_{\text{exc}}(V)$ alors on a*

$$\deg([l]V) \geq \deg(V).$$

2. Si $l \notin E_{\text{exc}}(V)$ et V n'est pas une réunion de translatés de sous-tores alors on a

$$\deg([l]V) \geq l \deg(V).$$

3. Si $l \notin E_{\text{exc}}(V)$ et $l' \notin E_{\text{exc}}([l]V)$ alors $ll' \notin E_{\text{exc}}(V)$.

4. Nous disposons de la majoration

$$|E_{\text{exc}}(V) \cap \{p \text{ premier}\}| \leq \frac{\dim V + 1}{\log 2} \log \deg(V).$$

Démonstration. – Il est clair que, par la définition de $E_{\text{exc}}(V)$, si $l \notin E_{\text{exc}}(V)$ 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 [13], 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 G_m^n/G_W^0 . Or, si $l \notin E_{\text{exc}}(V)$ 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 (2.1) et (2.2).

Si $l \notin E_{\text{exc}}(V)$ et $l' \notin E_{\text{exc}}([l]V)$, alors pour tout $\tau \in \text{Gal}(\bar{\mathbb{Q}}/K)$ tel que $W \neq \tau W$, on a $[l]W \neq \tau[l]W$ et ainsi $[l']([l]W) \neq \tau[l']([l]W)$ car $[l]W$ est une composante géométriquement irréductible de $[l]V$, dont le corps de définition est un sous-corps du corps de définition K de V . De plus, on a toujours $G_{[l]W} = [l]G_W \subset G_W$, $G_{[l]W}^0 = ([l]G_W)^0 = G_W^0$ et donc $(G_{[l]W}/G_{[l]W}^0) = ([l]G_W/G_W^0)$. Comme l est premier à $|G_W/G_W^0|$, on a $(G_W/G_W^0) = ([l]G_W/G_W^0)$ et ainsi l' est premier à $|G_W/G_W^0|$, donc le produit ll' l'est également et $ll' \notin E_{\text{exc}}(V)$.

Enfin, il y a au plus $\log(|G_W/G_W^0|)/\log 2$ nombres premiers qui divisent $|G_W/G_W^0|$ et l'on a

$$|G_W/G_W^0| \leq \deg(G_W) \leq \deg(W)^{\dim(W)+1}$$

où la dernière égalité est obtenue à l'aide du théorème de Bézout (voir [2] page 152). De plus, le lemme 2.3 (ii) de [2] (où l'on remplace \mathbb{Q} par le corps de définition de V) implique que l'ensemble des nombres premiers p tels qu'il existe $\tau \in \text{Gal}(\bar{\mathbb{Q}}/K)$ tel que $W \neq \tau W$ et $[p]W = \tau[p]W$ est de cardinal au plus $\log k / \log 2$ où k est le nombre de composantes géométriquement irréductibles de V . Ainsi on dispose de la majoration

$$|E_{\text{exc}}(V) \cap \{p \text{ premier}\}| \leq \frac{\dim W + 1}{\log 2} \log \deg(W) + \frac{\log k}{\log 2} \leq \frac{\dim V + 1}{\log 2} \log \deg(V)$$

car $\deg(V) = k \deg(W)$. □

Voici maintenant deux lemmes concernant les indices d'obstruction d'une variété.

LEMME 2.3. – Soient K un sous-corps de $\bar{\mathbb{Q}}$ et Z un ensemble algébrique. On a l'équivalence :

$$\mathcal{E}_{\bar{\mathbb{Q}}}(Z_K, T, L) = \{0\} \iff \mathcal{E}_K(Z_K, T, L) = \{0\}.$$

En particulier $\omega_K(Z) = \omega_{\bar{\mathbb{Q}}}(Z_K)$.

Démonstration. – L'implication directe est triviale, montrons la réciproque. Soit $f \in \mathcal{E}_{\mathbb{Q}}(Z_K, T, L)$ non 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 $\sigma \in \text{Gal}(\mathbb{F}/K)$. Donc le polynôme

$$g = \sum_{\sigma \in \text{Gal}(\mathbb{F}/K)} f^\sigma$$

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 $g \in \mathcal{E}_K(Z_K, T, L)$ et $\mathcal{E}_K(Z_K, T, L) \neq \{0\}$.

Remarquons que, pour tout corps $K' \subseteq \mathbb{Q}$, on a $L < \omega_{K'}(Z_K) \Leftrightarrow \mathcal{E}_{K'}(Z_K, 1, L) = \{0\}$. On en déduit $\omega_K(Z_K) = \omega_{\mathbb{Q}}(Z_K)$ et, comme $\omega_K(Z) = \omega_K(Z_K)$, on a $\omega_K(Z) = \omega_{\mathbb{Q}}(Z_K)$. \square

LEMME 2.4. – Soient K un sous-corps de \mathbb{Q} , W un ensemble algébrique et Z une variété de \mathbb{G}_m^n . On suppose que Z contient tous les conjugués de W au-dessus de K . Alors

$$\omega_K(W) \leq n(\deg Z)^{1/\text{codim}Z}.$$

Démonstration. – Par hypothèse Z contient W_K donc $\omega_{\mathbb{Q}}(W_K) \leq \omega_{\mathbb{Q}}(Z)$; le lemme 2.3 implique donc $\omega_K(W) \leq \omega_{\mathbb{Q}}(Z)$. Or par un résultat de M. Chardin (voir le corollaire 2 du chapitre 1 et l'exemple 1 de [9]), on a $\omega_{\mathbb{Q}}(Z) \leq n(\deg Z)^{1/\text{codim}Z}$. \square

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}_m^n . Si V est une sous-variété de \mathbb{G}_m^n , nous noterons

$$\ker[p] \cdot V = \bigcup_{\zeta \in \ker[p]} \zeta V.$$

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 $\phi_p \in \text{Gal}(\mathbb{L}/\mathbb{Q})$ le morphisme de Frobenius défini dans le lemme suivant :

LEMME 2.5. – 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 $\text{Gal}(\mathbb{L}/\mathbb{Q})$ tel que pour tout entier algébrique $\gamma \in \mathbb{L}$, on a

$$(2.3) \quad \phi_p \gamma \equiv \gamma^p \pmod{\pi_1 \cdots \pi_r}.$$

Démonstration. – Voir le lemme 3.1 de [6]. \square

Par abus de notation, nous poserons $\phi_1 = \text{Id}$ 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

$$(2.4) \quad [\mathbb{L} : \mathbb{L}_{(p)}] \geq \min(p, e_p(\mathbb{L})).$$

Par ailleurs nous avons la congruence suivante :

LEMME 2.6. – Soient \mathbb{L} une extension abélienne et p un nombre premier ramifié dans \mathbb{L} . Alors pour tout $\sigma \in \text{Gal}(\mathbb{L}/\mathbb{L}_{(p)})$ et tout $\gamma \in \mathcal{O}_{\mathbb{L}}$ on a

$$(2.5) \quad \sigma\gamma \equiv \gamma \pmod{\sqrt[p]{p}\mathcal{O}_{\mathbb{L}}}.$$

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, on a $\mathbb{L}_{(p)} = \mathbb{Q}(\zeta_{m/p}) \cap \mathbb{L}$, donc tout $\sigma \in \text{Gal}(\mathbb{L}/\mathbb{L}_{(p)})$ est la restriction à \mathbb{L} d'un élément $\tilde{\sigma}$ de $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p}))$. Ainsi, par le petit théorème de Fermat,

$$\sigma\gamma^p = \tilde{\sigma}\gamma^p = \tilde{\sigma}(P(\zeta_m))^p \equiv P(\tilde{\sigma}\zeta_m^p) = P(\zeta_m^p) \equiv (P(\zeta_m))^p = \gamma^p \pmod{p\mathbb{Z}[\zeta_m]}$$

et finalement

$$\sigma\gamma \equiv \gamma \pmod{\sqrt[p]{p}\mathcal{O}_{\mathbb{L}}}. \quad \square$$

Nous utiliserons à plusieurs reprises le lemme d'approximation suivant :

LEMME 2.7. – Soient K un corps de nombres, v_0 une place ultramétrique de K et $\gamma_1, \dots, \gamma_n$ des éléments de K . Alors il existe un élément $\beta \in \mathcal{O}_K$ tel que $\beta\gamma_1, \dots, \beta\gamma_n \in \mathcal{O}_K$ et $|\beta|_{v_0} = \max\{1, |\gamma_1|_{v_0}, \dots, |\gamma_n|_{v_0}\}^{-1}$.

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

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

Pour toute place $v \in \Sigma$, notons θ_v l'inverse de l'élément de $\{1, \gamma_1, \dots, \gamma_n\}$ de valeur absolue maximale en v . D'après le théorème de [8, chap II, 15, p. 67] il existe un élément $\beta \in K$ tel que

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

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 K on a $|\beta|_v \leq 1$ (donc $\beta \in \mathcal{O}_K$) et pour tout $i \in \llbracket 1, n \rrbracket$, $|\beta\gamma_i|_v \leq 1$ (donc $\beta\gamma_i \in \mathcal{O}_K$). Enfin, on a bien $|\beta|_{v_0} = \max\{1, |\gamma_1|_{v_0}, \dots, |\gamma_n|_{v_0}\}^{-1}$ car $v_0 \in \Sigma$. Le lemme est donc établi. \square

2.3. Hauteur

La hauteur considérée est la hauteur de Weil logarithmique et absolue, dont nous rappelons rapidement la définition. Soient $\mathbf{x} \in \mathbb{P}^n$, $(x_0 : x_1 : \dots : x_n)$ un choix de coordonnées homogènes pour \mathbf{x} , \mathbb{F} un corps de nombres contenant x_0, x_1, \dots, 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

$$\|\mathbf{x}\|_v = \max\{|x_0|_v, \dots, |x_n|_v\}.$$

Alors la hauteur de \mathbf{x} est le réel positif défini par

$$h(\mathbf{x}) = \sum_{v \in \mathcal{M}_{\mathbb{F}}} \frac{[\mathbb{F}_v : \mathbb{Q}_v]}{[\mathbb{F} : \mathbb{Q}]} \log \|\mathbf{x}\|_v.$$

La hauteur d'un point α de $\mathbb{G}_m^n(\bar{\mathbb{Q}})$ est alors la hauteur du point projectif correspondant :

$$h(\alpha) = h(\iota(\alpha)).$$

Enfin, si F est un polynôme, on note $h(F)$ (resp. $\|F\|_v$) la hauteur (resp. la norme v) de la famille de ses coefficients.

3. Transcendance

Nous fixons maintenant \mathbb{L} , une extension abélienne de \mathbb{Q} de degré fini. 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 [4]. 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.

3.1. Transcendance dans le cas de grande ramification

Nous allons montrer que si la hauteur de α est suffisamment petite et s'il existe un premier p ramifié dans une extension abélienne \mathbb{L} alors l'indice d'obstruction $\omega_{\mathbb{L}(p)}(\alpha^p)$ de α^p sur le sous-corps $\mathbb{L}(p)$ de \mathbb{L} est du même ordre que celui de α sur \mathbb{L} . Pour cela, nous utiliserons la congruence donnée dans le lemme 2.6 et le fait que si ζ est un point de p -torsion alors $\zeta\alpha$ et α 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 α en fonction de certaines valeurs de fonctions de Hilbert. Enfin, en supposant que la hauteur de α est petite, nous en déduirons la non-nullité des espaces vectoriels correspondants, ce qui nous permettra de construire une variété dont le degré réalise $\omega_{\mathbb{L}(p)}(\alpha^p)$.

Nous utilisons tout d'abord la congruence établie dans le lemme 2.6 pour démontrer le lemme suivant, qui va permettre d'extrapoler par la suite.

LEMME 3.1. – Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, \mathbb{L} une extension abélienne de \mathbb{Q} et p un premier ramifié dans \mathbb{L} . Soient $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$ et v une place de $\bar{\mathbb{Q}}$ divisant p . Alors pour tout conjugué $\tilde{\alpha}$ de α au-dessus de \mathbb{L} , pour tout $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$ et pour tout $\zeta \in \ker[p]$ on a

$$|F^\tau(\zeta \tilde{\alpha})|_v \leq p^{-T/p} \|F^\tau\|_v \|\iota(\tilde{\alpha})\|_v^L.$$

La démonstration de ce lemme s’inspire de la preuve alternative d’U. Zannier ([21]) pour généraliser le lemme clef de E. Dobrowolski en dimension supérieure (théorème 3.1 de [2]), et contourner le fait que dans ce cas les anneaux de polynômes ne sont plus principaux.

Démonstration. – Nous supposons que F est non nul, sinon le lemme est trivial. Remarquons tout d’abord que, grâce au lemme 2.7, quitte à multiplier F par un nombre 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 $\tilde{\alpha} = \alpha$. Nous supposerons de plus, dans un premier temps, que α 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 α 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 [19, 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 $i \in \llbracket 1, n \rrbracket$, il existe $a_i \in \mathcal{O}_{\mathbb{L}_v}[X]$ tel que

$$\alpha_i = a_i(\delta).$$

Considérons maintenant $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$; il induit un élément de $\text{Gal}(\mathbb{F}_v/\mathbb{L}_{(p)_v})$ que nous noterons encore τ . La congruence (2.5) se prolonge à $\mathcal{O}_{\mathbb{L}_v}$:

$$(3.1) \quad \forall \gamma \in \mathcal{O}_{\mathbb{L}_v}, \quad \tau \gamma \equiv \gamma \pmod{\sqrt[p]{p\mathcal{O}_{\mathbb{L}_v}}}.$$

Pour tout $i \in \llbracket 1, n \rrbracket$, posons

$$\beta_i = a_i^\tau(\delta)$$

de sorte que

$$(3.2) \quad \beta_i \equiv \alpha_i \pmod{\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}}.$$

Remarquons que $\partial_\lambda(F) \in \mathcal{O}_{\mathbb{F}}[\mathbf{X}]$. Nous allons montrer que pour tout polynôme $H \in \mathcal{O}_{\mathbb{F}}[\mathbf{X}]$ nul en $\{\alpha\}_{\mathbb{L}}$ avec multiplicité au moins t , on a

$$(3.3) \quad H^\tau(\beta) \equiv 0 \pmod{\left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^t}.$$

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 $G = H(a_1, \dots, a_n)$; 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

$$\left\{ \partial_\lambda(H)(a_1, \dots, a_n), |\lambda| \leq s \right\}$$

donc il existe un n -uplet $\lambda \in \mathbb{N}^n$ avec $|\lambda| \leq s$ tel que $\partial_\lambda(H)(a_1, \dots, a_n)$ ne soit pas divisible par Δ . Cela signifie qu’il existe $\sigma \in \text{Gal}(\mathbb{F}_v/\mathbb{L}_v)$ tel que

$$\partial_\lambda(H)(\alpha_1^\sigma, \dots, \alpha_n^\sigma) = \partial_\lambda(H)(a_1(\delta^\sigma), \dots, a_n(\delta^\sigma)) \neq 0.$$

Puisque H est nul en $\{\alpha\}_{\mathbb{L}}$ avec multiplicité au moins t , on en déduit $|\lambda| \geq t$ donc $s \geq t$. Ainsi, on vient de montrer que Δ^t divise $H(a_1, \dots, a_n)$ dans $\mathbb{F}_v[X]$ donc dans $\mathcal{O}_{\mathbb{F}_v}[X]$. On peut alors écrire

$$H^\tau(a_1^\tau(X), \dots, a_n^\tau(X)) = R^\tau(X)(\Delta^\tau(X))^t, \quad R \in \mathcal{O}_{\mathbb{F}_v}[X].$$

En évaluant en δ dans cette équation et en tenant compte du fait que, par (3.1),

$$\Delta^\tau(\delta) \equiv \Delta(\delta) \equiv 0 \pmod{\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}},$$

on obtient (3.3).

Si l'on applique (3.3) à $H = \partial_\lambda(F)$ et $t = T - |\lambda|$, pour un n -uplet quelconque λ vérifiant $|\lambda| \leq T$, on obtient

$$(3.4) \quad \partial_\lambda(F)^\tau(\beta) \equiv 0 \pmod{\left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^{T-|\lambda|}}.$$

Enfin, par la formule de Taylor, on a

$$F^\tau(\zeta\alpha) = \sum_{|\lambda| \geq 0} (\zeta\alpha - \beta)^\lambda \partial_\lambda(F)^\tau(\beta),$$

où $(\zeta\alpha - \beta)^\lambda = \prod_{i=1}^n (\zeta_i\alpha_i - \beta_i)^{\lambda_i}$. Or, pour tout ξ racine p -ième de l'unité, on a $\xi \equiv 1 \pmod{\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}}$. D'où, avec (3.2), $(\zeta\alpha - \beta)^\lambda \equiv 0 \pmod{\left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^{|\lambda|}}$. On en déduit avec (3.4)

$$F^\tau(\zeta\alpha) \equiv 0 \pmod{\left(\sqrt[p]{p\mathcal{O}_{\mathbb{F}_v}}\right)^T}$$

et le lemme est ainsi démontré sous l'hypothèse que $\alpha_1, \dots, \alpha_n$ soient des entiers algébriques.

