Minorations de la hauteur d'un nombre algébrique

Francesco Amoroso Damien Vergnaud

Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen, BP 5186, 14032 Caen cedex France

Questo testo riproduce il contenuto del corso di dottorato tenuto a Pisa nel giugno 2002 dal primo autore e proviene da una rielaborazione delle note di un precedente corso di DEA.

The following problem arises immediately. If ε is a positive quantity, to find a polynomial of the form

$$f(x) = x^r + a_1 x^{r-1} + \cdots + a_r$$

where the a's are integers, such that the absolute values of the product of those roots of f which lie outside the unit circle, lies between 1 *and* $1 + \varepsilon$.

D. H. Lehmer [6, page 477]

Table des matières

Chapitre 1

Mesure de Mahler

1.1 Mesure de Mahler d'un polynôme

Etudier la complexité d'un nombre algébrique α peut se faire en donnant une mesure de complexité de son polynôme minimal sur $\mathbb{Z}$ (*i.e.* le seul polynôme irréductible, à coefficients entiers rationnels, de coefficient dominant positif, s'annulant en α). Pour mesurer la complexité d'un polynôme

$$F(X) = a_D X^D + a_{D-1} X^{D-1} + \cdots + a_0$$

à coefficients dans $\mathbb{Z}$, une approche standard consiste à utiliser les différentes normes définies sur $\mathbb{C}[X]$:

$$\begin{aligned}
\|F\|_1 &= |a_0| + \cdots + |a_D| \,, \\
\|F\|_2 &= \sqrt{|a_0|^2 + \cdots + |a_D|^2} \,, \\
\|F\|_\infty &= \max(|a_0|, \ldots, |a_D|) \,, \\
|F|_1 &= \max_{|z|=1} |F(z)| \,,
\end{aligned}$$

que l'on nomme respectivement longueur, norme quadratique (ou euclidienne), hauteur (ou hauteur naïve), et norme de la convergence uniforme sur la boule unité[1]. Les relations parmi ces normes sont résumées dans la proposition suivante :

1. Les notations utilisées ici ne sont pas les notations classiques. L'usage veut que l'on note $L(F)$ la longueur du polynôme F et $H(F)$ sa hauteur naïve. Cependant, nous avons souhaité réserver les notations H et h pour la hauteur de Weil que nous introduirons au chapitre 2.

Proposition 1.1.1 *Pour tout polynôme $F \in \mathbb{C}[X]$ de degré au plus D, nous avons*

$$\|F\|_\infty \leq \|F\|_2 \leq |F|_1 \leq \|F\|_1 \leq (D+1)\|F\|_\infty \ .$$

Toutes ces relations sont évidentes, à l'exception peut-être de l'inégalité $\|F\|_2 \leq |F|_1$. Cette dernière découle cependant du lemme suivant, que l'on démontre facilement à l'aide de la formule de Parseval.

Lemme 1.1.2 *Pour tout polynôme $F \in \mathbb{C}[X]$, on a :*

$$\|F\|_2^2 = \frac{1}{2\pi} \int_0^{2\pi} |F(e^{it})|^2 dt \ ,$$

Il est clair que chacune des normes introduites mesure en un certain sens la complexité d'un polynôme à coefficients entiers F (par exemple, la longueur donne une idée du nombre de chiffres nécessaires à l'écriture de F), cependant il serait préférable de disposer d'une mesure canonique (en un sens que nous préciserons par la suite) de la complexité d'un polynôme.

Nous allons définir, pour cela, la mesure de Mahler qui répondra à cette exigence, en ayant en plus des propriétés arithmétiques suffisamment agréables :

Définition 1.1.3 *Soit $F \in \mathbb{C}[X]$ un polynôme non nul et notons*

$$F(X) = a(X - \alpha_1) \cdots (X - \alpha_D)$$

sa factorisation dans $\mathbb{C}$. On appelle mesure de Mahler de F et l'on note $M(F)$ le nombre réel défini par :

$$M(F) = |a| \prod_{j=1}^{D} \max(1, |\alpha_j|) \ .$$

On note aussi $M(0) = 1$.

La mesure de Mahler d'un polynôme F est donc le produit de son coefficient dominant et des modules de ses racines en dehors du disque unité (avec leur multiplicité).

Définition 1.1.4 *Soit α un nombre complexe algébrique. On appelle mesure de Mahler de α, et l'on note $M(\alpha)$ la mesure de Mahler du polynôme minimal sur $\mathbb{Z}$ de α.*

On déduit de la définition de la mesure de Mahler les propriétés suivantes valables pour tout F, $G \in \mathbb{C}[X]$:

1. $M(FG) = M(F)M(G)$.
2. $M(F)$ est minorée par la valeur absolue du coefficient dominant de F.
3. $M(F(X^n)) = M(F)$, pour tout entier $n \geq 1$.
4. $M(F^*) = M(F)$, où F^* désigne le polynôme réciproque de F (défini par $F^*(X) = X^{\deg(F)}F(X^{-1})$).

La mesure de Mahler avait déjà été introduite par de nombreux auteurs (notamment par D. H. Lehmer [6] ; nous reviendrons sur la contribution de cet auteur au chapitre 3), mais elle est connue sous ce nom depuis une série d'articles de K. Mahler parus dans les années 1960 et relatifs à cette quantité. Le théorème suivant qui donne une expression analytique de la mesure de Mahler d'un polynôme, est l'un des résultats élégants montrés par K. Mahler :

Théorème 1.1.5 *Soit $F \in \mathbb{C}[X]$, nous avons :*

$$M(F) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left(|F\left(e^{it}\right)|\right) dt\right).$$

Preuve. On pourrait facilement déduire cette formule en utilisant la formule de Jensen d'analyse complexe. Nous allons en donner, suivant Mahler, une preuve élémentaire. Posons

$$\tilde{M}(F) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left(|F\left(e^{it}\right)|\right) dt\right).$$

Nous avons déjà remarqué que la mesure de Mahler est multiplicative, et il est immédiat qu'il en est de même pour la fonction $\tilde{M}$. De plus, $M(a) = |a| = \tilde{M}(a)$ pour tout $a \in \mathbb{C}^*$. Pour montrer le théorème, il suffit donc de prouver que pour tout $\alpha \in \mathbb{C}$, nous avons $\tilde{M}(X-\alpha) = M(X-\alpha)$. Il est même suffisant de vérifier cette dernière assertion pour $\alpha \in \mathbb{R}^+$. En effet, pour $\alpha = re^{i\theta} \in \mathbb{C}$, avec $r \in \mathbb{R}^+$ et $\theta \in [0, 2\pi[$, nous avons d'une part $M(X-\alpha) = \max(1, |\alpha|) = \max(1, r) = M(X-r)$, et d'autre part

$$\begin{aligned}
\log(\tilde{M}(X-\alpha)) &= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - \alpha| dt \\
&= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{i(t-\theta)} - r| dt \\
&= \frac{1}{2\pi}\int_\theta^{2\pi+\theta} \log|e^{it} - r| dt = \log(\tilde{M}(X-r)) .
\end{aligned}$$