Dans le cas général, on se ramène, comme dans [2] et [4], au cas précédent en utilisant le lemme 2.7. Ce dernier affirme qu'il existe $\theta \in \mathcal{O}_{\mathbb{F}}$ tel que

$$\left\{ \begin{array}{l} \theta\alpha_1, \dots, \theta\alpha_n \in \mathcal{O}_{\mathbb{F}} \\ \text{et} \\ |\theta|_v = \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{-1}. \end{array} \right.$$

Le polynôme

$$\tilde{F}(X_0, \dots, X_n) = X_0^L F\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right) \in \mathcal{O}_{\mathbb{F}}[\mathbf{X}]$$

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

$$\begin{aligned} |\tilde{F}^\tau(\theta, \zeta_1\theta\alpha_1, \dots, \zeta_n\theta\alpha_n)|_v &= |\theta|_v^L |F^\tau(\zeta\alpha)|_v \\ &= |F^\tau(\zeta\alpha)|_v \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{-L}. \end{aligned}$$

Le lemme est ainsi complètement démontré. □

Nous pouvons maintenant minorer la hauteur de α , à la manière de [1], en utilisant un argument de déterminant qui s'inspire de [5].

PROPOSITION 3.2. – Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ 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

$$h(\alpha) \geq \left(1 - \frac{H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)}{H_{\bar{\mathbb{Q}}}(\ker[p] \cdot \{\alpha\}_{\mathbb{L}(p)}, 1, L)} \right) \frac{T \log p}{pL} - \frac{n}{2L} \log(L+1).$$

Démonstration. – Considérons la matrice de terme général $\beta_k^{\lambda_i}$ où β_k parcourt l'ensemble des points de $\ker[p] \cdot \{\alpha\}_{\mathbb{L}(p)}$ et λ_i l'ensemble des multi-indices de longueur inférieure ou égale à L . Le rang de cette matrice est $r = H_{\bar{\mathbb{Q}}}(\ker[p] \cdot \{\alpha\}_{\mathbb{L}(p)}, 1, L)$. Nous pouvons donc en extraire une matrice de taille $r \times r$ inversible : choisissons β_1, \dots, β_r et $\lambda_1, \dots, \lambda_r$ tels que

$$M = (\beta_i^{\lambda_j})_{1 \leq i, j \leq r}$$

soit de déterminant non nul. Alors l'espace vectoriel

$$\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L) \cap \text{Vect} \{ \mathbf{X}^{\lambda_1}, \dots, \mathbf{X}^{\lambda_r} \}$$

est de dimension supérieure ou égale à $r_0 = r - H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$. Si $r_0 \leq 0$, alors la proposition est triviale, par positivité de la hauteur. Sinon, il existe r_0 polynômes linéairement indépendants $G_k = \sum_{j=1}^r g_{k,j} \mathbf{X}^{\lambda_j}$ ($1 \leq k \leq r_0$) s'annulant sur $\{\alpha\}_{\mathbb{L}}$ 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 $\lambda_1, \dots, \lambda_r$, on peut supposer de plus (grâce au lemme 2.7) que, pour $k = 1, \dots, r_0$, les polynômes

$$G_k = \sum_{j=k}^r g_{k,j} \mathbf{X}^{\lambda_j}$$

sont à coefficients entiers algébriques et

$$(3.5) \quad |g_{k,j}|_v \begin{cases} = 1 & \text{si } j = k; \\ \leq 1 & \text{si } j \in \llbracket k+1, r \rrbracket. \end{cases}$$

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 $(G_k(\beta_1), \dots, G_k(\beta_r))^t$, $k \in \llbracket 1, r_0 \rrbracket$. Par la condition (3.5), on a $|\det(M)|_v = |\det(\tilde{M})|_v$. Comme $G_k \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$, le lemme 3.1 implique

$$|G_k^T(\zeta \alpha)|_{v'} \leq p^{-T/p} \max\{1, |\alpha_1|_{v'}, \dots, |\alpha_n|_{v'}\}^L$$

pour tout $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{L}(p))$, tout $\zeta \in \ker[p]$ et toute place v' divisant p . Pour tout $i \in \llbracket 1, r \rrbracket$ nous fixons $\tau_i \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{L}(p))$ et $\zeta_i \in \ker[p]$ tel que $\beta_i = \tau_i(\zeta_i \alpha)$. Alors

$$\begin{aligned} |G_k(\beta_i)|_v &= |G_k(\tau_i(\zeta_i \alpha))|_v \\ &= |G_k^{\tau_i^{-1}}(\zeta_i \alpha)|_{\tau_i^{-1}v} \\ &\leq p^{-T/p} \max\{1, |\alpha_1|_{\tau_i^{-1}v}, \dots, |\alpha_n|_{\tau_i^{-1}v}\}^L \\ &\leq p^{-T/p} \max\{1, |\beta_{i,1}|_v, \dots, |\beta_{i,n}|_v\}^L. \end{aligned}$$

En développant $\det(\tilde{M})$ suivant les r_0 premières colonnes, on a finalement

$$|\det(M)|_v = |\det(\tilde{M})|_v \leq p^{-r_0 T/p} \prod_{i=1}^{r_0} \max\{1, |\beta_{i,1}|_v, \dots, |\beta_{i,n}|_v\}^L.$$

La formule précédente est valable pour toute place v divisant p . Si v est une autre place finie, l'inégalité ultramétrique donne

$$|\det(M)|_v \leq \prod_{i=1}^r \max\{1, |\beta_{i,1}|_v, \dots, |\beta_{i,n}|_v\}^L.$$

Enfin, si v est une place archimédienne, l'inégalité de Hadamard fournit la majoration

$$\begin{aligned} |\det(M)|_v &\leq \prod_{i=1}^r \left(\sum_{j=1}^r |\beta_i^{\lambda_j}|_v^2 \right)^{1/2} \leq \prod_{i=1}^r (r \max\{1, |\beta_{i,1}|_v, \dots, |\beta_{i,n}|_v\}^{2L})^{1/2} \\ &\leq r^{r/2} \prod_{i=1}^r \max\{1, |\beta_{i,1}|_v, \dots, |\beta_{i,n}|_v\}^L. \end{aligned}$$

En appliquant la formule du produit à $\det(M)$ (qui n'est pas nul), on obtient

$$1 \leq p^{-r_0 T/p} r^{r/2} \prod_{i=1}^r \exp(Lh(\beta_i)) \leq p^{-r_0 T/p} r^{r/2} \exp(Lrh(\alpha))$$

et finalement, en utilisant l'inégalité $r \leq \binom{L+n}{n} \leq (L+1)^n$,

$$h(\alpha) \geq \frac{r_0 T \log p}{r p L} - \frac{n}{2L} \log(L+1),$$

ce qui achève la preuve de la proposition. \square

PROPOSITION 3.3. – *Il existe un nombre réel strictement positif c_0 ne dépendant que de n tel que la propriété suivante soit vraie. Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, \mathbb{L} une extension abélienne de \mathbb{Q} et p un premier ramifié dans \mathbb{L} . Si*

$$h(\alpha) \leq c_0^{-1} \frac{\log p}{p\omega_{\mathbb{L}}(\alpha)},$$

alors

$$\omega_{\mathbb{L}(p)}(\alpha^p) \leq c_0 \omega_{\mathbb{L}}(\alpha) \log(3\omega_{\mathbb{L}}(\alpha)).$$

Démonstration. – Afin d'alléger les notations, nous posons $\omega = \omega_{\mathbb{L}}(\alpha)$. 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

$$\frac{\log(L+1)}{L} \leq c'_2 \frac{\log C \log p}{C p \omega}.$$

Supposons

$$h(\alpha) \leq \frac{1}{C} \frac{\log p}{p\omega}.$$

Alors la proposition 3.2 implique

$$1 - \frac{H_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)}{H_{\mathbb{Q}}(\ker[p] \cdot \{\alpha\}_{\mathbb{L}_{(p)}}, 1, L)} \leq \left(h(\alpha) + \frac{n}{2L} \log(L+1) \right) \frac{pL}{T \log p} \leq c'_3 \frac{\log C}{C} < \frac{1}{2}.$$

Ainsi, $H_{\mathbb{Q}}(\ker[p] \cdot \{\alpha\}_{\mathbb{L}_{(p)}}, 1, L) < 2H_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)$. Or, si P_0 est un polynôme non nul s'annulant sur $\{\alpha\}_{\mathbb{L}}$ de degré minimal ω , alors $P \cdot P_0^T$ appartient à $\mathcal{E}_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)$ pour tout $P \in \mathbb{Q}[X]$ de degré inférieur ou égal à $L - \omega T$; donc

$$H_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L) \leq \binom{L+n}{n} - \binom{L-\omega T+n}{n}.$$

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 $H_{\mathbb{Q}}(\ker[p] \cdot \{\alpha\}_{\mathbb{L}_{(p)}}, 1, L) < \binom{L+n}{n}$, ce qui signifie qu'il existe un polynôme F non nul tel que $F \in \mathcal{E}_{\mathbb{Q}}(\ker[p] \cdot \{\alpha\}_{\mathbb{L}_{(p)}}, 1, L)$. Par le lemme 2.3, on peut supposer que F est à coefficients dans $\mathbb{L}_{(p)}$.

Soit X l'ensemble algébrique défini dans \mathbb{G}_m^n par les équations $F(\zeta X) = 0$ où ζ parcourt $\ker[p]$. Le polynôme F étant identiquement nul sur $\ker[p] \cdot \{\alpha\}_{\mathbb{L}_{(p)}}$, il existe une composante $\mathbb{L}_{(p)}$ -irréductible V de X qui contient $\{\alpha\}_{\mathbb{L}_{(p)}}$. 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 [14] implique

$$\deg(\ker[p]V) \leq L^{\text{codim}V}.$$

Or, par le lemme 2.1 de [10], si W est une variété géométriquement irréductible, on a

$$\deg([p]^{-1}W) = p^{\text{codim}W} \deg(W).$$

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

$$\deg(\ker[p]V) = \deg([p]^{-1}[p]V) = p^{\text{codim}V} \deg([p]V).$$

D'où

$$\deg([p]V) \leq \left(\frac{L}{p} \right)^{\text{codim}V} \leq ((2n+1)C\omega \log(3\omega))^{\text{codim}V}$$

et, par le lemme 2.4 appliqué à $\mathbb{L}_{(p)}$, α^p et $[p]V$,

$$\omega_{\mathbb{L}_{(p)}}(\alpha^p) \leq n(2n+1)C\omega \log(3\omega).$$

On pose alors $c_0 = n(2n+1)C$ et la proposition est démontrée. □

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.

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 $\{\alpha\}_{\mathbb{L}}$. Dans [4], 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 [10]) obtenue à l'aide du théorème plus général de S. Zhang sur les minima successifs d'une variété algébrique (voir [22]). Cette version est un raffinement du lemme de Siegel absolu de D. Roy et J. Thunder (voir [17]). 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 2.3 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 [18] par la formule

$$h_{L_2}(S) = \sum_{v \in \mathcal{M}_{\mathbb{F}}} \frac{[\mathbb{F}_v : \mathbb{Q}_v]}{[\mathbb{F} : \mathbb{Q}]} \log \|\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d\|_v,$$

où $(\mathbf{x}_1, \dots, \mathbf{x}_d)$ est une base de S , \mathbb{F} un corps de nombres contenant les coordonnées des \mathbf{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 $\mathbf{x} \in \bar{\mathbb{Q}}^{N+1}$, on notera $h_{L_2}(\mathbf{x}) = h_{L_2}(S)$.

Énonçons maintenant le lemme.

LEMME 3.4. – *Pour tout $\bar{\mathbb{Q}}$ -espace vectoriel non nul $S \subset \bar{\mathbb{Q}}^{N+1}$, il existe un vecteur non nul $\mathbf{x} \in S$ tel que*

$$h_{L_2}(\mathbf{x}) \leq \frac{h_{L_2}(S)}{\dim S} + \frac{1}{2} \log(\dim(S)).$$

Démonstration. – Voir le lemme 4.7 de [10]. □

Nous pouvons maintenant construire la fonction auxiliaire dont nous aurons besoin.

THÉORÈME 3.5. – *Soient \mathbb{L} une extension abélienne de \mathbb{Q} , α un point de $\mathbb{G}_m^n(\bar{\mathbb{Q}})$ et L, T deux entiers naturels non nuls tels que*

$$2n\omega_{\mathbb{L}}(\alpha)T \leq L \text{ et } h(\alpha) \leq \frac{T \log(L+1)}{L}.$$

Alors il existe $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$ tel que

$$h(F) \leq \frac{18n^2\omega_{\mathbb{L}}(\alpha)T^2 \log(L+1)}{L} + \frac{1}{2} \log \binom{L+n}{n}.$$

Démonstration. – Notons $\alpha_1, \dots, \alpha_d$ les conjugués de α au-dessus de \mathbb{L} . Pour $i \in \llbracket 1, d \rrbracket$ et $\lambda \in \mathbb{N}^n$, $|\lambda| \leq T$, on pose

$$\mathbf{y}_{\alpha_i, \lambda} = \left(\binom{\mu}{\lambda} \alpha_i^{\mu - \lambda} \right)_{\mu \in \mathbb{N}^n, |\mu| \leq L} \in \bar{\mathbb{Q}}^{\binom{L+n}{n}}, \text{ où } \binom{\mu}{\lambda} = \prod_{j=1}^n \binom{\mu_j}{\lambda_j}.$$

En identifiant $\bar{\mathbb{Q}}[\mathbf{X}]_{\leq L}$ à $\bar{\mathbb{Q}}^{\binom{L+n}{n}}$, les $\mathbf{y}_{\alpha_i, \lambda}$ sont des générateurs du sous-espace vectoriel $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)^\perp$, dont la dimension est $H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$. En utilisant l'inégalité

$$\begin{aligned} \left(\sum_{|\mu| \leq L} \binom{\mu}{\lambda} \right)^2 &\leq \sum_{|\mu| \leq L} \binom{\mu}{\lambda} \leq \sum_{\mu_1=0}^L \cdots \sum_{\mu_n=0}^L \binom{\mu_1}{\lambda_1} \cdots \binom{\mu_n}{\lambda_n} \\ &\leq \prod_{i=1}^n \binom{L+1}{\lambda_i+1} \leq (L+1)^{T+n}, \end{aligned}$$

on a la majoration $\|\mathbf{y}_{\alpha_i, \lambda}\|_{v, L_2} \leq (L+1)^{T+n} \|\iota(\alpha_i)\|_v^L$, où v est une place archimédienne et $\|\cdot\|_{v, L_2}$ désigne la norme euclidienne associée à v . Ainsi, la hauteur L_2 des $\mathbf{y}_{\alpha_i, \lambda}$ est majorée :

$$h_{L_2}(\mathbf{y}_{\alpha_i, \lambda}) \leq (T+n) \log(L+1) + Lh(\alpha).$$

On en déduit (voir le paragraphe 8 du chapitre 1 de [18])

$$\begin{aligned} h_{L_2}(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)) &= h_{L_2}(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)^\perp) \\ &\leq \dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)^\perp) \max h_{L_2}(\mathbf{y}_{\alpha_i, \lambda}) \\ &\leq H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L) ((T+n) \log(L+1) + Lh(\alpha)). \end{aligned}$$

Remarquons que $\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))$ est strictement positif. En effet, si $P_0 \in \mathbb{L}[\mathbf{X}]$ est un polynôme non nul s'annulant en α de degré minimal $\omega_{\mathbb{L}}(\alpha)$, alors pour tout $P \in \bar{\mathbb{Q}}[\mathbf{X}]$ de degré inférieur ou égal à $L - \omega_{\mathbb{L}}(\alpha)T$, le polynôme $P \cdot P_0^T$ appartient à $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$. Donc, en utilisant l'hypothèse $2nT\omega_{\mathbb{L}}(\alpha) \leq L$,

$$(3.6) \quad \dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)) \geq \binom{L - \omega_{\mathbb{L}}(\alpha)T + n}{n} \geq \binom{(2n-1)\omega_{\mathbb{L}}(\alpha)T + n}{n} > 0.$$

Le lemme de Siegel absolu (lemme 3.4) assure alors l'existence d'un élément non nul $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$ de hauteur

$$\begin{aligned} h_{L_2}(F) &\leq \frac{H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L) ((T+n) \log(L+1) + Lh(\alpha))}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))} + \frac{1}{2} \log(\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))) \\ &\leq \frac{H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))} ((T+n) \log(L+1) + Lh(\alpha)) + \frac{1}{2} \log \binom{L+n}{n}. \end{aligned}$$

En utilisant l'hypothèse $2nT\omega_{\mathbb{L}}(\alpha) \leq L$ et la première inégalité de (3.6), on a

$$\begin{aligned} \frac{H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))} &= \frac{\binom{L+n}{n} - \dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))} \leq \frac{\binom{L+n}{n} - \binom{L - \omega_{\mathbb{L}}(\alpha)T + n}{n}}{\binom{L - \omega_{\mathbb{L}}(\alpha)T + n}{n}} \\ &\leq \prod_{j=1}^n \left(1 + \frac{T\omega_{\mathbb{L}}(\alpha)}{L - T\omega_{\mathbb{L}}(\alpha) + j} \right) - 1 \leq \left(1 + \frac{2T\omega_{\mathbb{L}}(\alpha)}{L} \right)^n - 1. \end{aligned}$$

En appliquant l'inégalité des accroissements finis à $x \mapsto (x + 1)^n - 1$ entre 0 et $\frac{2T\omega_{\mathbb{L}}(\alpha)}{L}$, on obtient finalement

$$\begin{aligned} \frac{H_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)}{\dim(\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L))} &\leq n \left(1 + \frac{2T\omega_{\mathbb{L}}(\alpha)}{L}\right)^{n-1} \frac{2T\omega_{\mathbb{L}}(\alpha)}{L} \\ &\leq n \left(1 + \frac{1}{n}\right)^{n-1} \frac{2T\omega_{\mathbb{L}}(\alpha)}{L} \\ &\leq ne \frac{2T\omega_{\mathbb{L}}(\alpha)}{L}. \end{aligned}$$

L'hypothèse sur $h(\alpha)$, le fait que $2T + n \leq 3nT$ et l'inégalité $h(F) \leq h_{L_2}(F)$ permettent alors de conclure. □

3.2.2. Extrapolation

LEMME 3.6. – Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, \mathbb{L} une extension abélienne de \mathbb{Q} et p un nombre premier. Soient $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$ et v une place de $\bar{\mathbb{Q}}$ divisant p . Alors pour tout morphisme $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{\mathbb{L}} = \phi_p$ et tout conjugué $\tilde{\alpha}$ de α au-dessus de \mathbb{L} , on a

$$|F^\tau(\tilde{\alpha}^p)|_v \leq p^{-T/e_p(\mathbb{L})} \|F^\tau\|_v \|\iota(\tilde{\alpha})\|_v^{pL}.$$

Démonstration. – La démonstration de ce lemme est semblable à celle du lemme 3.1 en considérant maintenant $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\tau_{\mathbb{L}} = \phi_p$ et la congruence (2.3)

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}_v}, \quad \tau\gamma \equiv \gamma^p \pmod{\mathcal{Q}\mathcal{O}_{\mathbb{L}_v}},$$

où \mathcal{Q} est l'idéal de $\mathcal{O}_{\mathbb{L}}$ tel que $\mathcal{Q}^{e_p(\mathbb{L})} = p\mathcal{O}_{\mathbb{L}}$. Si pour tout $i \in \llbracket 1, n \rrbracket$, on a $\alpha_i = a_i(\delta)$ avec $a_i \in \mathcal{O}_{\mathbb{L}_v}[X]$, on pose

$$\beta_i = a_i^\tau(\delta^p)$$

de sorte que

$$\beta_i \equiv \alpha_i^p \pmod{\mathcal{Q}\mathcal{O}_{\mathbb{F}_v}}$$

et on conclut comme dans la démonstration du lemme 3.1 sans faire intervenir ici les points de p -torsion. □

Si x est un réel, nous notons $\lceil x \rceil$ l'entier qui lui est immédiatement supérieur.