Posons

$$I(r) = \frac{1}{2\pi} \int_0^{2\pi} \log|e^{it} - r| dt \ .$$

Il nous faut montrer que $I(r) = \log \max(1, r)$. Pour cela, nous allons prouver que $I(r^2) = 2I(r)$ pour tout $r \in \mathbb{R}^+$.

$$\begin{aligned}
I(r^2) &= \frac{1}{2\pi} \int_0^{2\pi} \log|e^{it} - r^2| dt \\
&= \frac{1}{4\pi} \int_0^{4\pi} \log|e^{it} - r^2| dt \\
&= \frac{1}{4\pi} \int_0^{2\pi} \log|e^{2is} - r^2| 2ds \qquad \text{(En posant t=2s)} \\
&= \frac{1}{2\pi} \int_0^{2\pi} \log|e^{is} - r| ds + \frac{1}{2\pi} \int_0^{2\pi} \log|e^{is} + r| ds \\
&= I(r) + I(-r) \\
&= I(r) + I(r) \qquad (\text{car } -r = re^{i\pi}) \\
&= 2I(r) \ .
\end{aligned}$$

En particulier, pour $r = 1$, nous obtenons $I(1) = I(1^2) = 2I(1)$ et par suite $I(1) = 0 = \log \max(1, 1)$.

Par récurrence, nous déduisons de ce qui précède que pour $n \in \mathbb{N}^*$, nous avons $I(r^{2^n}) = 2^n I(r)$. De plus, nous avons

$$|r^{2^n} - 1| \leq \ |e^{it} - r^{2^n}| \leq \ r^{2^n} + 1 \ ,$$

et, en intégrant cette inégalité, on obtient :

$$\frac{1}{2^n} \log|r^{2^n} - 1| \ \leq \ \underbrace{\frac{I(r^{2^n})}{2^n}}_{I(r)} \ \leq \ \frac{1}{2^n} \log|r^{2^n} + 1| \ .$$

En faisant tendre n vers $+\infty$, nous trouvons, pour $r < 1$,

$$I(r) = 0 = \log 1 = \log \max(1, r) \ ,$$

et pour $r > 1$,

$$I(r) = \log r = \log \max(1, r) \ .$$

□

1.2 Majorations de la mesure de Mahler en fonction des normes $\|F\|_1$, $\|F\|_2$, $\|F\|_\infty$, $|F|_1$

Nous pouvons maintenant comparer la mesure de Mahler avec les normes introduites au début du paragraphe précédent.

Commençons par majorer cette mesure en fonction des normes $\|F\|_1$, $\|F\|_2$, $\|F\|_\infty$, $|F|_1$. Au vue de la proposition 1.1.1, il suffit de majorer $M(F)$ en fonction de la norme euclidienne ; le résultat plus précis que l'on connait est le suivant :

Théorème 1.2.1 (Landau) *Pour tout polynôme $F \in \mathbb{C}[X]$, nous avons*

$$M(F) \leq \|F\|_2 \, . \tag{1.1}$$

Preuve. Soit $F \in \mathbb{C}[X]$ un polynôme de degré $D \geq 1$,

$$F(X) = a_D X^D + a_{D-1} X^{D-1} + \cdots + a_0 = a_D \prod_{i=1}^{D} (X - \alpha_i) \, ,$$

et posons :

$$G(X) = F(X) \prod_{|\alpha_j|>1} B(X;\alpha_j) = a_D \prod_{|\alpha_j|>1} (\overline{\alpha_j} X - 1) \prod_{|\alpha_j|\leq 1} (X - \alpha_j) \, ,$$

où l'on a noté :

$$B(X;\alpha) = \frac{\overline{\alpha} X - 1}{X - \alpha}.$$

(*facteur de Blasckhe*). On vérifie immédiatement que $|B(z;\alpha)| = 1$ si $|z| = 1$, d'où $|F(z)| = |G(z)|$ pour tout $|z|$ de module 1, et donc, par le lemme 1.1.2,

$$\|F\|_2^2 = \int_0^1 |F(e^{2\pi i\theta})|^2 d\theta = \int_0^1 |G(e^{2\pi i\theta})|^2 d\theta = \|G\|_2^2 \, .$$

Par ailleurs, le coefficient dominant b_D de G satisfait :

$$|b_D| = |a_D| \prod_{|\alpha_j|>1} |\overline{\alpha_j}| = M(F) \, ,$$

et donc :

$$\|F\|_2 = \|G\|_2 \geq |b_D| = M(F) \, .$$

□

En utilisant la proposition 1.1.1, on déduit du théorème 1.2.1 les majorations :

$$M(F) \leq \|F\|_1 \ , \tag{1.2}$$

$$M(F) \leq |F|_1 \ , \tag{1.3}$$

$$M(F) \leq \sqrt{\deg(F)+1}\ \|F\|_\infty \ . \tag{1.4}$$

Remarquons que l'inégalité (1.2) (et donc les autres) se déduit aussi directement à l'aide du théorème 1.1.5.

L'inégalité de Landau (1.1) ne peut être améliorée puisque, par exemple, pour tout entier $D \in \mathbb{N}^*$, nous avons $M(X^D) = \|X^D\|_2 = 1$. De même, les inégalités (1.2) et (1.3) sont optimales (choisir à nouveau $F(X) = X^D$). Par contre, nous ne savons pas si l'inégalité (1.4) est optimale. Cependant, A. Durand a montré que, pour tout entier D, il existe un polynôme F de degré D, tel que

$$\|F\|_\infty = 1 \qquad \text{et} \qquad M(F) \geq \sqrt{D+1} - \frac{\log D}{2}.$$

1.3 Minorations de la mesure de Mahler en fonction des normes $\|F\|_1$, $\|F\|_2$, $\|F\|_\infty$, $|F|_1$

Nous allons maintenant minorer la mesure de Mahler en fonction des normes introduites au début du paragraphe 1.1. Pour ce faire, nous avons besoin du lemme suivant :

Lemme 1.3.1 *Soit $F(X) = a_D X^D + a_{D-1}X^{D-1} + \cdots + a_0 \in \mathbb{C}[X]$ un polynôme de degré D. Pour $j = 1, \ldots, D$, nous avons*

$$|a_j| \leq \binom{D}{k} M(F) \ .$$

Preuve. Ecrivons la factorisation de F dans $\mathbb{C}$:

$$F(X) = a_D \prod_{j=1}^{D} (X - \alpha_i) \ .$$

En utilisant les formules de Newton sur les fonctions symétriques élémentaires, nous obtenons :

$$\begin{cases} a_{D-1} &= -a_D \sum_{j=1}^{D} \alpha_j \\ a_{D-2} &= a_D \sum_{1 \le j < k \le D} \alpha_j \alpha_k \\ & \vdots \\ a_0 &= (-1)^D a_D \prod_{j=1}^{D} \alpha_j \end{cases}$$

D'où, pour $j = 1, \dots D$,

$$\begin{aligned} |a_j| &\le |a_D| \binom{D}{j} \prod_{j=1}^{D} \max(1, |\alpha_j|) \\ &\le \binom{D}{j} M(F) \, . \end{aligned}$$

□

En utilisant ce lemme, on en déduit :

Théorème 1.3.2 *Pour tout polynôme $F \in \mathbb{C}[X]$ de degré $\le D$, nous avons*

$$\|F\|_2 \le \binom{2D}{D}^{1/2} M(F) \, , \tag{1.5}$$

$$|F|_1 \le 2^D M(F) \, , \tag{1.6}$$

$$\|F\|_1 \le 2^D M(F) \, , \tag{1.7}$$

$$\|F\|_\infty \le \binom{D}{[D/2]} M(F) \, , \tag{1.8}$$

où $[x]$ désigne la partie entière de x.

Preuve. Pour montrer (1.5), (1.7) et (1.8), il suffit d'appliquer le lemme 1.3.1 et les formules

$$\sum_{i=0}^{D} \binom{D}{i}^2 = \binom{2D}{D} ,$$

$$\sum_{i=0}^{D} \binom{D}{i} = 2^D ,$$

$$\max_{i=0,\dots,D} \binom{D}{i} \leq \binom{D}{[D/2]}$$

respectivement. L'inégalité (1.6) se déduit de $|F|_1 \leq \|F\|_1$ (*cf* proposition 1.1.1) et de (1.7).

□

Les inégalités (1.5), (1.6), (1.7) et (1.8) sont optimales, comme on peut le voir en considérant pour tout entier D, le polynôme $F(X) = (X+1)^D$.

Terminons ce paragraphe par la remarque suivante : soit

$$F(X) = a_D \prod_{i=1}^{D} (X - \alpha_i)$$

un polynôme à coefficients complexes de degré D et posons, pour tout entier $n \in \mathbb{N}^*$,

$$F_n(X) = a_D^n \prod_{i=1}^{D} (X - \alpha_i^n) .$$

Remarquons que F_n est de degré D pour tout $n \in \mathbb{N}^*$. D'après les résultats précédents, nous avons pour tout $n \in \mathbb{N}^*$,

$$M(F) = M(F_n)^{1/n} \leq \|F_n\|_1^{1/n} \leq (2^D)^{1/n} M(F_n)^{1/n} = 2^{D/n} M(F) .$$

En faisant tendre n vers l'infini, nous obtenons :

$$\lim_{n \to +\infty} \|F_n\|_1^{1/n} = M(F) .$$

Puisque l'ensemble $\mathbb{C}[X]_D$ des polynômes de $\mathbb{C}[X]$, de degré inférieur à D, est un espace vectoriel de dimension finie, toutes les normes définies sur $\mathbb{C}[X]_D$ sont équivalentes, et nous obtenons :

Proposition 1.3.3 *Soit $F \in \mathbb{C}[X]$ un polynôme de degré D et soit $\|\cdot\|$ une norme définie sur l'espace vectoriel $\mathbb{C}[X]_D$. Alors*

$$\lim_{n\to\infty} \|F_n\|^{1/n} = M(F) \ .$$

□

1.4 Théorème de finitude de Northcott

Grâce aux estimations du paragraphe précédent, nous allons pouvoir énoncer un théorème élémentaire, mais très important d'un point de vue théorique.

Théorème 1.4.1 (Théorème de finitude de Northcott) *Soit $D \in \mathbb{N}^*$ et soit $M_0 \in \mathbb{R}^+$. L'ensemble des nombres algébriques de degré borné par D et de mesure de Mahler bornée par M_0 est fini.*

Preuve. Nous savons que pour tout polynôme F de degré inférieur à D nous avons

$$\|F\|_\infty \leq \binom{D}{[D/2]} M(F) \ .$$

Nous en déduisons que chaque nombre algébrique de degré borné par D et de mesure de Mahler bornée par M_0 est racine d'un polynôme irréductible F de hauteur naïve inférieure à

$$\binom{D}{[D/2]} M_0 \ .$$

Le nombre de tels polynômes étant inférieur à

$$\left[2\binom{D}{[D/2]} M_0 + 1\right]^{D+1} ,$$

nous en déduisons que le cardinal des nombres algébriques de degré borné par D et de mesure de Mahler bornée par M_0 est inférieur à

$$D\left[2\binom{D}{[D/2]} M_0 + 1\right]^{D+1} .$$

□

Le théorème de Northcott permet d'obtenir le résultat suivant, implicite dans le théorème des unités de Dirichlet, et mis en évidence par L. Kronecker en 1857 ([5]).

Corollaire 1.4.2 *Soit $\alpha \in \overline{\mathbb{Q}}^*$, alors $M(\alpha) = 1$ si et seulement si α est une racine de l'unité.*

Preuve. Supposons que α soit une racine de l'unité, alors le polynôme minimal F de α sur $\mathbb{Z}$ est un polynôme cyclotomique; donc $F(X) = \prod_{j=1}^{D}(X-\alpha_j)$ avec $|\alpha_j| = 1$ pour tout $j \in \{1, \dots, D\}$, et $M(F) = 1$.

Réciproquement, soit α un complexe non nul tel que $M(\alpha) = 1$. Pour tout $n \in \mathbb{N}^*$, nous avons $M(\alpha^n) = 1$. En effet, puisque $M(\alpha) = 1$, α est un entier algébrique et tous ses conjugués sont de module ≤ 1, et il en est de même de α^n pour tout entier $n \in \mathbb{N}^*$. Notons D le degré de α. Pour tout $n \in \mathbb{N}^*$, nous avons $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] \leq D$. Par le théorème 1.4.1, nous déduisons de ces deux assertions qu'il existe deux entiers n et m avec $n \neq m$ et tels que

$$\alpha^n = \alpha^m,$$

et donc que α est une racine de l'unité.

□

Chapitre 2

Hauteur logarithmique de Weil d'un nombre algébrique

2.1 Valeurs absolues sur un corps commutatif

Définition 2.1.1 *Soit K un corps commutatif. Une valeur absolue sur K est une application $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ vérifiant les trois propriétés suivantes :*

1) pour tout $x \in K$ on a $|x| = 0$ si et seulement si $x = 0$;

2) pour tout x, $y \in K$ on a $|xy| = |x||y|$;

3) pour tout x, $y \in K$ on a $|x + y| \leq |x| + |y|$.

Si de plus, 3) est renforcée en :

3') pour tout x, $y \in K$ on a $|x + y| \leq \max(|x|, |y|)$

la valeur absolue est dite ultramétrique. Dans le cas contraire, la valeur absolue est dite archimédienne.