LEMME 3.7. – Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, \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 $F \in \mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha\}_{\mathbb{L}}, T, L)$. Supposons

$$(3.7) \quad h(\alpha) \leq \frac{1}{4} \frac{T \log p}{EpL} \quad \text{et} \quad h(F) \leq \frac{1}{4} \frac{T \log p}{E}.$$

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 $\mathcal{E}_{\bar{\mathbb{Q}}}(\{\alpha^p\}_{\mathbb{L}}, \lceil T_1 \rceil, L)$.

Démonstration. – Soit \mathbb{F} une extension galoisienne de \mathbb{Q} contenant \mathbb{L} , les coefficients de F et les coordonnées de α . Soient $\lambda \in \mathbb{N}^n$ tel que $|\lambda| = T^* < T$ et v une place de \mathbb{F} . Comme $F \in \mathcal{E}_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)$, on a $\partial_{\lambda}(F) \in \mathcal{E}_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T - T^*, L)$. Le lemme 3.6 affirme que, pour tout prolongement τ_p de ϕ_p à $\bar{\mathbb{Q}}$, on a

$$\begin{aligned} |\partial_{\lambda}(F)^{\tau_p}(\alpha^p)|_v &\leq p^{-(T-T^*)/e_p(\mathbb{L})} \|\partial_{\lambda}(F)^{\tau_p}\|_v \|\iota(\alpha)\|_v^{pL} \\ &\leq p^{-(T-T^*)/e_p(\mathbb{L})} \|F^{\tau_p}\|_v \|\iota(\alpha)\|_v^{pL} \end{aligned}$$

si v est une place divisant p . D’autre part, on déduit de l’inégalité

$$\sum_{|\mu| \leq L} \binom{\mu}{\lambda} \leq \binom{L+1}{\lambda_1+1} \cdots \binom{L+1}{\lambda_n+1} \leq (L+1)^{|\lambda|+n}$$

et de l’inégalité ultramétrique les majorations

$$|\partial_{\lambda}(F)^{\tau_p}(\alpha^p)|_v \leq \begin{cases} \|F^{\tau_p}\|_v \|\iota(\alpha)\|_v^{pL} & \text{si } v \nmid \infty, \\ (L+1)^{T^*+n} \|F^{\tau_p}\|_v \|\iota(\alpha)\|_v^{pL} & \text{si } v \mid \infty. \end{cases}$$

Ainsi, si $\partial_{\lambda}(F)^{\tau_p}(\alpha^p) \neq 0$, les inégalités ci-dessus et la formule du produit donnent

$$0 \leq (T^* + n) \log(L + 1) + h(F) + pLh(\alpha) - \frac{T - T^*}{e_p(\mathbb{L})} \log p.$$

Avec les hypothèses (3.7) 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 α au-dessus de \mathbb{L} , ce qui achève la preuve. \square

En utilisant r fois le lemme 3.7, on obtient :

LEMME 3.8. – Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ 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, \dots, 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 $F \in \mathcal{E}_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)$. Supposons

$$(3.8) \quad h(\alpha) \leq \frac{1}{4} \frac{T_{r-1} \min \log p_i}{EL p_1 \cdots p_r} \quad \text{et} \quad h(F) \leq \frac{1}{4} \frac{T_{r-1} \min \log p_i}{E}.$$

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 $\mathcal{E}_{\mathbb{Q}}(\{\alpha^{p_1 \cdots p_r}\}_{\mathbb{L}}, [T_r], L)$.

Démonstration. – On montre ce lemme par récurrence sur r . Le cas $r = 1$ correspond au lemme 3.7. 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 les indices de ramification dans \mathbb{L} sont inférieurs à E et $F \in \mathcal{E}_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)$ tels que les conditions (3.8) soient satisfaites. En particulier, on a

$$h(\alpha) \leq \frac{1}{4} \frac{T_{r-2} \min \log p_i}{EL p_1 \cdots p_{r-1}} \quad \text{et} \quad h(F) \leq \frac{1}{4} \frac{T_{r-2} \min \log p_i}{E}.$$

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

$$F^{\tau_{p_1} \cdots \tau_{p_{r-1}}} \in \mathcal{E}_{\mathbb{Q}}(\{\alpha^{p_1 \cdots p_{r-1}}\}_{\mathbb{L}}, [T_{r-1}], L).$$

Or $h(F^{\tau_{p_1} \cdots \tau_{p_{r-1}}}) = h(F)$ et $h(\alpha^{p_1 \cdots p_{r-1}}) = p_1 \cdots p_{r-1} h(\alpha)$, d'où

$$h(\alpha^{p_1 \cdots p_{r-1}}) \leq \frac{1}{4} \frac{T_{r-1} \log p_r}{E p_r L} \leq \frac{1}{4} \frac{[T_{r-1}] \log p_r}{E p_r L}.$$

On applique alors le lemme 3.7 en remplaçant respectivement $T, p, \{\alpha\}_{\mathbb{L}}$ et F par $[T_{r-1}], p_r, \{\alpha^{p_1 \cdots p_{r-1}}\}_{\mathbb{L}}$ et $F^{\tau_{p_1} \cdots \tau_{p_{r-1}}}$ pour conclure. \square

3.2.3. *Lemme de zéros.* – Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, \mathbb{L} une extension abélienne de \mathbb{Q} , L un entier naturel non nul et $N_j, j \in [1, n]$, des réels strictement positifs. 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 $\sigma_p \in \text{Gal}(\mathbb{L}/\mathbb{Q})$.

THÉORÈME 3.9. – Soit G un polynôme non nul tel que $G^{\sigma_{p_1} \cdots \sigma_{p_n}}$ appartient à $\mathcal{E}_{\mathbb{L}}(\{\alpha^{p_1 \cdots p_n}\}_{\mathbb{L}}, 1, L)$ 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}_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

$$\alpha^{p_{r+1} \cdots p_n} \in \sigma_{p_n} \cdots \sigma_{p_{r+1}} V$$

et

$$(3.9) \quad \deg \left(\bigcup_{p \in \mathcal{P}_r} \sigma_p^{-1} [p] V \right) \leq (N_1 \cdots N_{r-1} L)^{\text{codim}(V)}.$$

Démonstration. – À la manière de [2], on définit une suite d'idéaux $\mathcal{J}_1, \dots, \mathcal{J}_{n+1}$ de $\bar{\mathbb{Q}}[\mathbf{X}]$ en posant

$$\begin{aligned} \mathcal{J}_1 &= (G(\mathbf{X})), \\ \mathcal{J}_2 &= (G^{\sigma_{p_1}}(\mathbf{X}^{p_1}), p_1 \in \mathcal{P}_1), \\ \mathcal{J}_3 &= (G^{\sigma_{p_1} \sigma_{p_2}}(\mathbf{X}^{p_1 p_2}), (p_1, p_2) \in \mathcal{P}_1 \times \mathcal{P}_2), \\ &\vdots \\ \mathcal{J}_{n+1} &= (G^{\sigma_{p_1} \cdots \sigma_{p_n}}(\mathbf{X}^{p_1 \cdots p_n}), (p_1, \dots, p_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n). \end{aligned}$$

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 $(p_r, \dots, p_n) \in \mathcal{P}_r \times \cdots \times \mathcal{P}_n$ tel que

$$\alpha^{p_r \cdots p_n} \in \sigma_{p_n} \cdots \sigma_{p_r} V.$$

Par hypothèse sur G , on a $Y_r \neq \emptyset$. De plus, pour tout $r \in [1, n]$ et pour tout $p \in \mathcal{P}_r$,

$$(3.10) \quad [p]Y_{r+1} \subset \sigma_p Y_r.$$

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 (3.10), 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 [14] implique alors

$$\deg(W) \leq (N_1 \cdots N_{r-1}L)^{\text{codim}(V)},$$

ce qui achève la démonstration du théorème. □

3.3. Théorème clef

Le but de cette dernière partie est d'établir un théorème qui résume l'étape de transcendance. Soient $\alpha \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$ et \mathbb{L} une extension abélienne de \mathbb{Q} . Pour alléger les notations, nous posons $\omega = \omega_{\mathbb{L}}(\alpha)$. 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, \dots , des réels strictement positifs (effectivement calculables) ne dépendant que de n . Soient ρ et δ des nombres réels positifs tels que

$$(1 + \delta)(1 + \rho) \leq (1 + n)((n + 1)! - 1)(1 + 2n^2 + 1)^n.$$

Nous fixons les paramètres suivants ⁽²⁾ :

$$T = \left[C_0^{\delta n + 1/2} \frac{(\log(3\omega))^{n(\delta+1)}}{(\log \log(16\omega))^n} \right], \quad L = \omega T^2 \quad \text{et} \quad E = (C_0 \log(3\omega))^\delta.$$

Pour tout $j \in \llbracket 1, n \rrbracket$, nous posons

$$N_j = (C_0 \log(3\omega))^{2n(1+\rho)(1+\delta)j \cdot j!}$$

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

$$(3.11) \quad N_1 \cdots N_j = (C_0 \log(3\omega))^{2n(1+\rho)(1+\delta)((j+1)!-1)}.$$

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.

⁽²⁾ 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 .

PROPOSITION 3.10. – *Supposons*

$$(3.12) \quad h(\alpha) \leq \left(\omega(C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)((n+1)!-1)+2n(\delta+1)-1} \right)^{-1}$$

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 $F \in \mathbb{Q}[\mathbf{X}]$ de degré inférieur ou égal à L tel que, pour tout $(p_1, \dots, p_n) \in \mathcal{P}_1 \times \dots \times \mathcal{P}_n$ et pour tous $\tau_{p_1}, \dots, \tau_{p_n}$ prolongeant à \mathbb{Q} les morphismes $\phi_{p_1}, \dots, \phi_{p_n}$, le polynôme $F^{\tau_{p_1} \dots \tau_{p_n}}$ est nul sur $\{\alpha^{p_1 \dots p_n}\}_{\mathbb{L}}$.

Démonstration. – On a

$$\frac{2n\omega T}{L} = \frac{2n}{T} < 1$$

et, avec l’hypothèse (3.12),

$$\frac{L}{T \log(L+1)} h(\alpha) \leq \omega T h(\alpha) \leq \omega C_0^{\delta n+1/2} (\log(3\omega))^{n(\delta+1)} h(\alpha) < 1,$$

de sorte que les hypothèses du théorème 3.5 sont vérifiées. On en déduit l’existence de $F \in \mathcal{E}_{\mathbb{Q}}(\{\alpha\}_{\mathbb{L}}, T, L)$ 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 3.8, que ce polynôme F convient. Pour cela, vérifions que les hypothèses de ce lemme sont satisfaites. Soit $(q_1, \dots, q_n) \in \mathcal{P}_1 \times \dots \times \mathcal{P}_n$; supposons q_{j_1}, \dots, q_{j_r} premiers et $q_j = 1$ pour $j \notin \{j_1, \dots, j_r\}$. Pour $i \in \llbracket 1, r \rrbracket$, 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 3.8; on a

$$\begin{aligned} T_{r-1}^{-1} &= 2^{r-1} T^{-1} \prod_{j=1}^{r-1} \left(1 + \frac{(n+1)E \log(L+1)}{\log p_j} \right) \\ &\leq c_4 T^{-1} \prod_{j=1}^{r-1} \left(\frac{E \log(L+1)}{\log \log(16\omega)} \right) \\ &\leq c_5 C_0^{-(\delta n+1/2)} \frac{(\log \log(16\omega))^n}{(\log(3\omega))^{n(\delta+1)}} \left(\frac{C_0^\delta (\log C_0) (\log(3\omega))^{\delta+1}}{\log \log(16\omega)} \right)^{n-1} \\ &\leq c_5 \frac{(\log C_0)^{n-1} \log \log(16\omega)}{C_0^{(\delta+1/2)} (\log(3\omega))^{(\delta+1)}}. \end{aligned}$$

Ainsi,

$$\begin{aligned} \frac{4Eh(F)}{T_{r-1} \min \log p_i} &\leq c_6 \frac{(C_0 \log(3\omega))^\delta (\log C_0) (\log(3\omega)) (\log C_0)^{n-1} \log \log(16\omega)}{\log \log(16\omega) C_0^{(\delta+1/2)} (\log(3\omega))^{(\delta+1)}} \\ &\leq c_6 \frac{(\log C_0)^n}{C_0^{1/2}} < 1. \end{aligned}$$

Par ailleurs, par hypothèse sur $h(\alpha)$ et en utilisant (3.11) avec $j = n$, on a

$$N_1 \cdots N_n h(\alpha) \leq \omega^{-1} (C_0 \log(3\omega))^{-(2n(\delta+1)-1)}.$$

D'où

$$\begin{aligned} \frac{4ELp_1 \cdots p_r}{T_{r-1} \min \log p_i} h(\alpha) &\leq \frac{4\omega ET^2 N_{j_1} \cdots N_{j_r} h(\alpha)}{T_{r-1} (\log \log(16\omega))} \\ &\leq c_7 \omega \frac{C_0^{2\delta n + \delta + 1} (\log(3\omega))^{2n(\delta+1) + \delta}}{(\log \log(16\omega))^{2n+1}} T_{r-1}^{-1} N_1 \cdots N_n h(\alpha) \\ &\leq c_8 \frac{C_0^{2\delta n + 1/2} (\log C_0)^{n-1} (\log(3\omega))^{2n(\delta+1)-1}}{(\log \log(16\omega))^{2n}} \\ &\quad \times (C_0 \log(3\omega))^{-(2n(\delta+1)-1)} \\ &\leq c_8 \frac{(\log C_0)^{n-1}}{C_0^{2n-3/2}} < 1. \end{aligned}$$

Le lemme 3.8 assure alors que, pour tous $\tau_{p_1}, \dots, \tau_{p_r}$ prolongeant respectivement $\phi_{p_1}, \dots, \phi_{p_r}$, le polynôme $F^{\tau_{p_1} \cdots \tau_{p_r}}$ est nul sur $\{\alpha^{p_1 \cdots p_r}\}_{\mathbb{L}}$ 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 $(q_1, \dots, q_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ et pour tous $\tau_{q_1}, \dots, \tau_{q_n}$ prolongeant respectivement $\phi_{q_1}, \dots, \phi_{q_n}$, le polynôme $F^{\tau_{q_1} \cdots \tau_{q_n}}$ est nul sur $\{\alpha^{q_1 \cdots q_n}\}_{\mathbb{L}}$. \square

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 3.11. – Soient \mathbb{L} une extension abélienne de \mathbb{Q} et V une variété définie sur \mathbb{L} telle que

$$(3.13) \quad \log \deg(V) \leq (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)-1}.$$

Pour tout $j \in \llbracket 1, n \rrbracket$, 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 $p_1 \cdots p_n \notin E_{\text{exc}}(V)$ pour tout $(p_1, \dots, p_n) \in \mathcal{P}_1(V) \times \cdots \times \mathcal{P}_n(V)$.

Démonstration. – On procède comme dans le lemme 5.2 de [2], en minorant le cardinal des ensembles \mathcal{P}_j à l'aide du théorème des nombres premiers puis en posant, pour tout $j \in \llbracket 1, n \rrbracket$,

$$E_j = \bigcup_{p_1 \in \mathcal{P}_1} \cdots \bigcup_{p_{j-1} \in \mathcal{P}_{j-1}} E_{\text{exc}}([p_1 \cdots p_{j-1}]V)$$

et $\mathcal{P}_j(V) = \mathcal{P}_j \setminus E_j$. Par le troisième point du lemme 2.2, on a alors $p_1 \cdots p_n \notin E_{\text{exc}}(V)$ pour tout $(p_1, \dots, p_n) \in \mathcal{P}_1(V) \times \cdots \times \mathcal{P}_n(V)$. En utilisant le dernier point du lemme 2.2, on montre alors que le cardinal de l'ensemble des nombres premiers contenus dans E_j est négligeable par rapport au cardinal de \mathcal{P}_j et on obtient ainsi la minoration voulue pour le cardinal de $\mathcal{P}_j(V)$. \square

Nous pouvons maintenant énoncer et montrer le théorème clef.

THÉORÈME 3.12. – Soit V une sous-variété de \mathbb{G}_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

$$(3.14) \quad h(\alpha) \leq \left(\omega(C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)((n+1)!-1)+2n(\delta+1)-1} \right)^{-1}.$$

Supposons de plus qu'il n'existe pas de sous-variété de torsion B définie sur \mathbb{L} et contenant un conjugué de α telle que

$$(3.15) \quad (\deg B)^{1/\text{codim}(B)} \leq \omega(C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(n+1)!}.$$

Alors l'une des deux propriétés suivantes est vraie :

1. Il existe un premier $p \notin E_{\text{exc}}(V)$ tel que

$$E \leq p \leq N_n$$

qui est ramifié dans \mathbb{L} avec

$$e_p(\mathbb{L}) \geq E$$

et tel que

$$(3.16) \quad \omega_{\mathbb{L}(p)}(\alpha^p) \leq c_0 \omega_{\mathbb{L}}(\alpha) \log(3\omega_{\mathbb{L}}(\alpha)).$$

2. Il existe un entier $l \notin E_{\text{exc}}(V)$ tel que

$$l \leq (C_0 \log(3\omega))^{2n(1+\delta)(\rho+1)((n+1)!-1)}$$

et

$$(3.17) \quad \omega_{\mathbb{L}}(\alpha^l) \leq \frac{\omega_{\mathbb{L}}(\alpha)}{C_0^{1/2} (C_0 \log(3\omega_{\mathbb{L}}(\alpha)))^{2n(1+\delta)\rho}}.$$

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 3.3 ; on a

$$c_0 \frac{p\omega}{\log p} h(\alpha) \leq c_0 (C_0 \log(3\omega))^{-e},$$

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

$$c_0 \frac{p\omega}{\log p} h(\alpha) < 1.$$

Ainsi, la proposition 3.3 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 3.10. Ainsi $F^{\tau_{p_1} \cdots \tau_{p_n}}$ est nul sur $\{\alpha^{p_1 \cdots p_n}\}_{\mathbb{L}}$ pour tout $(p_1, \dots, p_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ et pour tous $\tau_{p_1}, \dots, \tau_{p_n}$ prolongeant à \mathbb{Q} les morphismes $\phi_{p_1}, \dots, \phi_{p_n}$. 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

$$G = \sum_{\sigma \in \text{Gal}(\mathbb{F}/\mathbb{L})} F^\sigma$$

est non nul et satisfait les hypothèses du lemme de zéros (théorème 3.9) appliqué aux ensembles d'entiers $\mathcal{P}_j(V)$ définis dans le lemme précédent (lemme 3.11) et aux morphismes ϕ_p correspondants. Le lemme de zéros nous fournit donc un indice r et une sous-variété Z de \mathbb{G}_m^n définie sur \mathbb{L} , de codimension inférieure ou égale à r , contenant un conjugué d'une certaine puissance α^l , avec $l \notin E_{\text{exc}}(V)$ (par le lemme 3.11) 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 (3.9) est satisfaite. Cette inégalité donne en particulier (car $1 \in \mathcal{P}_r(V)$):

$$\begin{aligned} \deg(Z)^{1/\text{codim}(Z)} &\leq LN_1 \cdots N_{r-1} \\ &\leq LN_1 \cdots N_{n-1} \\ (3.18) \quad &\leq \omega C_0^{2\delta n+1} (\log(3\omega))^{2n(\delta+1)} (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(n!-1)} \\ &\leq \omega (C_0 \log(3\omega))^{2n(\delta+1)((\rho+1)(n!-1)+1)} \\ &\leq \omega (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)n!}. \end{aligned}$$

Une composante \mathbb{L} -irréductible B de $[l]^{-1}Z$ contient un conjugué de $\{\alpha\}_{\mathbb{L}}$ et son degré satisfait l'inégalité

$$\begin{aligned} \deg(B)^{1/\text{codim}(B)} &\leq l \deg(Z)^{1/\text{codim}(Z)} \\ &\leq N_{r+1} \cdots N_n LN_1 \cdots N_{r-1} \\ &\leq \omega (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(n+1)!}. \end{aligned}$$

Par hypothèse, la variété B (donc Z) n'est pas de torsion. Par ailleurs, l'inégalité (3.18) montre en particulier que

$$\log(\deg(Z)) \leq c_{12} \log(C_0) \log(3\omega).$$

Soit $\mathcal{Q} = \mathcal{P}_r(V) \setminus E_{\text{exc}}(Z)$; la proposition 2.2 et l'inégalité ci-dessus assurent que $|E_{\text{exc}}(Z) \cap \{p \text{ premiers}\}|$ est négligeable devant la minoration de $|\mathcal{P}_j(V)|$ fournie par le lemme 3.11, de sorte que

$$(3.19) \quad |\mathcal{Q}| \geq c_{13} \frac{(C_0 \log(3\omega))^{2n(\rho+1)(\delta+1)r \cdot r!}}{(\log C_0) \log \log(16\omega)}.$$

Comme Z n'est pas de torsion, le lemme 2.3, point (i) de [2] 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 (3.9) du lemme de zéros (théorème 3.9),

$$|\mathcal{Q}| \deg(Z) \leq \deg\left(\bigcup_{p \in \mathcal{P}_r(V)} \tau_p^{-1}[p]Z\right) \leq (LN_1 \cdots N_{r-1})^{\text{codim}Z}.$$

Ainsi, en utilisant l'inégalité $\text{codim}Z \leq r$, on obtient la majoration suivante pour le degré de Z :

$$\deg(Z)^{1/\text{codim}(Z)} \leq LN_1 \cdots N_{r-1} |\mathcal{Q}|^{-1/r}.$$

En utilisant la relation (3.11) et la minoration (3.19) de $|\mathcal{Q}|$, on a

$$\begin{aligned} \deg(Z)^{1/\text{codim}(Z)} &\leq c_{14}\omega C_0^{2\delta n+1} \frac{(\log(3\omega))^{2n(\delta+1)}}{(\log \log(16\omega))^{2n}} (C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)(r-1)} \\ &\quad \times \frac{((\log C_0) \log \log(16\omega))^{1/r}}{(C_0 \log(3\omega))^{2n(\delta+1)(\rho+1)r!}} \\ &\leq c_{14}\omega C_0^{-1} (\log C_0) (C_0 \log(3\omega))^{-2n(\delta+1)\rho}. \end{aligned}$$

Or il existe $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que τZ contienne $\{\alpha^l\}_{\mathbb{L}}$. En appliquant le lemme 2.4 à \mathbb{L}, α et τZ , on obtient

$$\omega_{\mathbb{L}}(\alpha^l) \leq n \deg(\tau Z)^{1/\text{codim}(\tau Z)} \leq \frac{\omega}{C_0^{1/2} (C_0 \log(3\omega))^{2n(\delta+1)\rho}},$$

ce qui correspond à la deuxième assertion de la conclusion alternative du théorème. □

4. Descente

Nous fixons $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ et \mathbb{L} extension abélienne de \mathbb{Q} . Si nous pouvions assurer dans le théorème clef (théorème 3.12) que nous sommes dans la deuxième conclusion avec $l = 1$, le théorème 1.5 s'en déduirait immédiatement. Plus généralement, si nous sommes dans la deuxième conclusion du 3.12, alors il existe un entier l n'appartenant pas à l'ensemble exceptionnel d'une certaine variété V tel que $\omega_{\mathbb{L}}(\alpha^l) < \omega_{\mathbb{L}}(\alpha)$. Soient V_l une hypersurface \mathbb{L} -irréductible contenant α^l telle que $\deg V_l = \omega_{\mathbb{L}}(\alpha^l)$ et V'_l une composante \mathbb{L} -irréductible de $[l]^{-1}V_l$ contenant α . Alors $\omega_{\mathbb{L}}(\alpha) \leq \deg V'_l$ et $\deg([l]V'_l) = \deg V_l = \omega_{\mathbb{L}}(\alpha^l)$.

Si nous pouvions assurer, *a priori*, que l n'est pas dans $E_{\text{exc}}(V'_l)$, le théorème 1.5 serait alors démontré dans la mesure où l'on aurait

$$\omega_{\mathbb{L}}(\alpha) \leq \deg V'_l \leq \deg([l]V'_l) \leq \omega_{\mathbb{L}}(\alpha^l)$$

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 construire, à l'aide d'un bon choix de paramètres, une suite de variétés possédant des propriétés particulières en appliquant plusieurs fois de suite le théorème 3.12.

Nous commençons par introduire les paramètres suivants, pour $i \in \llbracket 1, n \rrbracket$:

$$\begin{aligned} \nu_i &= (1+n)((n+1)!-1)(1+2n^2+1)^{n-i}; \\ P_i &= (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n\nu_i n n!}; \\ L_i &= (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n\nu_i((n+1)!-1)}; \\ \delta_i &= n \left(1 + 2n((n+1)!-1) \sum_{j=i+1}^n \nu_j \right); \\ E_i &= \left(\frac{C_0}{(\log C_0)^2} \log(3\omega_{\mathbb{L}}(\alpha)) \right)^{\delta_i}; \\ \varepsilon_i &= \frac{1}{C_0^{1/2} (C_0(\log C_0)^{-2} \log(3\omega_{\mathbb{L}}(\alpha)))^{2n((n+1)!-1)} \sum_{j=i+1}^n \nu_j}. \end{aligned}$$

Remarquons que, pour tout $i \in \llbracket 1, n \rrbracket$, un calcul simple donne

$$(4.1) \quad \nu_i = (\delta_i + 1) + ((n+1)!-1) \sum_{j=i+1}^n \nu_j.$$

En effet, en posant $\gamma = (((n+1)!-1)(1+2n^2+1))$, on obtient

$$\begin{aligned} & \nu_i - (\delta_i + 1) - ((n+1)!-1) \sum_{j=i+1}^n \nu_j \\ &= \nu_i - n \left(1 + 2n((n+1)!-1) \sum_{j=i+1}^n \nu_j \right) - 1 - ((n+1)!-1) \sum_{j=i+1}^n \nu_j \\ &= \nu_i - n - 1 - (((n+1)!-1)(2n^2+1)) \sum_{j=i+1}^n \nu_j \\ &= (1+n) \left(\gamma^{n-i} - 1 - (\gamma-1) \sum_{j=i+1}^n \gamma^{n-j} \right) \\ &= 0. \end{aligned}$$

Remarquons également les égalités suivantes que nous utiliserons plusieurs fois dans la suite :

$$(4.2) \quad L_1 \cdots L_k = (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n((n+1)!-1) \sum_{i=1}^k \nu_i}$$

et

$$(4.3) \quad L_{k+1} \cdots L_n = (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n((n+1)!-1) \sum_{i=k+1}^n \nu_i}.$$

Si nous appliquons plusieurs fois de suite le théorème 3.12, nous pourrions construire une suite de variétés possédant des propriétés particulières, ce qui motive la définition suivante.

DÉFINITION 4.1. – On note \mathcal{W} l'ensemble des quadruplets $(k, \mathbf{l}, \mathbf{V}, \mathbf{L})$ où $k \in \llbracket 0, n \rrbracket$, $\mathbf{l} = (l_1, \dots, l_k)$ est un k -uplet d'entiers, $\mathbf{V} = (V_0, \dots, V_k)$ est un $(k+1)$ -uplet de sous-variétés propres de \mathbb{G}_m^n et $\mathbf{L} = (\mathbb{L}_0, \dots, \mathbb{L}_k)$ est un $(k+1)$ -uplet d'extensions abéliennes de \mathbb{Q} tels que :

- (a₀) $\mathbb{L}_0 = \mathbb{L}$;
- (b₀) V_0 est définie sur \mathbb{L}_0 et est \mathbb{L}_0 -irréductible ;
- (c₀) $\alpha \in V_0$;
- (d₀) $\deg V_0 \leq (L_1 \cdots L_n \omega_{\mathbb{L}}(\alpha))^{\text{codim} V_0}$;

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) $l_i \notin E_{\text{exc}}(V_{i-1})$;
- (d) $\mathbb{L}_i = (\mathbb{L}_{i-1})_{(l_i)}$;
- (e) V_i est définie sur \mathbb{L}_i et est \mathbb{L}_i -irréductible ;
- (f) $[l_i]V_{i-1} \subset V_i$;
- (g) $\deg V_i \leq (L_{i+1} \cdots L_n \omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}))^{\text{codim} V_i}$;
- (h) $\omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}) \leq c_0 \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) \log(3\omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}))$.

2. Soit l'indice i est de type II :

- (a) l_i est un entier ;
- (b) $l_i \leq L_i$;
- (c) $l_i \notin E_{\text{exc}}(V_{i-1})$;
- (d) $\mathbb{L}_i = \mathbb{L}_{i-1}$;
- (e) V_i est définie sur \mathbb{L}_i et est \mathbb{L}_i -irréductible ;
- (f) $[l_i]V_{i-1} \subset V_i$;
- (g) $\deg V_i \leq (L_{i+1} \cdots L_n \omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}))^{\text{codim} V_i}$;
- (h) $\omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}) \leq \varepsilon_i \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}})$.

Si $(k, \mathbf{l}, \mathbf{V}, \mathbf{L}) \in \mathcal{W}$, nous noterons r_{I} l'ensemble des indices de type I dans $(k, \mathbf{l}, \mathbf{V}, \mathbf{L})$ et r_{II} l'ensemble des indices de type II (on a alors $|r_{\text{I}}| + |r_{\text{II}}| = k$).

Remarquons que cette définition implique en particulier que le n -uplet $\mathbf{L} = (\mathbb{L}_0, \dots, \mathbb{L}_k)$ 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 3.12 à une certaine puissance $\alpha^{l_1 \cdots l_k}$ de α , issue d'un élément de \mathcal{W} . Pour vérifier les hypothèses du théorème 3.12, il nous faut des informations concernant l'indice d'obstruction de ⁽³⁾ $\alpha^{l_1 \cdots l_k}$. Or, le point $\alpha^{l_1 \cdots l_k}$ étant issu d'un élément de \mathcal{W} , nous pouvons comparer son indice d'obstruction à celui de α :

LEMME 4.2. – Soit $(k, \mathbf{l}, \mathbf{V}, \mathbf{L}) \in \mathcal{W}$. Alors, pour tout $j \in \llbracket 0, k \rrbracket$, on a

$$(4.4) \quad \omega_{\mathbb{L}_j}(\alpha^{l_1 \cdots l_j}) \leq c_{15} \omega_{\mathbb{L}}(\alpha) (\log(3\omega_{\mathbb{L}}(\alpha)))^{|r_{\text{I}} \cap \llbracket 1, j \rrbracket|}$$

et

$$(4.5) \quad \frac{1}{(\log C_0)^2} \log(3\omega_{\mathbb{L}}(\alpha)) \leq \log(3\omega_{\mathbb{L}_j}(\alpha^{l_1 \cdots l_j})) \leq c_{16} \log(3\omega_{\mathbb{L}}(\alpha)).$$

⁽³⁾ Notons, à ce propos, qu'il y a une légère erreur dans [2] et [4] : les auteurs ne vérifient pas exactement les hypothèses de la proposition qui résume la transcendance (proposition 5.3 dans [2] et proposition 2.8 dans [4]) ; 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 (4), (5) et (6) pour plus de précisions.

Démonstration. – L’inégalité (4.4) est immédiate, après avoir noté que pour tout $i \in \llbracket 1, j \rrbracket$:

– si l’indice i est de type I, alors

$$\omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}) \leq c_0 \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) \log(3\omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}})) ;$$

– si l’indice i est de type II, alors

$$\omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}) \leq \varepsilon_i \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) \leq \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}).$$

On en déduit la deuxième inégalité de (4.5). De plus, comme $\mathbb{L}_j \subseteq \mathbb{L}_0$, on a

$$\omega_{\mathbb{L}}(\alpha) = \omega_{\mathbb{L}_0}(\alpha) \leq l_1 \cdots l_j \omega_{\mathbb{L}_0}(\alpha^{l_1 \cdots l_j}) \leq l_1 \cdots l_j \omega_{\mathbb{L}_j}(\alpha^{l_1 \cdots l_j})$$

et ainsi, par le choix des paramètres,

$$\log(3\omega_{\mathbb{L}}(\alpha)) \leq c_{17}(\log C_0) \log(3\omega_{\mathbb{L}_j}(\alpha^{l_1 \cdots l_j})) \leq (\log C_0)^2 \log(3\omega_{\mathbb{L}_j}(\alpha^{l_1 \cdots l_j})). \quad \square$$

Introduisons maintenant deux définitions :

DÉFINITION 4.3. – On note \mathcal{W}_0 le sous-ensemble de \mathcal{W} défini de la façon suivante :

$$\mathcal{W}_0 = \{(k, \mathbf{l}, \mathbf{V}, \mathbf{L}) \in \mathcal{W}, \dim V_0 < \dim V_1 < \cdots < \dim V_k\}.$$

DÉFINITION 4.4. – 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 binaire réflexive, transitive et complète) en posant

$$(4.6) \quad (k, \mathbf{l}, \mathbf{V}, \mathbf{L}) \preceq (k', \mathbf{l}', \mathbf{V}', \mathbf{L}') \text{ si } (\dim V_i)_{0 \leq i \leq k} \preceq (\dim V'_i)_{0 \leq i \leq k'}.$$

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 4.5. – *Supposons qu’il n’existe pas de sous-variété de torsion B contenant α telle que*

$$(4.7) \quad \deg(B)^{1/\text{codim}(B)} \leq \omega_{\mathbb{L}}(\alpha) (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n \cdot (n+1)! \sum_{j=1}^n \nu_j + n - 1}$$

et que l’on ait

$$h(\alpha) < \omega_{\mathbb{L}}(\alpha)^{-1} \left((C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n((n+1)!-1) \sum_{j=1}^n \nu_j + 2n(\delta_1+1)-1} \right)^{-1}.$$

Alors il existe $(k, \mathbf{l}, \mathbf{V}, \mathbf{L}) \in \mathcal{W} \setminus \mathcal{W}_0$.