Une valeur absolue $|\cdot|$ sur un corps commutatif K vérifie les propriétés immédiates suivantes :

1. $|1| = 1$;
2. toute racine de l'unité ω dans K vérifie $|\omega| = 1$;
3. si $|\cdot|$ est ultramétrique, alors pour tout x, $y \in K$ vérifiant $|x| \neq |y|$, nous avons $|x + y| = \max(|x|, |y|)$.

Remarque. Supposons que le corps commutatif K soit le corps de fractions d'un anneau A. S'il existe une application $|\cdot|$ de A dans $\mathbb{R}_{\geq 0}$ vérifiant pour tout x, $y \in A$ les propriétés *1)*, *2)* et *3)* de la définition 2.1.1, alors $|\cdot|$ définit de façon unique une valeur absolue sur K. Si, de plus, $|\cdot|$ vérifie pour tout

x, $y \in A$ la propriété *3')* de la définition 2.1.1, alors $|\cdot|$ définit une valeur absolue ultramétrique sur K.

Définition 2.1.2 *Soit K un corps commutatif. Une valuation sur K est une application $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ vérifiant les trois propriétés suivantes :*

1) pour tout $x \in K$ on a $v(x) = \infty$ si et seulement si $x = 0$;

2) pour tout x, $y \in K$ on a $v(xy) = v(x) + v(y)$;

3) pour tout x, $y \in K$ on a $v(x + y) \geq \min(v(x), v(y))$.

Si v est une valuation sur un corps commutatif K, et si a désigne un réel > 1, alors l'application définie par :

$$\begin{array}{rccl} |\cdot| & K & \longrightarrow & \mathbb{R}_+^* \\ & x & \longmapsto & |x| = \left\{ \begin{array}{cc} 0 & \text{si } x = 0 \\ a^{-v(x)} & \text{si } x \neq 0 \end{array} \right. \end{array}$$

est une valeur absolue ultramétrique sur K, appelée valeur absolue associée à v. Nous utiliserons désormais la convention : $a^{-\infty} = 0$ pour tout réel a strictement positif. Réciproquement, si $|\cdot|$ est une valeur absolue ultramétrique sur un corps commutatif K, et si b désigne un réel strictement positif, alors l'application définie par :

$$\begin{array}{rccl} v & K & \longrightarrow & \mathbb{R} \cup \{\infty\} \\ & x & \longmapsto & v(x) = \left\{ \begin{array}{cc} \infty & \text{si } x = 0 \\ -b \log |x| & \text{si } x \neq 0 \end{array} \right. \end{array}$$

est une valuation sur K. Nous utiliserons désormais la convention : $b \log 0 = -\infty$, pour tout réel b strictement positif.

La démonstration de la prochaine proposition est immédiate.

Proposition 2.1.3 *Soit K un corps commutatif, et soit v une valuation sur K.*

1) $A = \{x \in K \mid v(x) \geq 0\}$ est un sous-anneau de K appelé anneau de valuation de K.

2) Pour tout $x \in K$ on a $x \in A$ ou $x^{-1} \in A$

3) K est le corps de fractions de A.

4) $A^* = \{x \in K \mid v(x) = 0\}$.

5) $M = \{x \in K \mid v(x) > 0\}$ est le seul idéal maximal de A. Le corps A/M s'appelle corps résiduel de K.

□

Dans le cas d'un corps commutatif K muni d'une valeur absolue ultramétrique $|\cdot|$ définie à partir d'une valuation v comme dans la remarque précédente (*i.e.* $|\cdot| = a^{-v(\cdot)}$ pour un réel $a > 1$), les ensembles

$$A = \{x \in K,\ |x| \leq 1\} \text{ et } M = \{x \in K,\ |x| < 1\}\ ,$$

ne dépendent pas du choix de a et sont respectivement l'anneau de valuation de K et l'idéal maximal de A, pour la valuation v.

Définition 2.1.4 *Soit K un corps commutatif, et soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur K. On dit que $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes, et l'on note $|\cdot|_1 \sim |\cdot|_2$, si et seulement si elles définissent la même topologie d'espace métrique. On appelle place de K toute classe d'équivalence de valeurs absolues de K. On note enfin $\mathcal{M}_K$ l'ensemble des places de K non triviales.*

Proposition 2.1.5 *Soit K un corps commutatif, et soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur K. Les assertions suivantes sont équivalentes :*

1. *les valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes ;*
2. *on a $\{x \in K, |x|_1 < 1\} = \{x \in K, |x|_2 < 1\}$;*
3. *il existe un nombre réel $a > 0$ tel que $|x|_1 = |x|_2^a$ pour tout $x \in K$.*

Preuve. Montrons tout d'abord que l'assertion *1* est équivalente à l'assertion *2*. L'assertion *2* affirme que les deux valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ ont les mêmes boules ouvertes pour les distances d_1 et d_2 qu'elles induisent. Elles définissent donc la même topologie, et par définition, les deux valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes. Réciproquement, supposons que $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes, et notons

$$M_j = \{x \in K, |x|_j < 1\}$$

pour $j = 1, 2$. Puisqu'une condition nécessaire et suffisante pour qu'un élément λ de $\mathbb{R}_+^*$ soit strictement inférieur à 1, est que la suite $(\lambda^n)_{n\in\mathbb{N}}$ tende vers 0, un élément x de K appartient à M_j si et seulement si la suite $(x^n)_{n\in\mathbb{N}}$ converge vers 0 dans K pour la topologie induite par $|\cdot|_j$. Les topologies induites par $|\cdot|_1$ et $|\cdot|_2$ étant équivalentes, nous en déduisons que $M_1 = M_2$.

Montrons que les assertions *2* et *3* sont équivalentes. Le fait que la troisième assertion entraîne la deuxième est immédiat par la positivité du réel a, et il suffit de montrer que si $M_1 = M_2$, avec les notations qui

précèdent, alors il existe un réel $a > 0$ tel que pour tout $x \in K$, $|x|_1 = |x|_2^a$. Notons $M = M_1 = M_2$. Si M est réduit à $\{0\}$, les deux valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sont triviales, donc $|\cdot|_1 = |\cdot|_2$, et le choix $a = 1$ convient. Dans le cas contraire, considérons $y \in M$, $y \neq 0$, et posons

$$a = \frac{\log |y|_1}{\log |y|_2} .$$

Nous avons $a > 0$, puisque l'hypothèse $y \in M$ implique $\log |y|_j < 0$ pour $j = 1, 2$. Soit $x \in K^*$, et soient $m, n \in \mathbb{Z}$. Pour $j = 1, 2$, nous avons

$$\begin{aligned} n \log |x|_j < m \log |y|_j \quad &\iff \quad |x|_j^n < |y|_j^m \\ &\iff \quad \left| \frac{x^n}{y^m} \right|_j < 1 \\ &\iff \quad \frac{x^n}{y^m} \in M \end{aligned}$$

et cette dernière condition est indépendante de j. Pour $n, m \in \mathbb{Z}$, nous avons donc :

$$n \log |x|_1 < m \log |y|_1 \iff n \log |x|_2 < m \log |y|_2 ,$$

d'où :

$$\frac{\log |x|_1}{\log |y|_1} = \frac{\log |x|_2}{\log |y|_2} .$$

Nous avons montré que $|x|_1 = |x|_2^a$ pour tout $x \in K^*$, ce qui achève la preuve de l'équivalence des deux dernières assertions, et par conséquent celle de la proposition.