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 (4.6)). Puis à partir de cet élément, nous construisons une nouvelle suite de sous-variétés, à l’aide du théorème 3.12. Nous montrons ensuite que cette suite de sous-variétés est en fait un élément de \mathcal{W} qui est strictement inférieur (pour l’ordre (4.6)) 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 : si V_0 est une hypersurface définie sur \mathbb{L} contenant α de degré minimal $\omega_{\mathbb{L}}(\alpha)$, alors le quadruplet $(0, \emptyset, V_0, \mathbb{L}_0)$ appartient trivialement à \mathcal{W}_0 .

Par ailleurs, l’ensemble des suites finies d’entiers compris entre 0 et $n - 1$ strictement croissantes (au sens usuel) est fini (de cardinal $2^n - 1$). Ainsi, il existe un élément minimal $(k, \mathbf{l}, \mathbf{V}, \mathbf{L})$ dans \mathcal{W}_0 pour l’ordre introduit précédemment, c’est-à-dire satisfaisant

$$\forall (k', \mathbf{l}', \mathbf{V}', \mathbf{L}') \in \mathcal{W}_0, \quad (\dim V_i)_{0 \leq i \leq k} \preceq (\dim V'_i)_{0 \leq i \leq k'}.$$

Nous allons appliquer le théorème 3.12 à $\alpha^{l_1 \cdots l_k}$, 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 (4.5),

$$(4.8) \quad E \geq (C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k})))^\delta \geq \left(\frac{C_0}{(\log C_0)^2} \log(3\omega_{\mathbb{L}}(\alpha)) \right)^{\delta_{k+1}} = E_{k+1}.$$

Vérifions que les hypothèses du théorème 3.12 sont satisfaites. On a

$$h(\alpha^{l_1 \cdots l_k}) = l_1 \cdots l_k h(\alpha)$$

et, par l’inégalité (4.4),

$$\omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k}) \leq c_{15} \omega_{\mathbb{L}}(\alpha) (\log(3\omega_{\mathbb{L}}(\alpha)))^{|r_{\mathbb{I}}|}.$$

Donc par l’hypothèse faite sur la hauteur de α ,

$$\begin{aligned} h(\alpha^{l_1 \cdots l_k}) \omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k}) &\leq l_1 \cdots l_k h(\alpha) c_{15} \omega_{\mathbb{L}}(\alpha) (\log(3\omega_{\mathbb{L}}(\alpha)))^{|r_{\mathbb{I}}|} \\ &\leq h(\alpha) \omega_{\mathbb{L}}(\alpha) \left(\prod_{i \in r_{\mathbb{I}}} l_i (c_{15} \log(3\omega_{\mathbb{L}}(\alpha))) \right) \prod_{i \in r_{\mathbb{II}}} l_i \\ &\leq h(\alpha) \omega_{\mathbb{L}}(\alpha) \left(\prod_{i \in r_{\mathbb{I}}} P_i (c_{15} \log(3\omega_{\mathbb{L}}(\alpha))) \right) \prod_{i \in r_{\mathbb{II}}} L_i \\ &\leq h(\alpha) \omega_{\mathbb{L}}(\alpha) \prod_{i=1}^k L_i \\ &\leq (C_0 (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{-e} \end{aligned}$$

avec

$$\begin{aligned} e &= 2n((n+1)! - 1) \sum_{j=1}^n \nu_j + 2n(\delta_1 + 1) - 1 - 2n((n+1)! - 1) \sum_{j=1}^k \nu_j \\ &= 2n((n+1)! - 1) \sum_{j=k+1}^n \nu_j + 2n(\delta_1 + 1) - 1 \\ &\geq 2n((n+1)! - 1) \nu_{k+1} + 2n(\delta_{k+1} + 1) - 1 \\ &\geq 2n((n+1)! - 1)(\rho + 1)(\delta_{k+1} + 1) + 2n(\delta_{k+1} + 1) - 1. \end{aligned}$$

D’où ⁽⁴⁾, par l’inégalité (4.5),

$$h(\alpha^{l_1 \cdots l_k}) \omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k}) \leq (C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k})))^{-e}.$$

⁽⁴⁾ C’est ici que s’est glissée l’erreur dans [2] (resp. [4]) : les auteurs ont une majoration en fonction de $\delta(\alpha)$ (resp. w_*) à la place de $\delta(\alpha^{l_1 \cdots l_k})$ (resp. $[K : \mathbb{Q}] w_K(\alpha^{l_1 \cdots l_k})$).

De plus, il n'existe pas de sous-variété de torsion B contenant $\alpha^{l_1 \cdots l_k}$ qui satisfait la majoration (3.15). En effet, si tel était le cas, il existerait B' , sous-variété de torsion contenant α , composante irréductible de $[l_1 \cdots l_k]^{-1}B$, telle que (avec les inégalités (4.4), (4.5) et l'égalité (4.2))

$$\begin{aligned} \deg(B')^{1/\text{codim}(B')} &\leq \left((l_1 \cdots l_k)^{\text{codim}(B)} \deg(B) \right)^{1/\text{codim}(B')} \\ &\leq L_1 \cdots L_k \deg(B)^{1/\text{codim}(B)} \\ &\leq L_1 \cdots L_k \omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k}) (C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k})))^{2n\nu_{k+1}(n+1)!} \\ &\leq \omega_{\mathbb{L}}(\alpha) (C_0 (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n \cdot (n+1)! \sum_{j=1}^n \nu_j + n - 1}, \end{aligned}$$

ce qui contredirait l'hypothèse (4.7).

Considérons la variété V_k . On a

$$\deg V_k \leq (L_{k+1} \cdots L_n \omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k}))^{\text{codim} V_k},$$

ce qui entraîne⁽⁵⁾ par le choix des paramètres et l'inégalité (4.5)

$$\log \deg V_k \leq c_{18} (\log C_0) \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k})) \leq C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \cdots l_k})),$$

de sorte que toutes les hypothèses du théorème 3.12 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 \mathbb{L}_{k+1} le corps $(\mathbb{L}_k)_{(l_{k+1})}$ (resp. \mathbb{L}_k) et Z une hypersurface définie sur \mathbb{L}_{k+1} contenant $\alpha^{l_1 \cdots l_{k+1}}$ de degré minimal : $\deg(Z) = \omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \cdots l_{k+1}})$.

Nous allons maintenant montrer qu'il existe un entier $k' \in \llbracket 0, k+1 \rrbracket$ et une sous-variété $Z_{k'}$ définie sur $\mathbb{L}_{k'}$ et $\mathbb{L}_{k'}$ -irréductible tels que :

1. $\deg(Z_{k'}) \leq l_{k'+1} \cdots l_{k+1} \omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \cdots l_{k+1}}) \deg(V_{k'})$;
2. $[l_{k'}]V_{k'-1} \subset Z_{k'}$;
3. $\text{codim}(Z_{k'}) = \text{codim}(V_{k'}) + 1$;

en posant les conventions $\text{codim}(V_{k+1}) = 0$, $\deg(V_{k+1}) = 1$, $V_{-1} = \{\alpha\}_{\mathbb{L}_0}$ et $l_0 = 1$. Remarquons que cela impliquera notamment

$$(4.9) \quad (\dim(V_0), \dots, \dim(V_{k'-1}), \dim(Z_{k'})) \prec (\dim(V_0), \dots, \dim(V_k)).$$

Nous distinguons deux cas.

Supposons dans un premier temps qu'il existe $i \in \llbracket 0, k \rrbracket$ tel que

$$[l_{i+1} \cdots l_{k+1}]V_i \not\subset Z.$$

Soit k' le plus petit entier vérifiant cette propriété. Considérons l'ensemble algébrique équidimensionnel $V_{k'} \cap [l_{k'+1} \cdots l_{k+1}]^{-1}Z$; la variété $V_{k'}$ et l'ensemble algébrique $[l_{k'+1} \cdots l_{k+1}]^{-1}Z$ étant définis respectivement sur $\mathbb{L}_{k'}$ et $\mathbb{L}_{k+1} \subset \mathbb{L}_{k'}$, leur intersection est elle aussi définie sur $\mathbb{L}_{k'}$. De plus, on a $[l_{k'}]V_{k'-1} \subset V_{k'}$ par hypothèse et $[l_{k'}]V_{k'-1}$ est contenu dans $[l_{k'+1} \cdots l_{k+1}]^{-1}Z$ par minimalité de k' , donc $[l_{k'}]V_{k'-1}$ est contenu dans $V_{k'} \cap [l_{k'+1} \cdots l_{k+1}]^{-1}Z$. Soit $Z_{k'}$ une des composantes $\mathbb{L}_{k'}$ -irréductibles

(5) Même remarque que la note (4).

de $V_{k'} \cap [l_{k'+1} \dots l_{k+1}]^{-1}Z$ contenant $[l_{k'}]V_{k'-1}$. La propriété 2 est ainsi assurée par la définition de $Z_{k'}$ et la propriété 1 par l'inégalité de Bézout :

$$\begin{aligned} \deg(Z_{k'}) &\leq \deg([l_{k'+1} \dots l_{k+1}]^{-1}Z) \deg(V_{k'}) \\ &\leq l_{k'+1} \dots l_{k+1} \omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \dots l_{k+1}}) \deg(V_{k'}). \end{aligned}$$

Enfin, on a $\text{codim}(Z_{k'}) = \text{codim}(V_{k'}) + 1$ (propriété 3) par construction.

Supposons dans un deuxième temps que $\forall i \in \llbracket 0, k \rrbracket, [l_{i+1} \dots l_{k+1}]V_i \subset Z$. Posons alors $k' = k + 1$ et $Z_{k+1} = Z$. Les propriétés 1, 2 et 3 sont alors trivialement vérifiées par la définition de Z_{k+1} .

Nous allons maintenant montrer

$$(k', (l_1, \dots, l_{k'}), (V_1, \dots, V_{k'-1}, Z_{k'}), (\mathbb{L}_1, \dots, \mathbb{L}_{k'})) \in \mathcal{W}$$

en distinguant 3 cas.

Cas 1. Si $k' = k + 1$ et que nous sommes dans la conclusion 1 du théorème 3.12, 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 (4.8)), ce qui assure la condition (a). De plus, $l_{k+1} \notin E_{\text{exc}}(V_k)$ et, en utilisant encore (4.5) et (4.8), on obtient

$$\begin{aligned} E_{k+1} \leq l_{k+1} &\leq (C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})))^{2n(1+\delta)(\rho+1)n.n!} \\ &\leq (c_{16}C_0 \log(3\omega_{\mathbb{L}}(\alpha)))^{2n\nu_{k+1}n.n!} \leq P_{k+1}. \end{aligned}$$

Donc les conditions (b) et (c) sont satisfaites. De même, grâce à l'inégalité (3.16), la condition (h) est vérifiée :

$$\omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \dots l_{k+1}}) = \omega_{\mathbb{L}_k(l_{k+1})}(\alpha^{l_1 \dots l_{k+1}}) \leq c_0 \omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}) \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})).$$

La variété Z_{k+1} est définie sur \mathbb{L}_{k+1} (condition (e)) et vérifie la propriété 2 qui correspond à la condition (f). Enfin, la condition (g) est assurée :

$$\deg(Z_{k+1}) = \omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \dots l_{k+1}}).$$

Donc l'indice $k + 1$ est de type I 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 2. Si $k' = k + 1$ et que nous sommes dans la conclusion 2 du théorème 3.12, nous allons montrer que $k + 1$ est un indice de type II. En effet, l_{k+1} est alors un entier tel que ⁽⁶⁾ (en utilisant (4.5))

$$\begin{aligned} l_{k+1} &\leq (C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})))^{2n(1+\delta)(\rho+1)((n+1)!-1)} \\ &\leq (c_{16}C_0 \log(3\omega_{\mathbb{L}}(\alpha)))^{2n\nu_{k+1}((n+1)!-1)} \leq L_{k+1} \end{aligned}$$

⁽⁶⁾ Même remarque que la note (4).

et $l_{k+1} \notin E_{\text{exc}}(V_k)$ de sorte que les conditions (a), (b) et (c) sont satisfaites. De même, à l'aide des inégalités (3.17) et (4.5), la condition (h) est vérifiée :

$$\begin{aligned} \omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \dots l_{k+1}}) &= \omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_{k+1}}) \\ &\leq \frac{\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})}{C_0^{1/2} (C_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})))^{2n(\delta_{k+1}+1)\rho}} \\ &\leq \frac{\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})}{C_0^{1/2} (C_0 (\log C_0)^{-2} \log(3\omega_{\mathbb{L}}(\alpha)))^{2n(\delta_{k+1}+1)\rho}} \\ &\leq \frac{\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})}{C_0^{1/2} (C_0 (\log C_0)^{-2} \log(3\omega_{\mathbb{L}}(\alpha)))^{2n((n+1)!-1) \sum_{j=k+2}^n \nu_j}} \\ &\leq \varepsilon_{k+1} \omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}). \end{aligned}$$

En effet, grâce à l'égalité (4.1) on a

$$((n+1)!-1) \sum_{j=k+2}^n \nu_j = \nu_{k+1} - (\delta_{k+1} + 1) = (\delta_{k+1} + 1)\rho.$$

Enfin, les conditions (d), (f) et (g) 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. ⁽⁷⁾ Si $k' < k+1$, on vérifie aisément que, par hypothèse sur $(k, l, \mathbf{V}, \mathbf{L})$ et grâce à la propriété 2 de $Z_{k'}$, nous sommes dans l'un des deux cas de la définition 4.1, sauf éventuellement pour les conditions (g) ou (d₀). Posons $\theta = 1$ si nous sommes dans la première conclusion du théorème 3.12 et $\theta = 0$ sinon. On a alors

$$\omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \dots l_{k+1}}) \leq \omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}) (c_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})))^\theta.$$

Donc, en utilisant la relation sur le degré de $Z_{k'}$ (propriété 1) et l'inégalité (4.5)

$$\begin{aligned} \deg(Z_{k'}) &\leq l_{k'+1} \dots l_{k+1} \omega_{\mathbb{L}_{k+1}}(\alpha^{l_1 \dots l_{k+1}}) \deg(V_{k'}) \\ &\leq l_{k'+1} \dots l_{k+1} \omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}) (c_0 \log(3\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k})))^\theta \deg(V_{k'}). \\ &\leq l_{k'+1} \dots l_{k+1} \omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}) (c_0 c_{16} \log(3\omega_{\mathbb{L}}(\alpha)))^\theta \deg(V_{k'}). \end{aligned}$$

De plus, par un argument similaire à celui de la démonstration du lemme 4.2, on montre

$$\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}) \leq c_{19} \omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}}) (\log(3\omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}})))^{|r_{\mathbb{I}} \cap \llbracket k'+1, k \rrbracket|}$$

et de nouveau avec l'inégalité (4.5)

$$\omega_{\mathbb{L}_k}(\alpha^{l_1 \dots l_k}) \leq c_{20} \omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}}) (\log(3\omega_{\mathbb{L}}(\alpha)))^{|r_{\mathbb{I}} \cap \llbracket k'+1, k \rrbracket|}.$$

⁽⁷⁾ Remarquons que si $n = 1$, on a nécessairement $k' = k + 1 = 1$, donc ce cas ne peut pas se produire.