□

En particulier, deux valeurs absolues sur un corps de nombres K associées à la même valuation sont équivalentes. Cela justifie la définition suivante :

Définition 2.1.6 *Soit K un corps commutatif, et soient v_1 et v_2 deux valuations sur K. On dit que v_1 et v_2 sont équivalentes, et l'on note $v_1 \sim v_2$ si et seulement si les valeurs absolues associées à v_1 et v_2 sont équivalentes.*

On déduit alors de la proposition 2.1.5 le corollaire suivant :

Corollaire 2.1.7 *Soit K un corps commutatif, et soient v_1, v_2 deux valuations sur K. Les assertions suivantes sont équivalentes :*

1. *v_1 et v_2 sont équivalentes;*
2. *$\{x \in K, v_1(x) > 0\} = \{x \in K, v_2(x) > 0\}$;*
3. *il existe un nombre réel $a > 0$ tel que $v_1(x) = a v_2(x)$ pour tout $x \in K$.*

□

2.2 Valeurs absolues sur $\mathbb{Q}$

Outre la valeur absolue triviale et la valeur absolue usuelle, notée $|\cdot|_\infty$, on peut associer à tout nombre premier p une valeur absolue ultramétrique sur $\mathbb{Q}$.

Définition 2.2.1 *Pour tout premier p, on définit une valuation v_p en posant, pour $x \in \mathbb{Q}^*$,*

$$x = p^{v_p(x)}\frac{a}{b},$$

avec a et b deux entiers non divisibles par p.

On définit également la valeur absolue p-adique $|\cdot|_p$ en posant, pour tout rationnel x, $|x|_p = p^{-v_p(x)}$.

Il est clair que les valeurs absolues p-adiques, la valeur absolue usuelle, et la valeur absolue triviale, sont 2 à 2 non équivalentes. Nous allons montrer (théorème d'Ostrowski) que toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente soit à une valeur absolue p-adique, soit à la valeur absolue usuelle.

Lemme 2.2.2 *Soit $|\cdot|$ une valeur absolue sur $\mathbb{Q}$ telle qu'il existe un premier p tel que $|p| < 1$, alors pour tout entier non nul $n \in \mathbb{N}^*$, $|n| \leq 1$.*

Preuve. Soit $n \in \mathbb{N}^*$ un entier non nul fixé. Pour tout entier non nul $k \in \mathbb{N}^*$, considérons le développement p-adique de n^k :

$$n^k = c_{k,0} + c_{k,1}p + \cdots + c_{k,h_k}p^{h_k}$$

où les $c_{k,j}$ sont des entiers satisfaisant $0 \leq c_{k,j} < p$ pour $j = 0, \ldots, h_k$, et $c_{k,h_k} \neq 0$. Nous avons donc $n^k \geq p^{h_k}$, d'où :

$$h_k \leq k\frac{\log n}{\log p}\,.$$

Posons d'autre part, $M = \max(1, |2|, \ldots, |p-1|)$, alors, puisque $|p| < 1$,

$$|n|^k = |n^k| \leq M(1 + h_k)$$

et

$$|n| \leq \left(1 + k\frac{\log n}{\log p}\right)^{1/k} M^{1/k}\,,$$

pour tout entier $k \in \mathbb{N}^*$. En faisant tendre k vers $+\infty$, le membre de droite de cette dernière inégalité tend vers 1, d'où :

$$|n| \leq 1\,.$$

□

Lemme 2.2.3 *Soit $|\cdot|$ une valeur absolue sur $\mathbb{Q}$ telle qu'il existe un premier p tel que $|p| < 1$, alors pour tout premier q, $q \neq p$, nous avons $|q| = 1$.*

Preuve. Soit q un premier différent de p. D'après le lemme 2.2.2, nous avons $|q| \leq 1$. Supposons par l'absurde $|q| < 1$. Pour tout entier $k \in \mathbb{N}^*$, le théorème de Bézout nous assure l'existance de deux entiers λ_k et $\mu_k \in \mathbb{Z}$ tels que

$$\lambda_k p^k + \mu_k q^k = 1\,.$$

Par le lemme 2.2.2, nous avons alors

$$1 \leq \ |\lambda_k|\ |p^k| + |\mu_k|\ |q^k| \leq |p^k| + |q^k|\,,$$

pour tout $k \in \mathbb{N}^*$, et faisant tendre k vers l'infini, le terme de droite tend vers 0, ce qui amène la contradiction recherchée, et achève la preuve du lemme. □

Lemme 2.2.4 *Soit $|\cdot|$ une valeur absolue sur $\mathbb{Q}$ telle qu'il existe un entier $n \in \mathbb{N}^*$ tel que $|n| > 1$, alors pour tout entier $x \geq 2$,*

$$\frac{\log|x|}{\log x} \leq \frac{\log|n|}{\log n}\,.$$

Preuve. Soit $n \in \mathbb{N}^*$ tel que $|n| > 1$ et soit $x,\ k \in \mathbb{N}^*$. Considérons le développement en base n de x^k :

$$x^k = c_{k,0} + c_{k,1}n + \cdots + c_{k,h_k}n^{h_k}$$

où les $c_{k,j}$ sont des entiers satisfaisants $0 \leq c_{k,j} < n$ pour tout $j = 0, \ldots, h_k$, et $c_{k,h_k} \neq 0$. Nous avons donc

$$h_k \leq k\frac{\log x}{\log n}\,.$$

Posons $M = \max(1, |2|, \ldots, |n-1|)$; on a alors

$$|x|^k = |x^k| \leq M(1 + |n| + \cdots + |n|^{h_k}) = M\frac{|n|^{h_k+1} - 1}{|n| - 1}\,.$$

Donc pour tout $k \in \mathbb{N}^*$,

$$|x| \leq \left(\frac{|n|^{1+k\log x/\log n} - 1}{|n| - 1}\right)^{1/k} M^{1/k}\,,$$

et en faisant tendre k vers l'infini dans le terme de droite, nous obtenons

$$|x| \leq |n|^{\frac{\log x}{\log n}},$$

ce qui achève la preuve du lemme.

□

Nous pouvons maintenant démontrer le théorème d'Ostrowski.

Théorème 2.2.5 *Soit $|\cdot|$ une valeur absolue non triviale sur $\mathbb{Q}$, alors*

1. *S'il existe $n \in \mathbb{N}^*$ tel que $|n| < 1$, alors il existe un premier p et un réel $a \in]0,1[$ tel que $|x| = a^{v_p(x)}$ pour tout $x \in \mathbb{Q}$.*
2. *Dans le cas contraire (i.e. $|n| \geq 1$ pour tout $n \in \mathbb{N}^*$), il existe un réel $a \in]0,1]$ tel que $|\cdot| = |\cdot|_\infty^a$.*

Preuve.