D'où, en posant $A_{k'} = \deg(Z_{k'}) (\omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}}) \deg(V_{k'}))^{-1}$, on a

$$\begin{aligned} A_{k'} &\leq c_{20} l_{k'+1} \dots l_{k+1} (\log(3\omega_{\mathbb{L}}(\alpha)))^{|\Gamma \cap \llbracket k'+1, k \rrbracket|} (c_0 c_{16} \log(3\omega_{\mathbb{L}}(\alpha)))^\theta \\ &\leq l_{k+1} (c_0 c_{16} \log(3\omega_{\mathbb{L}}(\alpha)))^\theta \prod_{\substack{i=k'+1 \\ i \in \Gamma}}^k c_{20} l_i \log(3\omega_{\mathbb{L}}(\alpha)) \prod_{\substack{i=k'+1 \\ i \in \Gamma}}^k l_i \\ &\leq L_{k+1} \prod_{\substack{i=k'+1 \\ i \in \Gamma}}^k L_i \prod_{\substack{i=k'+1 \\ i \in \Gamma}}^k L_i \leq \prod_{i=k'+1}^{k+1} L_i. \end{aligned}$$

Enfin, la relation sur la codimension de $Z_{k'}$ (propriété 3) et la majoration du degré de $V_{k'}$ (condition (g) ou (d₀) de la définition 4.1) donnent

$$\begin{aligned} \deg(Z_{k'}) &\leq L_{k'+1} \dots L_{k+1} \omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}}) (L_{k'+1} \dots L_n \omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}}))^{\text{codim}(V_{k'})} \\ &\leq (L_{k'+1} \dots L_n \omega_{\mathbb{L}_{k'}}(\alpha^{l_1 \dots l_{k'}}))^{\text{codim}(Z_{k'})}, \end{aligned}$$

ce qui montre que la condition (g) ou (d₀) 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 (4.9)) 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. □

5. Démonstration des théorèmes principaux

Nous allons maintenant montrer les théorèmes 1.5 et 1.6 par récurrence sur n , la dimension du tore. L'initialisation de la récurrence est contenue dans la démonstration, dans la mesure où l'hypothèse de récurrence n'est invoquée que dans le cas où $n \geq 2$.

Nous commençons par montrer que, si la hauteur de α est « petite » et que α n'appartient pas à une sous-variété de torsion de petit degré, alors nous pouvons minorer l'indice d'obstruction de α sur \mathbb{L} en fonction de la racine n -ième du degré $[\mathbb{L}(\alpha) : \mathbb{L}]$. Ainsi, il suffira d'obtenir une minoration de la hauteur de α en fonction de ce degré pour conclure.

5.1. Minoration de l'indice d'obstruction

Par souci de clarté, nous commençons par estimer les quantités suivantes :

$$\begin{aligned} &2n((n+1)! - 1) \sum_{j=1}^n \nu_j + 2n(\delta_1 + 1) - 1 \\ &= 2n((n+1)! - 1)\nu_1 + 2n\nu_1 - 1 \\ &= 2n(n+1)!(1+n) (((n+1)! - 1)(1+2n^2) + 1)^{n-1} - 1 \\ &\leq 2(n+1)^2(n+1)! ((n+1)!2(n+1)^2)^{n-1} \\ &\leq (2(n+1)^2(n+1)!)^n \end{aligned}$$

et

$$2n \cdot (n + 1)! \sum_{j=1}^n \nu_j + n - 1 \leq 4n((n + 1)! - 1) \sum_{j=1}^n \nu_j \leq 2(2(n + 1)^2(n + 1)!)^n.$$

On pose alors $\tilde{\kappa}(n) = (2(n + 1)^2(n + 1)!)^n$ et $\tilde{\mu}(n) = 4(n - 1)!(\tilde{\kappa}(n) + 2\tilde{\kappa}(n - 1))$ (avec $\tilde{\kappa}(0) = 0$).

THÉORÈME 5.1. – *Supposons qu'il n'existe pas de sous-variété de torsion B contenant α telle que*

$$(5.1) \quad \deg(B)^{1/\text{codim}(B)} \leq \omega_{\mathbb{L}}(\alpha)^{n_1(n)} (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{\tilde{\mu}(n)}$$

et que l'on ait

$$h(\alpha) < \omega_{\mathbb{L}}(\alpha)^{-1} \left((C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2\tilde{\kappa}(n)} \right)^{-1}.$$

Alors on a

$$[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n} \leq \omega_{\mathbb{L}}(\alpha) (C_0(\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{\tilde{\kappa}(n)}$$

et il existe un nombre premier p ramifié dans \mathbb{L} n'appartenant pas à $E_{\text{exc}}(\{\alpha\}_{\mathbb{L}})$ tel que

$$\mathbb{L}_{(p)}(\alpha^p) \subsetneq \mathbb{L}(\alpha^p).$$

Démonstration. – Le point α satisfait les hypothèses du théorème 4.5, ainsi $\mathcal{W} \setminus \mathcal{W}_0$ n'est pas vide. Soient $(k, \mathbf{l}, \mathbf{V}, \mathbf{L}) \in \mathcal{W} \setminus \mathcal{W}_0$ et $i \in \llbracket 1, k \rrbracket$ tel que V_i et V_{i-1} soient de même dimension. On a $[l_i]V_{i-1} \subset V_i$ avec $l_i \notin E_{\text{exc}}(V_{i-1})$. Nous allons montrer que nécessairement i est de type I et que V_{i-1} est une réunion de translatsés de sous-tores.

En effet, si i est de type I et que V_{i-1} n'est pas une réunion de translatsés de sous-tores, on a, par la proposition 2.2,

$$\deg([l_i]V_{i-1}) \geq l_i \deg V_{i-1},$$

car $l_i \notin E_{\text{exc}}(V_{i-1})$. 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 $\alpha^{l_1 \cdots l_{i-1}}$ d'où, par le lemme 2.4,

$$\omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) \leq n \deg(V_{i-1})^{1/\text{codim}(V_{i-1})}.$$

En combinant ces inégalités avec celles de la définition 4.1, on obtient

$$\begin{aligned} \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) &\leq n (l_i^{-1} \deg(V_i))^{1/\text{codim}(V_i)} \leq n E_i^{-1/n} L_{i+1} \cdots L_n \omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}) \\ &\leq n E_i^{-1/n} L_{i+1} \cdots L_n \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) c_0 \log(3\omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}})) \\ &\leq c_0 c_{16} n E_i^{-1/n} L_{i+1} \cdots L_n \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) \log(3\omega_{\mathbb{L}}(\alpha)). \end{aligned}$$

On aboutit alors à une contradiction :

$$\begin{aligned} 1 &\leq c_0 c_{16} n (C_0 \log(3\omega))^{-\delta_i/n + 2n((n+1)!-1)} \sum_{j=i+1}^n \nu_j \\ &\quad \times (\log C_0)^{2\delta_i/n + 2n((n+1)!-1)} \sum_{j=i+1}^n \nu_j \log(3\omega_{\mathbb{L}}(\alpha)) \\ &\leq c_0 c_{16} n (C_0)^{-1} (\log C_0)^{2\delta_i/n + 2n((n+1)!-1)} \sum_{j=i+1}^n \nu_j. \end{aligned}$$

De même, si i est de type II, on a

$$\deg([l_i]V_{i-1}) \geq \deg V_{i-1},$$

car $l_i \notin E_{\text{exc}}(V_{i-1})$. 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 $\alpha^{l_1 \cdots l_{i-1}}$, d'où

$$\omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) \leq n \deg(V_{i-1})^{1/\text{codim}(V_{i-1})}.$$

En combinant ces inégalités avec celles de la définition 4.1, on obtient

$$\begin{aligned} \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}) &\leq n (\deg(V_i))^{1/\text{codim}(V_i)} \\ &\leq n L_{i+1} \cdots L_n \omega_{\mathbb{L}_i}(\alpha^{l_1 \cdots l_i}) \\ &\leq n L_{i+1} \cdots L_n \varepsilon_i \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}). \end{aligned}$$

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 de nouveau une contradiction.

Ainsi i est de type I et V_{i-1} est une réunion de translatés de sous-tores ; écrivons

$$V_{i-1} = \bigcup_{\tau \in \text{Gal}(\mathbb{Q}/\mathbb{L}_{i-1})} \tau(\alpha^{l_1 \cdots l_{i-1}} H) = \bigcup_{k=1}^d \alpha_k^{l_1 \cdots l_{i-1}} H,$$

où H est un sous-tore de \mathbb{G}_m^n et les $\alpha_k, k \in [1, d]$, sont des conjugués de α au-dessus de \mathbb{L}_{i-1} tels que $\alpha_{k_1}^{l_1 \cdots l_{i-1}}$ et $\alpha_{k_2}^{l_1 \cdots l_{i-1}}$ sont distincts modulo H dès que $k_1 \neq k_2$ (en d'autres termes, $(\alpha_{k_1} \alpha_{k_2}^{-1})^{l_1 \cdots l_{i-1}} \notin H$).

Nous allons montrer que H est nécessairement le sous-tore trivial. Si $n = 1$, c'est immédiat. Sinon, raisonnons par l'absurde : supposons que le sous-tore H est de dimension strictement positive et considérons l'application

$$\begin{aligned} \phi : \mathbb{G}_m^n &\longrightarrow \mathbb{G}_m^n / H \simeq \mathbb{G}_m^r \\ \mathbf{x} &\longmapsto (\mathbf{x}^{e_1}, \dots, \mathbf{x}^{e_r}) \end{aligned}$$

où r est la codimension de H et $(e_1, \dots, e_r) \in (\mathbb{Z}^n)^r$ engendre le réseau Λ associé au sous-tore H . D'après le paragraphe 4 de [15], on dispose de l'inégalité

$$\binom{n}{r}^{-1/2} \text{Vol}(\Lambda) \leq \deg(H)$$

où $\text{Vol}(\Lambda)$ désigne le volume de $(\Lambda \otimes \mathbb{R})/\Lambda$. En appliquant le théorème des minima successifs de Minkowski respectivement à la norme du sup (voir page 218 de [7]) dont le volume de la boule unité dans $(\Lambda \otimes \mathbb{R})$ est au moins 2^r (voir [20]) et en utilisant le lemme 8 page 135 de [7], on peut choisir les e_j de sorte que

$$(5.2) \quad \prod_{j=1}^r \|e_j\|_\infty \leq r! \text{Vol}(\Lambda) \leq r! \binom{n}{r}^{1/2} \deg(H) \leq n! \deg(H).$$

Notons β l'image de $\alpha^{l_1 \cdots l_{i-1}}$ par le morphisme ϕ . Le nombre de composantes géométriquement irréductibles de V_{i-1} vaut alors $d = [\mathbb{L}_{i-1}(\beta) : \mathbb{L}_{i-1}] \geq [\mathbb{Q}^{\text{ab}}(\beta) : \mathbb{Q}^{\text{ab}}]$. Étant donné

que $r < n$, nous pouvons appliquer, par hypothèse de récurrence, le théorème 1.6 à $\beta \in \mathbb{G}_m^r$. Ainsi, on a

$$(5.3) \quad \prod_{j=1}^r h(\beta_j) \geq (c_2(r)d(\log 3d)^{\kappa_2(r)})^{-1}$$

ou il existe une variété de torsion $B \subset \mathbb{G}_m^r$ contenant β telle que

$$(5.4) \quad (\deg B)^{1/\text{codim}(B)} \leq c_2(r)d^{\eta_2(r)}(\log(3d))^{\mu(r)}.$$

Or, en utilisant les inégalités (5.2), (4.4) et (g) de la définition (4.1), on dispose de la majoration

$$\begin{aligned} \prod_{j=1}^r h(\beta_j) &\leq \prod_{j=1}^r (\|e_j\|_\infty h(\alpha^{l_1 \cdots l_{i-1}})) \\ &\leq n! \deg(H) h(\alpha^{l_1 \cdots l_{i-1}})^r \\ &\leq n! \frac{\deg V_{i-1}}{d} (l_1 \cdots l_{i-1} h(\alpha))^r \\ &\leq \frac{n!}{d} (c_{15} h(\alpha) \omega_{\mathbb{L}}(\alpha) (\log(3\omega_{\mathbb{L}}(\alpha)))^{n-1} \prod_{j=1}^n L_j)^r \\ &\leq \frac{n!}{d} (C_0 (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{r(-2\tilde{\kappa}(n) + n - 1 + 2n((n+1)! - 1) \sum_{j=1}^n \nu_j)}. \end{aligned}$$

Dans la mesure où $\log(3d) \leq \log(3 \deg V_{i-1}) \leq c_{21} (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha))$ et

$$\kappa_2(r) = 3r\tilde{\kappa}(r) \leq 3r\tilde{\kappa}(n-1) \leq r\tilde{\kappa}(n) < r \left(2\tilde{\kappa}(n) - (n-1) - 2n((n+1)! - 1) \sum_{j=1}^n \nu_j \right),$$

cette dernière majoration contredit l'inégalité (5.3). De même, supposons qu'il existe une sous-variété de torsion $B \subset \mathbb{G}_m^r$ contenant β vérifiant (5.4); il existe un point de torsion ζ et un sous-tore \tilde{H} de \mathbb{G}_m^r de même dimension et de degré inférieur à B tel que $\zeta\beta$ appartienne à \tilde{H} . En utilisant comme précédemment le théorème de Minkowski, on peut exhiber un caractère non trivial de \mathbb{G}_m^r , $\chi = \prod_{k=1}^r X_k^{s_k}$, trivial sur \tilde{H} et tel que $\max\{|s_k|, k \in \llbracket 1, r \rrbracket\} \leq r^{1/2} (\deg \tilde{H})^{1/\text{codim}(\tilde{H})}$. Alors le caractère $\tilde{\chi}$ de \mathbb{G}_m^n défini par $\tilde{\chi} = \prod_{j=1}^n X_j^{l_1 \cdots l_{i-1} \sum_{k=1}^r s_k e_{k,j}}$ (où $e_{k,j}$ représente la j -ième composante de e_k) est non trivial (car les $e_k, k \in \llbracket 1, r \rrbracket$, sont linéairement indépendants) et vérifie

$$\tilde{\chi}(\alpha) = \prod_{j=1}^n \alpha_j^{l_1 \cdots l_{i-1} \sum_{k=1}^r s_k e_{k,j}} = \prod_{k=1}^r \beta_k^{s_k} = \chi(\beta) = \chi(\zeta^{-1}) = \zeta$$

où ζ est une racine de l'unité. Ainsi α est contenu dans une hypersurface de torsion \tilde{B} telle que

$$\begin{aligned} \deg \tilde{B} &\leq n \max_{j \in [1, n]} \{ |l_1 \cdots l_{i-1} \sum_{k=1}^r s_k e_{k,j}| \} \\ &\leq n r l_1 \cdots l_{i-1} \max_{k \in [1, r]} \{ |s_k| \} \max_{k \in [1, r]} \|e_k\|_\infty \\ &\leq n r L_1 \cdots L_{i-1} r^{1/2} (\deg B)^{1/\text{codim}(B)} n! \deg(H) \\ &\leq c_{22} L_1 \cdots L_{i-1} d^{\eta_2(r)} (\log(3d))^{\mu(r)} \deg(H) \\ &\leq c_{22} L_1 \cdots L_{i-1} (\deg(V_{i-1}))^{\eta_2(r)} (\log(3d))^{\mu(r)} \\ &\leq c_{22} (L_1 \cdots L_n \omega_{\mathbb{L}_{i-1}}(\alpha^{l_1 \cdots l_{i-1}}))^{r \eta_2(r)} (\log(3d))^{\mu(r)} \\ &\leq \omega_{\mathbb{L}}(\alpha)^{r \eta_2(r)} (C_0 (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{\mu(r) + r \eta_2(r) (2n((n+1)! - 1) \sum_{j=1}^n \nu_j + n)} \end{aligned}$$

ce qui contredit l'hypothèse (5.1) car

$$r \eta_2(r) \leq (n - 1) \eta_2(n - 1) = \eta_1(n)$$

et

$$\begin{aligned} \mu(r) + r \eta_2(r) (2n((n + 1)! - 1) \sum_{j=1}^n \nu_j + n) &\leq \mu(n - 1) + (n - 1) \eta_2(n - 1) \tilde{\kappa}(n) \\ &\leq 8(n - 1)! \tilde{\kappa}(n - 1) + 4(n - 1)! \tilde{\kappa}(n) \leq \tilde{\mu}(n). \end{aligned}$$

Ainsi, le sous-tore H est trivial et la sous-variété V_{i-1} est de dimension 0. Nous pouvons alors supposer $i = 1$. Dans ce cas, la variété V_0 est la réunion des conjugués au-dessus de $\mathbb{L}_0 = \mathbb{L}$, d'où $\deg V_0 = [\mathbb{L}(\alpha) : \mathbb{L}]$ et, par la propriété (c_0) de la définition 4.1,

$$\begin{aligned} [\mathbb{L}(\alpha) : \mathbb{L}]^{1/n} &\leq \omega_{\mathbb{L}}(\alpha) (C_0 (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{2n((n+1)! - 1) \sum_{j=1}^n \nu_j} \\ &\leq \omega_{\mathbb{L}}(\alpha) (C_0 (\log C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{\tilde{\kappa}(n)}. \end{aligned}$$

De même, la variété V_1 est la réunion des conjugués de α^{l_1} au-dessus de $\mathbb{L}_1 = \mathbb{L}_{(l_1)}$ et $\deg(V_1) = [\mathbb{L}_1(\alpha^{l_1}) : \mathbb{L}_1]$. Or, si l'on suppose $\mathbb{L}_1(\alpha^{l_1}) = \mathbb{L}(\alpha^{l_1})$ on a, avec (2.4) et les hypothèses 1(a), 1(b) et 1(c) de la définition 4.1,

$$\deg(V_1) = [\mathbb{L}(\alpha^{l_1}) : \mathbb{L}] [\mathbb{L} : \mathbb{L}_1] \geq [\mathbb{L}(\alpha^{l_1}) : \mathbb{L}] \min(l_1, e_{l_1}(\mathbb{L})) \geq [\mathbb{L}(\alpha) : \mathbb{L}] E_1.$$

Finalement, en combinant cette inégalité avec les inégalités 1(g) et 1(h) de la définition 4.1, on obtient

$$\begin{aligned} \omega_{\mathbb{L}}(\alpha) &\leq n [\mathbb{L}(\alpha) : \mathbb{L}]^{1/n} \leq n (E_1^{-1} \deg(V_1))^{1/n} \\ &\leq c_0 n E_1^{-1/n} L_2 \cdots L_n \omega_{\mathbb{L}}(\alpha) \log(3\omega_{\mathbb{L}}(\alpha)), \end{aligned}$$

ce qui constitue une contradiction (identique à la première rencontrée dans cette démonstration). En posant $p = l_1$, le théorème est entièrement démontré. \square

5.2. Minoration de la hauteur en fonction du degré

Nous allons dans cette partie démontrer le théorème suivant :

THÉORÈME 5.2. – Il existe un réel $\tilde{c}(n)$ strictement positif ne dépendant que de n tel que la proposition suivante soit vraie. Soient $\alpha \in \mathbb{G}_m^n(\mathbb{Q})$ et \mathbb{L} une extension abélienne de \mathbb{Q} . S’il n’existe pas de sous-variété de torsion B contenant α telle que

$$(5.5) \quad \deg(B)^{1/\text{codim}(B)} \leq [\mathbb{L}(\alpha) : \mathbb{L}]^{\eta_1(n)/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{\tilde{\mu}(n)}$$

alors

$$h(\alpha) \geq [\mathbb{L}(\alpha) : \mathbb{L}]^{-1/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{-2\tilde{\kappa}(n)}.$$

À la manière de [6], nous commençons par établir une réduction sur le couple (α, \mathbb{L}) . Pour cela, nous devons établir un lemme préliminaire.