1. Soit n un entier tel que $|n| < 1$. Il existe donc un diviseur premier de p tel que $|p| < 1$ (puisque dans le cas contraire nous obtiendrons $|n| \geq 1$). Posons $a = |p| \in]0,1[$ et écrivons, pour $x \in \mathbb{Q}^*$,

$$x = p^{v_p(x)} \frac{r}{s},$$

avec r et s entiers premiers avec p. Par le lemme 2.2.3, tous les facteurs premiers q divisant r ou s vérifient $|q| = 1$, et donc :

$$|x| = a^{v_p(x)} .$$

2. Par hypothèse, il existe $n \in \mathbb{N}^*$ tel que $|n| > 1$. Nous avons donc

$$0 < \log|n| \leq \log(\underbrace{|1| + \cdots + |1|}_{n \text{ termes}}) \leq \log n ,$$

et en posant $a = \frac{\log|n|}{\log n}$, nous avons $a \in]0,1]$. Il nous suffit de vérifier que pour tout $x \in \mathbb{N}^*$, nous avons $|x| = x^a$. Soit donc $x \in \mathbb{N}^*$; si $|x| > 1$, nous obtenons en appliquant deux fois le lemme 2.2.4 :

$$\frac{\log|x|}{\log x} = \frac{\log|n|}{\log n} .$$

et $|x| = |x|_\infty^a$. Si $|x| \leq 1$, alors, par hypothèse, $|x| = 1$ et :

$$|nx| = |n||x| = |n| > 1$$

d'où, pour ce qui précède, $|nx| = |nx|_\infty^a$. Comme $|n| = |n|_\infty^a$, on obtient à nouveau $|x| = |x|_\infty^a$.

□

Nous terminons ce paragraphe avec la formule du produit dans $\mathbb{Q}$:

Proposition 2.2.6 *Pour tout $x \in \mathbb{Q}^*$, nous avons*

$$|x|_\infty \prod_{p \text{ premier}} |x|_p = 1.$$

Preuve. Il suffit de montrer le résultat pour tout $x \in \mathbb{Z}$. Soit donc x un entier ; par le théorème fondamental de l'arithmétique, nous avons :

$$|x|_\infty = \prod_{p \text{ premier}} p^{v_p(x)} = \prod_{p \text{ premier}} |x|_p^{-1} .$$

□

2.3 Valeurs absolues sur un corps de nombres

Nous allons étudier dans cette section les valeurs absolues sur un corps de nombres. Soit K un corps de nombres; à chaque plongement σ de K dans $\mathbb{C}$, nous pouvons associer une valeur absolue archimédienne normalisée $|\cdot|_\sigma$ en posant pour tout $x \in K$,

$$|x|_\sigma = |\sigma(x)|_\infty$$

où $|\cdot|_\infty$ désigne la valeur absolue archimédienne usuelle sur $\mathbb{C}$. Remarquons que, si τ est le plongement de K dans $\mathbb{C}$ complexe conjuguée de σ ($i.e. \tau(x) = \overline{\sigma}(x)$) alors clairement $|\cdot|_\sigma = |\cdot|_\tau$. Nous admettrons le théorème suivant qui caractérise les valeurs absolues archimédiennes d'un corps de nombres.

Théorème 2.3.1 *Soit K un corps de nombres.*

1. *Soient σ et τ deux plongements de K dans $\mathbb{C}$. Alors, les valeurs absolues $|\cdot|_\sigma$ et $|\cdot|_\tau$ sont équivalentes si et seulement si $\tau = \sigma$ ou $\tau = \overline{\sigma}$.*
2. *Toute valeur absolue archimédienne sur K est équivalente à une valeur absolue $|\cdot|_\sigma$, pour un certain plongement σ de K dans $\mathbb{C}$.*

□

Avant de définir des valeurs absolues ultramétriques de K, nous aurons besoin de faire quelques rappels sur la factorisation dans l'anneau des entiers d'un corps de nombres.

Soient K et L deux corps de nombres avec $K \subseteq L$. Soient aussi $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers de K et L respectivement, tels que $\mathfrak{q} \mid \mathfrak{p}$. On appelle

indice de ramification de $\mathfrak{q}$ sur $\mathfrak{p}$, et l'on note $e(\mathfrak{q},\mathfrak{p})$, le plus grand entier e tel que

$$\mathfrak{q}^e \mid \mathfrak{p}\ .$$

On appelle aussi degré d'inertie de $\mathfrak{q}$ sur $\mathfrak{p}$, et l'on note $f(\mathfrak{q},\mathfrak{p})$, l'entier défini par

$$f(\mathfrak{q},\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}].$$

L'indice de ramification et le degré d'inertie sont multiplicatif dans une tour d'extension : si $K \subseteq L \subseteq F$ sont trois corps de nombres et $\mathfrak{p}$, $\mathfrak{q}$ et $\mathfrak{f}$ sont trois idéaux premiers de K, L et F respectivement, tels que $\mathfrak{f} \mid \mathfrak{q} \mid \mathfrak{p}$, alors

$$e(\mathfrak{f},\mathfrak{p}) = e(\mathfrak{f},\mathfrak{q}) \times e(\mathfrak{q},\mathfrak{p})$$

et

$$f(\mathfrak{f},\mathfrak{p}) = f(\mathfrak{f},\mathfrak{q}) \times f(\mathfrak{q},\mathfrak{p})\,.$$

Rappelons également la notion de norme d'un idéal. Soit K un corps de nombre et I un idéal de $\mathcal{O}_K$. On appelle norme de I et l'on note $N(I)$ l'indice de I dans $\mathcal{O}_K$. La norme est une fonction multiplicative : si I et J sont deux idéaux d'un corps de nombres, alors $N(IJ) = N(I)N(J)$. Si $I = (\alpha)$ un idéal principal de K, alors $N(I) = |N_{\mathbb{Q}}^K(\alpha)|$. Enfin, si $\mathfrak{p}$ un idéal premier de K au dessus d'un premier rationnel p, alors $N(\mathfrak{p}) = p^{f(\mathfrak{p},p)}$.

Rappelons enfin le théorème de factorisation dans l'anneau des entiers d'un corps de nombres :

Théorème 2.3.2 *Soient K et L deux corps de nombres avec $K \subseteq L$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, et soit*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e(\mathfrak{q}_1,\mathfrak{p})}\mathfrak{q}_2^{e(\mathfrak{q}_2,\mathfrak{p})}\dots\mathfrak{q}_k^{e(\mathfrak{q}_k,\mathfrak{p})}\ ,$$

la décomposition de l'idéal $\mathfrak{p}$ en produit d'idéaux premiers de $\mathcal{O}_L$. Alors

$$\sum_{j=1}^{k} e(\mathfrak{q}_j,\mathfrak{p})f(\mathfrak{q}_j,\mathfrak{p}) = [L : K].$$

□

Nous pouvons désormais définir, de façon analogue aux valeurs absolues p-adiques sur $\mathbb{Q}$, des valeurs absolues ultramétriques sur un corps de nombres.