LEMME 5.3. – Soit α un point de $\mathbb{G}_m^n(\bar{\mathbb{Q}})$. Soient K un corps de nombres, p un nombre premier et ζ_p une racine primitive p -ième de l’unité. Alors l’extension

$$K(\alpha^p, \zeta_p) \subseteq K(\alpha, \zeta_p)$$

est abélienne de degré une puissance de p . De plus, si $K(\alpha, \zeta_p) = K(\alpha^p, \zeta_p)$, il existe $\xi \in \ker[p]$ tel que $K(\xi\alpha) = K(\alpha^p)$.

Démonstration. – Soit $\tau \in \text{Gal}(\bar{\mathbb{Q}}/K(\alpha^p, \zeta_p))$. On a $\tau\alpha^p = \alpha^p$ donc il existe $\xi \in \ker[p]$ tel que $\tau(\alpha) = \xi\alpha$ et $\tau\alpha$ appartient à $K(\alpha, \zeta_p)$. L’extension $K(\alpha^p, \zeta_p) \subseteq K(\alpha, \zeta_p)$ est donc galoisienne. D’autre part, si l’on considère l’application

$$\begin{aligned} \phi : \text{Gal}(K(\alpha, \zeta_p)/K(\alpha^p, \zeta_p)) &\longrightarrow \ker[p] \\ \tau &\longmapsto \xi \end{aligned}$$

on vérifie aisément que ϕ est un morphisme injectif. Ainsi $\text{Gal}(K(\alpha, \zeta_p)/K(\alpha^p, \zeta_p))$ 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,

$$K(\alpha^p) \subseteq K(\alpha) \subseteq K(\alpha, \zeta_p) = K(\alpha^p, \zeta_p).$$

Si $K(\alpha) = K(\alpha^p)$ le résultat est trivial. Supposons donc que $K(\alpha^p) \subsetneq K(\alpha)$. Soit σ un générateur du groupe cyclique

$$G = \text{Gal}(K(\alpha^p, \zeta_p)/K(\alpha^p))$$

et notons $\tilde{\sigma}$ un de ses prolongements à $\bar{\mathbb{Q}}$. Comme on a $\tilde{\sigma}(\alpha^p) = \alpha^p$, il existe $\xi \in \ker[p]$ tel que $\tilde{\sigma}(\alpha) = \xi\alpha$.

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

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

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

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

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

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

5.2.1. *Réduction.* – Si p est un nombre premier, on note $\tilde{e}_p(\mathbb{L})$ la puissance maximale de p divisant l'entier m minimal tel que $\mathbb{L} \subset \mathbb{Q}(\zeta_m)$. On définit également

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

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

Pour démontrer le théorème 5.2, on raisonne par l'absurde. Supposons donc qu'il existe $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ et \mathbb{L} une extension abélienne de \mathbb{Q} tels que le théorème 5.2 soit faux :

$$(5.6) \quad h(\alpha) < \left([\mathbb{L}(\alpha) : \mathbb{L}]^{1/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{2\tilde{\kappa}(n)} \right)^{-1}$$

et il n'existe pas de sous-variété de torsion B contenant α telle que

$$(5.7) \quad (\deg B)^{1/\text{codim} B} \leq [\mathbb{L}(\alpha) : \mathbb{L}]^{\eta_1(n)/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{\tilde{\mu}(n)}.$$

Nous pouvons supposer de plus que le degré $d = [\mathbb{L}(\alpha) : \mathbb{L}]$ est minimal dans (5.6) et (5.7) : pour tout point $\alpha' \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ et toute extension abélienne \mathbb{L}' de \mathbb{Q} vérifiant $[\mathbb{L}'(\alpha') : \mathbb{L}'] < d$, la conclusion du théorème 5.2 est vérifiée.

En particulier, ceci implique que pour tout $\zeta \in (\mathbb{G}_m^n(\bar{\mathbb{Q}}))_{\text{tors}}$ et toute extension abélienne \mathbb{L}' de \mathbb{Q} , on a

$$(5.8) \quad [\mathbb{L}'(\zeta\alpha) : \mathbb{L}'] \geq d.$$

En effet, si $[\mathbb{L}'(\zeta\alpha) : \mathbb{L}'] < d$, alors par minimalité de d , on a

$$(5.9) \quad h(\zeta\alpha) \geq \left([\mathbb{L}(\alpha) : \mathbb{L}]^{1/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{2\tilde{\kappa}(n)} \right)^{-1}$$

ou il existe une sous-variété de torsion \tilde{B} contenant $\zeta\alpha$ telle que

$$(5.10) \quad (\deg \tilde{B})^{1/\text{codim} \tilde{B}} < [\mathbb{L}(\alpha) : \mathbb{L}]^{\eta_1(n)/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{\tilde{\mu}(n)}.$$

Cependant, on a $h(\alpha) = h(\zeta\alpha)$ donc l'inégalité (5.9) contredit (5.6). De même, l'inégalité (5.10) est impossible car la variété $B = \zeta^{-1}\tilde{B}$ est une variété de torsion de même degré et même dimension que \tilde{B} et contient α , ce qui contredit (5.7).

Enfin, soit \mathcal{A} l'ensemble des extensions abéliennes \mathbb{L}' de \mathbb{Q} telles qu'il existe $\zeta \in (\mathbb{G}_m^n(\bar{\mathbb{Q}}))_{\text{tors}}$ vérifiant $[\mathbb{L}'(\zeta\alpha) : \mathbb{L}'] = d$. Posons

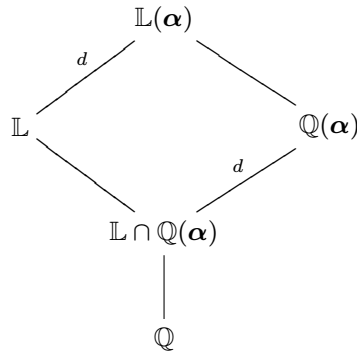
$$\tilde{e} = \min_{\mathbb{L} \in \mathcal{A}} \tilde{e}(\mathbb{L}).$$

Quitte à remplacer α par $\zeta\alpha$ pour un certain $\zeta \in (\mathbb{G}_m^n(\bar{\mathbb{Q}}))_{\text{tors}}$ et \mathbb{L} par $\mathbb{L}' \in \mathcal{A}$, nous pouvons supposer que \mathbb{L} vérifie les deux conditions suivantes :

$$(5.11) \quad [\mathbb{L}(\alpha) : \mathbb{L}] = d,$$

$$(5.12) \quad \tilde{e}(\mathbb{L}) = \tilde{e}.$$

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



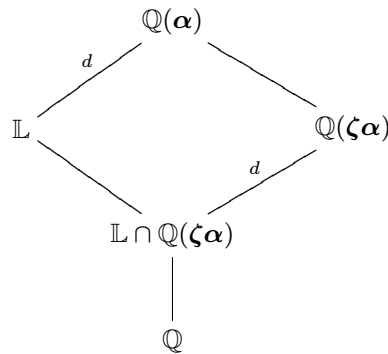
Étant donné que $\mathbb{L} \cap \mathbb{Q}(\alpha)$ est une extension abélienne de \mathbb{Q} et que $\tilde{e}(\mathbb{L} \cap \mathbb{Q}(\alpha)) \leq \tilde{e}(\mathbb{L}) = \tilde{e}$, on a $\tilde{e}(\mathbb{L} \cap \mathbb{Q}(\alpha)) = \tilde{e}$. Cela nous permet de supposer, quitte à remplacer \mathbb{L} par $\mathbb{L} \cap \mathbb{Q}(\alpha)$, que $\mathbb{L} \subseteq \mathbb{Q}(\alpha)$, c'est-à-dire

$$(5.13) \quad \mathbb{Q}(\alpha) = \mathbb{L}(\alpha).$$

Remarquons enfin que l'on peut également supposer

$$(5.14) \quad \forall \zeta \in (\mathbb{G}_m^n(\bar{\mathbb{Q}}))_{\text{tors}}, \quad \mathbb{Q}(\zeta\alpha) \subseteq \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\zeta\alpha) = \mathbb{Q}(\alpha).$$

En effet, s'il existe ζ tel que $\mathbb{Q}(\zeta\alpha) \subsetneq \mathbb{Q}(\alpha)$, nous avons $\mathbb{L}(\zeta\alpha) \subseteq \mathbb{L}(\alpha)$, ce qui implique nécessairement (par (5.8)) $\mathbb{L}(\zeta\alpha) = \mathbb{L}(\alpha) = \mathbb{Q}(\alpha)$. Nous avons ainsi le diagramme



Par le même argument, nous pouvons donc remplacer α par $\zeta\alpha$ et \mathbb{L} par $\mathbb{L} \cap \mathbb{Q}(\zeta\alpha)$. Nous pouvons itérer ce procédé, jusqu'à obtenir (5.14) (nombre d'itérations fini car le degré décroît strictement à chaque étape).

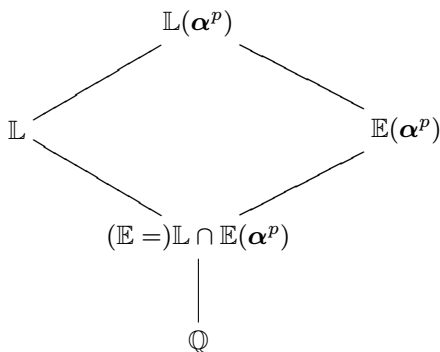
Ainsi, nous considérons désormais un point α et une extension abélienne \mathbb{L} de \mathbb{Q} contenue dans $\mathbb{Q}(\alpha)$ qui satisfont (5.6), (5.7), (5.8), (5.11), (5.12), (5.13) et (5.14).

5.2.2. *Lemme auxiliaire.* – Le but de la précédente réduction est de montrer le lemme suivant.

LEMME 5.4. – Soit p un nombre premier ramifié dans \mathbb{L} n'appartenant pas à $E_{\text{exc}}(\{\alpha\}_{\mathbb{L}})$. On a

$$\mathbb{L}_{(p)}(\alpha^p) = \mathbb{L}(\alpha^p).$$

Démonstration. – Soit $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{L}_{(p)})$ tel que $\tau|_{\mathbb{L}} \neq \text{Id}$. Raisonnons par l'absurde : supposons $\tau\alpha^p = \alpha^p$. Ceci équivaut à dire que $\mathbb{Q}(\alpha^p)$ est stable sous l'action de τ . Notons \mathbb{E} le sous-corps de \mathbb{L} fixé par τ . On a alors $\mathbb{Q}(\alpha^p) \cap \mathbb{L} \subseteq \mathbb{E}$ donc $\mathbb{E}(\alpha^p) \cap \mathbb{L} = \mathbb{E}$. Par un argument galoisien, les « côtés » opposés du diagramme suivant ont même degré :



On en déduit

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

Or, le premier p n'appartient pas à $\mathbb{E}_{\text{exc}}(\{\alpha\}_{\mathbb{L}})$ donc $\mathbb{L}(\alpha^p) = \mathbb{L}(\alpha)$, ce qui donne avec l'égalité (5.13)

$$(5.15) \quad \mathbb{L}(\alpha^p) = \mathbb{L}(\alpha) = \mathbb{Q}(\alpha).$$

Ainsi $[\mathbb{Q}(\alpha) : \mathbb{E}(\alpha^p)] = [\mathbb{L} : \mathbb{E}]$. D'une part, comme $\mathbb{E} \subsetneq \mathbb{L}$ (sinon $\tau|_{\mathbb{L}} = \text{Id}$), on a $[\mathbb{L} : \mathbb{E}] > 1$. D'autre part, on a $\mathbb{L}_{(p)} \subset \mathbb{E}$, d'où l'encadrement

$$(5.16) \quad 2 \leq [\mathbb{Q}(\alpha) : \mathbb{E}(\alpha^p)] \leq p.$$

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 $\mathbb{Q}(\alpha, \zeta_p)/\mathbb{Q}(\alpha)$, $\mathbb{E}(\alpha^p, \zeta_p)/\mathbb{E}(\alpha^p)$ et $\mathbb{Q}(\alpha^p, \zeta_p)/\mathbb{Q}(\alpha^p)$ dont le degré divise $p - 1$. Remarquons que l'on a (voir (5.15))

$$\mathbb{Q}(\alpha^p, \zeta_p) \subseteq \mathbb{E}(\alpha^p, \zeta_p) \subseteq \mathbb{L}(\alpha^p, \zeta_p) = \mathbb{L}(\alpha, \zeta_p) = \mathbb{Q}(\alpha, \zeta_p).$$

Par ailleurs, par le lemme 5.3, l'extension $\mathbb{Q}(\alpha, \zeta_p)/\mathbb{Q}(\alpha^p, \zeta_p)$ est abélienne de degré une puissance de p . Il en est donc de même pour l'extension intermédiaire $\mathbb{Q}(\alpha, \zeta_p)/\mathbb{E}(\alpha^p, \zeta_p)$. Supposons $\mathbb{Q}(\alpha, \zeta_p) = \mathbb{E}(\alpha^p, \zeta_p)$. On a

$$\mathbb{E}(\alpha^p, \zeta_p) \subseteq \mathbb{E}(\alpha, \zeta_p) \subseteq \mathbb{L}(\alpha, \zeta_p) = \mathbb{Q}(\alpha, \zeta_p)$$

donc $\mathbb{E}(\alpha, \zeta_p) = \mathbb{E}(\alpha^p, \zeta_p)$. Le lemme 5.3 implique alors l'existence d'un élément $\zeta \in \ker[p]$ tel que $\mathbb{E}(\zeta\alpha) = \mathbb{E}(\alpha^p)$. Ainsi :

$$\mathbb{Q}(\zeta\alpha) \subseteq \mathbb{E}(\zeta\alpha) = \mathbb{E}(\alpha^p) \subseteq \mathbb{L}(\alpha^p) = \mathbb{L}(\alpha) = \mathbb{Q}(\alpha).$$

L'hypothèse (5.14) faite sur α implique que ces six corps sont égaux ; en particulier $\mathbb{Q}(\alpha) = \mathbb{E}(\alpha^p)$, ce qui est impossible d'après (5.16). Donc $[\mathbb{Q}(\alpha, \zeta_p) : \mathbb{E}(\alpha^p, \zeta_p)] = p^\alpha$, avec $\alpha \geq 1$. Ainsi p divise

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

Or $[\mathbb{Q}(\alpha, \zeta_p) : \mathbb{Q}(\alpha)]$ divise $p - 1$ donc, par le lemme de Gauss, p divise $[\mathbb{Q}(\alpha) : \mathbb{E}(\alpha^p)]$. L'encadrement (5.16) implique alors

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

On a ainsi montré que $[\mathbb{L} : \mathbb{E}] = [\mathbb{Q}(\alpha) : \mathbb{E}(\alpha^p)] = p$. On en déduit que $[\mathbb{L} : \mathbb{L}_{(p)}] = p$ et que p^2 divise m . 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 $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p}))$ induit par restriction un sous-groupe non trivial de $\text{Gal}(\mathbb{L}(\zeta_q)/\mathbb{Q})$, qui est nécessairement cyclique d'ordre p . Notons \mathbb{F} le corps fixé par ce sous-groupe et ρ un générateur de $\text{Gal}(\mathbb{L}(\zeta_q)/\mathbb{F})$. Alors $\mathbb{E} \subseteq \mathbb{F}$ et

$$(5.17) \quad \rho\zeta_q = \tilde{\zeta}_p\zeta_q$$

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

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

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

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

$$r : \text{Gal}(\mathbb{L}(\alpha, \zeta_q)/\mathbb{F}(\alpha^p)) \rightarrow \text{Gal}(\mathbb{L}(\zeta_q)/\mathbb{F})$$

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

$$\tilde{\rho}\alpha = \xi\alpha$$

et, par (5.17),

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

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

$$\tilde{\rho}(\zeta\alpha) = \tilde{\rho}(\zeta)\tilde{\rho}(\alpha) = (\tilde{\zeta}_p^{-\alpha_1}\zeta_q^{-\alpha_1}, \dots, \tilde{\zeta}_p^{-\alpha_n}\zeta_q^{-\alpha_n})\xi\alpha = \zeta\alpha.$$

Ainsi $\zeta\alpha$ est stable sous l'action de $\text{Gal}(\mathbb{L}(\alpha, \zeta_q)/\mathbb{F}(\alpha^p))$ donc $\mathbb{F}(\zeta\alpha) \subseteq \mathbb{F}(\alpha^p)$.

On en déduit

$$[\mathbb{F}(\zeta\alpha) : \mathbb{F}] \leq [\mathbb{F}(\alpha^p) : \mathbb{F}] \leq [\mathbb{E}(\alpha^p) : \mathbb{E}] = d.$$

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 (5.12) faite sur α , ce qui achève la démonstration du lemme. \square

5.2.3. *Démonstration du théorème 5.2.* – Nous pouvons maintenant passer à la démonstration proprement dite du théorème 5.2 :

Démonstration. – Par la réduction qui précède, on peut supposer que α vérifie le lemme 5.4. Posons $\tilde{c}(n) = n^2 C_0 \log C_0$ et supposons qu'il n'existe pas de sous-variété de torsion B contenant α vérifiant (5.5) et que l'on ait

$$h(\alpha) < [\mathbb{L}(\alpha) : \mathbb{L}]^{-1/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{-2\tilde{\kappa}(n)}.$$

Dans la mesure où l'on a $\omega_{\mathbb{L}}(\alpha) \leq n[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}$, le couple (α, \mathbb{L}) vérifie les hypothèses du théorème 5.1. La (seconde) conclusion de ce dernier est alors en contradiction avec le lemme 5.4. \square

5.3. Démonstration des résultats principaux

5.3.1. *Démonstration du théorème 1.5.* – Soit $c_1(n)$ un réel tel que $c_1(n) \geq (4n^2 C_0 \tilde{\kappa}(n) (\log(C_0))^2)^{\mu(n)}$. Soient $\alpha \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$ et \mathbb{L} une extension abélienne finie de \mathbb{Q} telle que $\omega_{\mathbb{L}}(\alpha) = \omega_{\mathbb{Q}^{\text{ab}}}(\alpha)$. Supposons que α ne soit pas contenu dans une variété de torsion vérifiant

$$(\deg B)^{1/\text{codim}(B)} \leq c_1(n) \omega_{\mathbb{L}}(\alpha)^{\eta_1(n)} (\log(3\omega_{\mathbb{L}}(\alpha)))^{\mu(n)}$$

et que l'on ait

$$h(\alpha) < \left(c_1(n) \omega_{\mathbb{L}}(\alpha) \log(3\omega_{\mathbb{L}}(\alpha)) \right)^{3\tilde{\kappa}(n)-1}.$$

Le couple (α, \mathbb{L}) vérifie alors les hypothèses du théorème 5.1. En particulier, on a

$$[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n} \leq \omega_{\mathbb{L}}(\alpha) (C_0 \log(C_0) \log(3\omega_{\mathbb{L}}(\alpha)))^{\tilde{\kappa}(n)}.$$

Ainsi, α n'est pas contenu dans une variété de torsion vérifiant (5.5) (par le choix de $c_1(n)$ et le fait que $\tilde{\kappa}(n)\eta_1(n) + \tilde{\mu}(n) \leq \mu(n)$). D'après le théorème 5.2, ceci implique

$$\begin{aligned} h(\alpha) &\geq [\mathbb{L}(\alpha) : \mathbb{L}]^{-1/n} \left(\tilde{c}(n) \log(3[\mathbb{L}(\alpha) : \mathbb{L}]^{1/n}) \right)^{-2\tilde{\kappa}(n)} \\ &\geq \omega_{\mathbb{L}}(\alpha)^{-1} \left((c_1(n) \log(3\omega_{\mathbb{L}}(\alpha)))^{3\tilde{\kappa}(n)-1} \right)^{-1}, \end{aligned}$$

ce qui contredit notre hypothèse et achève la démonstration du théorème 1.5.

5.3.2. *Démonstration du théorème 1.6.* – Nous suivons la preuve du théorème 1.6 de [2], en contrôlant le degré de la sous-variété de torsion. Posons $c_2(n) = (2n^2 c_1(n))^n$ et raisonnons par l'absurde en supposant qu'il n'existe pas de sous-variété de torsion B contenant α telle que

$$(5.18) \quad (\deg B)^{1/\text{codim}(B)} \leq c_2(n) [\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]^{\eta_2(n)} (\log(3[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]))^{\mu(n)}.$$

En particulier, aucune des coordonnées de α n'est une racine de l'unité. Soit $h = \min\{h(\alpha_1), \dots, h(\alpha_n)\}$; d'après le théorème 1.5 dans le cas $n = 1$, on a

$$(5.19) \quad h \geq \left(c_1(1) [\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}] (\log(3[\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]))^{\kappa_1(1)} \right)^{-1}$$

car $[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}] \geq [\mathbb{Q}^{\text{ab}}(\alpha_i) : \mathbb{Q}^{\text{ab}}] = \omega_{\mathbb{Q}^{\text{ab}}}(\alpha_i)$, quel que soit $i \in \llbracket 1, n \rrbracket$. Pour $i \in \llbracket 1, n \rrbracket$, nous posons $A_i = \lceil 2h(\alpha_i)/h \rceil$ et choisissons $\beta_i \in \bar{\mathbb{Q}}$ tel que $\beta_i^{A_i} = \alpha_i$. Nous notons $A = \prod_{i=1}^n A_i$; par hypothèse et l'inégalité (5.19), nous avons

$$\begin{aligned} A &\leq \prod_{i=1}^n (2h(\alpha_i)/h) \leq 2^n \frac{(c_1(1)[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}] (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\kappa_1(1)})^n}{c_2(n)[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}] (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\kappa_2(n)}} \\ &\leq \frac{(2c_1(1))^n}{c_2(n)} [\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]^{n-1}. \end{aligned}$$

De plus, l'indice d'obstruction du point $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ vérifie (5.20)

$$\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta}) \leq n[\mathbb{Q}^{\text{ab}}(\boldsymbol{\beta}) : \mathbb{Q}^{\text{ab}}]^{1/n} \leq n(A[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}])^{1/n} \leq \frac{2nc_1(1)}{c_2(n)^{1/n}} [\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}] \leq [\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]$$

et $\boldsymbol{\beta}$ n'appartient pas à une sous-variété de torsion dont le degré vérifie

$$(\deg B_{\boldsymbol{\beta}})^{1/\text{codim}(B_{\boldsymbol{\beta}})} \leq c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta})^{\eta_1(n)} (\log(3\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta})))^{\mu(n)}.$$

En effet, si tel était le cas, il existerait un point de torsion ζ et un caractère non trivial $\chi = \prod_{i=1}^n X_i^{r_i}$ tel que $\chi(\zeta\boldsymbol{\beta}) = 1$ et $\|\mathbf{r}\|_{\infty} \leq n^{1/2}(\deg B_{\boldsymbol{\beta}})^{1/\text{codim}(B_{\boldsymbol{\beta}})}$ (obtenu grâce au théorème de Minkowski, comme dans la démonstration du théorème 5.1). Alors le caractère $\tilde{\chi} = \prod_{i=1}^n X_i^{r_i} \prod_{j \neq i} A_j$ vérifierait

$$\tilde{\chi}(\tilde{\boldsymbol{\zeta}}\boldsymbol{\alpha}) = \prod_{i=1}^n (\tilde{\zeta}_i \alpha_i)^{r_i} \prod_{j \neq i} A_j = \prod_{i=1}^n (\zeta_i \beta_i)^{A r_i} = \chi(\zeta\boldsymbol{\beta})^A = 1$$

où $\tilde{\boldsymbol{\zeta}} = (\zeta_1^{A_1}, \dots, \zeta_n^{A_n})$. Ainsi le point $\boldsymbol{\alpha}$ serait contenu dans une hypersurface de torsion $B_{\boldsymbol{\alpha}}$ telle que, en utilisant la majoration de A et l'inégalité (5.20),

$$\begin{aligned} \deg B_{\boldsymbol{\alpha}} &\leq n^{3/2} A c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta})^{\eta_1(n)} (\log(3\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta})))^{\mu(n)} \\ &\leq n^{3/2} c_1(n) \frac{2^n c_1(1)^n}{c_2(n)} [\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]^{n-1} [\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]^{\eta_1(n)} (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\mu(n)} \\ &\leq c_2(n) [\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]^{\eta_2(n)} (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\mu(n)} \end{aligned}$$

ce qui contredit l'hypothèse (5.18).

En appliquant la contraposée du théorème 1.5 à $\boldsymbol{\beta}$, on obtient alors la minoration

$$h(\boldsymbol{\beta}) > (c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta}) (\log(3\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta})))^{\kappa_1(n)})^{-1}.$$

Or la hauteur de $\boldsymbol{\beta}$ est majorée :

$$h(\boldsymbol{\beta}) \leq \sum_{i=1}^n h(\beta_i) = \sum_{i=1}^n \frac{h(\alpha_i)}{A_i} \leq nh.$$

En combinant ces deux inégalités et en utilisant (5.20) et l'hypothèse, on obtient

$$\begin{aligned} 1 &< c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta}) (\log(3\omega_{\mathbb{Q}^{\text{ab}}}(\boldsymbol{\beta})))^{\kappa_1(n)} nh \\ &< n^2 c_1(n) (A[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}])^{1/n} (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\kappa_1(n)} h \\ &< 2n^2 c_1(n) \left([\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}] \prod_{i=1}^n h(\alpha_i) \right)^{1/n} (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\kappa_1(n)} \\ &< 2n^2 c_1(n) c_2(n)^{-1/n} (\log(3[\mathbb{Q}^{\text{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\text{ab}}]))^{\kappa_1(n) - \kappa_2(n)/n} \end{aligned}$$

ce qui est absurde par le choix de $c_2(n)$, $\kappa_1(n)$ et $\kappa_2(n)$.

5.3.3. *Démonstration du corollaire 1.7.* – C'est une conséquence quasi-immédiate du théorème 1.1 de [3] : celui-ci affirme que, pour tout nombre réel $\varepsilon > 0$, l'ensemble des points de V dont les coordonnées sont multiplicativement indépendantes et dont la hauteur est majorée par $(\dim(V) + 1)\hat{\mu}^{\text{ess}}(V) + \varepsilon$ est Zariski-dense dans V (en particulier, il est non vide). Soit α dans cet ensemble ; comme α n'est contenu dans aucune sous-variété de torsion et que $\omega_{\mathbb{Q}^{\text{ab}}}(\alpha) \leq \omega_{\mathbb{Q}^{\text{ab}}}(V)$ (si une hypersurface contient V , alors elle contient α) le théorème 1.5 implique

$$h(\alpha) \geq \left(c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(V)(\log(3\omega_{\mathbb{Q}^{\text{ab}}}(V)))^{\kappa_1(n)} \right)^{-1}$$

donc

$$(\dim(V) + 1)\hat{\mu}^{\text{ess}}(V) + \varepsilon \geq \left(c_1(n)\omega_{\mathbb{Q}^{\text{ab}}}(V)(\log(3\omega_{\mathbb{Q}^{\text{ab}}}(V)))^{\kappa_1(n)} \right)^{-1}.$$

Cette dernière inégalité étant valable pour tout $\varepsilon > 0$, on a donc la minoration voulue.

Appendice

Nous donnons ici des valeurs indicatives pour les constantes utilisées tout au long du texte. Nous ne prétendons pas à l'optimalité de celles-ci. Elles permettent néanmoins de fournir des valeurs pour $c_1(n)$, $c_2(n)$ et $c_3(n)$.

Dans le paragraphe 3.1 : $c_0 = (5n)^5$, $c'_1 = 7n$, $c'_2 = 7$, $c'_3 = 15n^2$ et $C = (10n)^3$.

Dans le paragraphe 3.3 : $c_1 = 4\delta n + 2$, $c_2 = 19n^2 c_1$, $c_3 = 1$, $c_4 = (2n + 4)^{n-1}$, $c_5 = c_1^n c_4$, $c_6 = 4c_2 c_5$, $c_7 = 4$, $c_8 = 4c_5$, $c_9 = (2n + 4)^{-n}$, $c_{10} = c_9/2c_1^n$, $c_{11} = (2^5 n^{n+1} (1 + \delta)(1 + \rho))^{-1}$ (on utilise le résultat de Rosser (voir [16]) qui assure que $|\mathcal{P}_j| \geq N_j/4 \log N_j$ si $N_j \geq 10^9$), $c_{12} = 4n^2(1 + \rho)(1 + \delta)n!$, $c_{13} = c_{11}/2$ et $c_{14} = 1/c_{13}$. Les calculs de ce paragraphe et le théorème clef sont assurés si $C_0 \geq (2^7 n^3 (\delta + 1)(\rho + 1))^{4n}$.

Dans la partie 4 : $c_{15} = c_0^{2n} = (5n)^{10n}$, $c_{16} = 19n^2$, $c_{17} = 8n\nu_0$, $c_{18} = 8n^2\nu_0$, $c_{19} = c_{15}$, $c_{20} = c_{15}c_{16}^n$ et toutes les conditions demandées sur C_0 sont conséquences de $C_0 \geq \exp(8n\nu_0)$.

Dans la partie 5 : $c_{21} = c_{18}$, $c_{22} = c_2(r)n^{5/2}n!$ et toutes les conditions demandées sur C_0 sont vérifiées dès que $C_0 \geq \exp(6n\tilde{\kappa}(n))$.

Ainsi, la valeur $\exp(6n\tilde{\kappa}(n))$ convient pour C_0 et on peut alors prendre $c_1(n) = \exp(8n\tilde{\kappa}(n)\mu(n))$ et $c_2(n) = (2n^2)^n \exp(8n^2\tilde{\kappa}(n)\mu(n))$.

RÉFÉRENCES

- [1] F. AMOROSO, Bogomolov on tori revisited, <http://hal.archives-ouvertes.fr/hal-00132119/fr/>, 2007.
- [2] F. AMOROSO, S. DAVID, Le problème de Lehmer en dimension supérieure, *J. reine angew. Math.* **513** (1999), 145–179.

- [3] F. AMOROSO, S. DAVID, Densité des points à coordonnées multiplicativement indépendantes, *Ramanujan J.* **5** (2001), 237–246.
- [4] F. AMOROSO, S. DAVID, Distribution des points de petite hauteur dans les groupes multiplicatifs, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* **3** (2004), 325–348.
- [5] F. AMOROSO, E. DELSINNE, Une minoration relative explicite pour la hauteur dans une extension d’une extension abélienne, in *Diophantine geometry* (U. Zannier, éd.), CRM Series **4**, Ed. Norm., Pisa, 2007, 1–24.
- [6] F. AMOROSO, U. ZANNIER, A relative Dobrowolski lower bound over abelian extensions, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **29** (2000), 711–727.
- [7] J. W. S. CASSELS, *An introduction to the geometry of numbers*, Grundlehren der math. Wissenschaften **99**, Springer, 1959.
- [8] J. W. S. CASSELS, A. FRÖHLICH, *Algebraic number theory*, Proceedings of an instructional conference organized by the London Mathematical Society, Academic Press, 1967.
- [9] M. CHARDIN, Une majoration de la fonction de Hilbert et ses conséquences pour l’interpolation algébrique, *Bull. Soc. Math. France* **117** (1989), 305–318.
- [10] S. DAVID, P. PHILIPPON, Minorations des hauteurs normalisées des sous-variétés des tores, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **28** (1999), 489–543.
- [11] E. DELSINNE, Problème de Lehmer relatif dans un tore : cas des hypersurfaces, prépublication du LMNO, [arXiv:math/0509196](https://arxiv.org/abs/math/0509196), 2005.
- [12] E. DOBROWOLSKI, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.
- [13] M. HINDRY, Autour d’une conjecture de Serge Lang, *Invent. math.* **94** (1988), 575–603.
- [14] P. PHILIPPON, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* **114** (1986), 355–383.
- [15] P. PHILIPPON, M. SOMBRA, Quelques aspects diophantiens des variétés toriques projectives, in *Diophantine Approximation : Festschrift for Wolfgang Schmidt*, Dev. Math. **16**, Springer, 2008, 295–338.
- [16] B. ROSSER, Explicit bounds for some functions of prime numbers, *Amer. J. Math.* **63** (1941), 211–232.
- [17] D. ROY, J. L. THUNDER, An absolute Siegel’s lemma, *J. reine angew. Math.* **476** (1996), 1–26.
- [18] W. M. SCHMIDT, Heights of points on subvarieties of \mathbf{G}_m^n , in *Number theory (Paris, 1993–1994)*, London Math. Soc. Lecture Note Ser. **235**, Cambridge Univ. Press, 1996, 157–187.
- [19] J-P. SERRE, *Corps locaux*, Hermann, 1968, deuxième édition, Publications de l’Université de Nancago, No. VIII.
- [20] J. D. VAALER, A geometric inequality with applications to linear forms, *Pacific J. Math.* **83** (1979), 543–553.
- [21] U. ZANNIER, 2001, communication personnelle.

- [22] S. ZHANG, Small points and adelic metrics, *J. Algebraic Geom.* **4** (1995), 281–300.

(Manuscrit reçu le 5 mars 2009 ;
accepté, après révision, le 4 mai 2009.)

Emmanuel DELSINNE
University of Ottawa
Department of Mathematics and Statistics
585 King Edward
Ottawa, ON K1N 6N5, Canada
E-mail: edelsinn@uottawa.ca