Définition 2.3.3 *Soit K un corps de nombres, et soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Notons p le premier rationnel en dessous de $\mathfrak{p}$.*

1. *On appelle valuation $\mathfrak{p}$-adique, l'application qui à tout $x \in K^*$ non nul*

associe :

$$v_{\mathfrak{p}}(x) = \frac{\lambda}{e(\mathfrak{p}, p)},$$

où $\lambda \in \mathbb{Z}$ est l'exposant de $\mathfrak{p}$ dans la décomposition de (x) en produit d'idéaux premiers de $\mathcal{O}_K$.

2. *On appelle valeur absolue $\mathfrak{p}$-adique sur K, l'application :*

$$\begin{array}{rccc} |\cdot|_{\mathfrak{p}} & : & K & \longrightarrow & \mathbb{R} \\ & & x & \longmapsto & p^{-v_{\mathfrak{p}}(x)} \end{array}.$$

Nous admettrons le théorème suivant qui caractérise les valeurs absolues ultramétriques non triviales d'un corps de nombres.

Théorème 2.3.4 *Soit K un corps de nombres.*

1. *Les valeurs absolues $|\cdot|_{\mathfrak{p}}$ ($\mathfrak{p} \subseteq \mathcal{O}_K$ idéal premier non nul) sont 2 à 2 non équivalentes ;*
2. *Toute valeur absolue ultramétrique non triviale sur K est équivalente à une valeur absolue $|\cdot|_{\mathfrak{p}}$, avec $\mathfrak{p} \subseteq \mathcal{O}_K$ idéal premier non nul.*

□

Soit K un corps de nombres. En utilisant, ce qui précède nous allons choisir pour toute place $v \in \mathcal{M}_K$ un représentant normalisé $|\cdot|_v$ de la classe d'équivalence de v. Si v est une place archimédienne (ce que l'on notera $v|\infty$), toute valeur absolue de v est équivalente à une valeur absolue $|\cdot|_\sigma$, où σ est l'un des plongements du corps K dans $\mathbb{C}$ (on dira dans la suite que la place v est associée à σ). Nous choisissons donc naturellement pour représentant de v la valeur absolue $|\cdot|_v = |\cdot|_\sigma$. Si v est une place ultramétrique (ce que l'on notera $v \nmid \infty$), toute valeur absolue de v est équivalente à une valeur absolue $|\cdot|_{\mathfrak{p}}$, où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$ (on dira de même que v est associée à $\mathfrak{p}$). Nous choisissons, là encore naturellement, pour représentant de v la valeur absolue $|\cdot|_v = |\cdot|_{\mathfrak{p}}$. Remarquons que pour tout $\alpha \in K$ il existe seulement un nombre fini de places v pour lesquelles $|\alpha|_v \neq 1$.

Pour toute place $v \in \mathcal{M}_K$, notons K_v et $\mathbb{Q}_v$ les complétés des corps K et $\mathbb{Q}$ (respectivement) pour la valeur absolue normalisée $|\cdot|_v$ et pour sa restriction à $\mathbb{Q}$ (respectivement), et posons

$$n_v = [K_v : \mathbb{Q}_v].$$

Proposition 2.3.5 *Soit K un corps de nombres et soit v une place de K. Si v est archimédienne, alors $n_v = 1$ (resp. $n_v = 2$), si v est associée à un plongement réel (resp. complexe) de K. Si v est ultramétrique, alors :*

$$n_v = e(\mathfrak{p}, p\mathbb{Z}) f(\mathfrak{p}, p\mathbb{Z}),$$

où $\mathfrak{p}$ est l'idéal premier associé à v et $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Nous ne démontrerons pas cette proposition ; le lecteur pourra la prendre comme définition de n_v.

Nous pouvons maintenant énoncer et démontrer la formule du produit.

Théorème 2.3.6 *Soit K un corps de nombres, pour tout $\alpha \in K^*$, nous avons*

$$\prod_{v \in \mathcal{M}_K} |\alpha|_v^{n_v} = 1.$$

Remarque. Comme dans le cas de la formule du produit sur $\mathbb{Q}$, le produit semble infini, mais il a cependant bien un sens, puisque $|\alpha|_v = 1$ pour presque tout place v de K (au sens de toutes sauf un nombre fini).
Preuve. Considérons la décomposition de l'idéal principal (α) en produit d'idéaux premiers de $\mathcal{O}_K$

$$(\alpha) = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_k^{a_k}$$

et notons p_j le premier rationnel en dessous de $\mathfrak{p}_j$; nous avons :

$$\begin{aligned} \prod_{\substack{v \in \mathcal{M}_K \\ v|\infty}} |\alpha|_v^{n_v} &= |N_{\mathbb{Q}}^K(\alpha)| \\ &= \prod_{j=1}^{k} N(\mathfrak{p}_j)^{a_j} \\ &= \prod_{j=1}^{k} p_j^{f(\mathfrak{p}_j, p_j) a_j} \\ &= \prod_{j=1}^{k} p_j^{e(\mathfrak{p}_j, p_j) f(\mathfrak{p}_j, p_j) v_{\mathfrak{p}_j}(\alpha)}. \end{aligned}$$

Puisque, nous avons aussi :

$$\prod_{\substack{v \in \mathcal{M}_K \\ v \nmid \infty}} |\alpha|_v^{n_v} = \prod_{\substack{\mathfrak{p} \text{ premier} \\ \mathfrak{p} \neq (0)}} |\alpha|_{\mathfrak{p}}^{e(\mathfrak{p}, \mathfrak{p} \cap \mathbb{Z}) f(\mathfrak{p}, \mathfrak{p} \cap \mathbb{Z})} = \prod_{j=1}^{k} p_j^{-e(\mathfrak{p}_j, p_j) f(\mathfrak{p}_j, p_j) v_{\mathfrak{p}_j}(\alpha)},$$

on obtient le résultat annoncé.

□

Définition 2.3.7 *Soient K et L deux corps de nombres tels que $K \subseteq L$, et soient v et w deux places de K et L (respectivement). On dit que w divise v, et l'on note $w \mid v$, si et seulement si $|\alpha|_v = |\alpha|_w$ pour tout $\alpha \in K$.*

La proposition suivante clarifie cette définition.

Proposition 2.3.8 *Soient K et L deux corps de nombres tels que $K \subseteq L$.*

1. *Soient $\sigma : K \to \mathbb{C}$ et $\tau : L \to \mathbb{C}$ deux plongements et notons v et w les places archimédiennes de K et L associées à σ et τ respectivement. Alors, w divise v si et seulement si la restriction de τ à K coincide avec σ ou avec $\overline{\sigma}$.*
2. *Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers non nuls de $\mathcal{O}_K$ et $\mathcal{O}_L$ respectivement et notons v et w les places ultramétriques de K et L associées à $\mathfrak{p}$ et $\mathfrak{q}$ respectivement. Alors, w divise v si et seulement si $\mathfrak{q}$ divise $\mathfrak{p}$.*

Preuve.

1. Clair d'après le théorème 2.3.1.
2. Supposons $\mathfrak{q} \nmid \mathfrak{p}$; alors il existe $\alpha \in \mathfrak{p} \backslash \mathfrak{q}$, et donc $|\alpha|_v < 1$ et $|\alpha|_w = 1$. Donc $w \nmid v$. Supposons maintenant que $\mathfrak{q} \mid \mathfrak{p}$ et soit $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. Notons a le plus grand entier tel que $\mathfrak{p}^a \mid (\alpha)$. On a alors :

$$v_{\mathfrak{q}}(\alpha) = \frac{a\, e(\mathfrak{q}, \mathfrak{p})}{e(\mathfrak{q}, \mathfrak{p} \cap \mathbb{Z})} = \frac{a}{e(\mathfrak{p}, \mathfrak{p} \cap \mathbb{Z})} = v_{\mathfrak{p}}(\alpha)$$

   et donc $w \mid v$.

□

Enfin, terminons ce paragraphe par une formule dont nous aurons besoin pour montrer que la hauteur absolue de Weil d'un nombre algébrique est indépendante du corps de nombres le contenant que l'on considère.

Proposition 2.3.9 *Soient K et L deux corps de nombres tels que $\mathbb{Q} \subseteq K \subseteq L$. Alors, pour toute place v de K, nous avons*

$$\sum_{\substack{w \in \mathcal{M}_L \\ w \mid v}} \frac{n_w}{n_v} = [L : K] \,.$$

Preuve. Soit v une place archimédienne ; d'après les propositions 2.3.5 et 2.3.8 il suffit de vérifier que le nombre de plongements de L dans $\mathbb{C}$ dont la restriction à K coincide avec le plongement σ associé à v est égal à $[L : K]$, ce qui est bien connu.

Dans le cas d'une place v ultramétrique, soit $\mathfrak{p}$ l'idéal premier non nul de $\mathcal{O}_K$ associé à v, et

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e(\mathfrak{q}_1,\mathfrak{p})}\mathfrak{q}_2^{e(\mathfrak{q}_2,\mathfrak{p})}\dots\mathfrak{q}_k^{e(\mathfrak{q}_k,\mathfrak{p})}\,,$$

la décomposition de $\mathfrak{p}\mathcal{O}_L$ en facteurs premiers dans $\mathcal{O}_L$. Nous avons (utiliser à nouveau les propositions 2.3.5 et 2.3.8) :

$$\sum_{\substack{w\in\mathcal{M}_L\\ w|v}} \frac{n_w}{n_v} = \sum_{j=1}^{k} \frac{e(\mathfrak{q}_j,\mathfrak{p}\cap\mathbb{Z})f(\mathfrak{q}_j,\mathfrak{p}\cap\mathbb{Z})}{e(\mathfrak{p},\mathfrak{p}\cap\mathbb{Z})f(\mathfrak{p},\mathfrak{p}\cap\mathbb{Z})} = \sum_{j=1}^{k} e(\mathfrak{q}_j,\mathfrak{p})f(\mathfrak{q}_j,\mathfrak{p}) = [L:K]\,.$$

□

Remarque. En particulier, pour tout corps de nombres K et tout premier rationnel p, nous avons,

$$\sum_{\substack{v\in\mathcal{M}_K\\ v|\infty}} n_v = \sum_{\substack{v\in\mathcal{M}_K\\ v|p}} n_v = [K:\mathbb{Q}]\,.$$

2.4 Hauteur de Weil d'un nombre algébrique

Soit $\alpha \in \overline{\mathbb{Q}}$ et K un corps qui contient α. On note provisoirement :

$$h_K(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v\in\mathcal{M}_K} n_v \log^+|\alpha|_v\,,$$

où $\log^+ x = \log\max(1,x)$ pour x réel ≥ 0.

Proposition 2.4.1 *La définition précédente ne dépend pas de K. Plus précisément, soient $K \subseteq L$ deux corps et $\alpha \in K$; alors*

$$h_K(\alpha) = h_L(\alpha)\,.$$

Preuve. Soit $\alpha \in K$; nous avons

$$\begin{aligned} h_L(\alpha) &= \frac{1}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_L} n_v \log^+ |\alpha|_v \\ &= \frac{1}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} \sum_{\substack{w \in \mathcal{M}_L \\ w|v}} n_w \log^+ |\alpha|_w \\ &= \frac{1}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} \Big(\sum_{\substack{w \in \mathcal{M}_L \\ w|v}} n_w \Big) \log^+ |\alpha|_v \ . \end{aligned}$$

Par la proposition 2.3.9, pour tout $v \in \mathcal{M}_K$ on a

$$\sum_{\substack{w \in \mathcal{M}_L \\ w|v}} n_w = [L:K] n_v \ ,$$

et donc :

$$h_L(\alpha) = \frac{[L:K]}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+ |\alpha|_v = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+ |\alpha|_v = h_K(\alpha) \ .$$

□

Cette proposition justifie la définition suivante :

Définition 2.4.2 *Soit $\alpha \in \overline{\mathbb{Q}}$ et soit K un corps de nombres contenant α. On appelle hauteur (absolue et logarithmique) de Weil α le nombre réel défini par :*

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

Il est aussi utile, dans certaines situations, de considérer la hauteur non logarithmique $H(\alpha) = \exp h(\alpha)$.

Proposition 2.4.3 *La fonction hauteur h vérifie, pour α, $\beta \in \overline{\mathbb{Q}}^*$, les propriétés suivantes.*

1. *$h(\alpha) \geq 0$. De plus : $h(\alpha) = 0$ si et seulement si α est une racine de l'unité.*
2. *$h(\alpha\beta) \leq h(\alpha) + h(\beta)$. De plus, si β est une racine de l'unité, on a $h(\alpha\beta) = h(\alpha)$.*
3. *Pour tout $n \in \mathbb{Z}$ on a $h(\alpha^n) = |n| h(\alpha)$.*

Preuve. Soit K un corps de nombres contenant α et β.

1. La première assertion est claire, d'après la définition. Pour montrer la deuxième, remarquons que :

$$h(\alpha) = 0 \iff |\alpha|_v \leq 1 \text{ pour toute place } v \in \mathcal{M}_K.$$

On en déduit que $h(\alpha) = 0$ si et seulement si α est un entier algébrique (en considérant les places ultramétriques) et si $|\sigma(\alpha)| \leq 1$ pour tout plongement σ de K dans $\mathbb{C}$ (en considérant les places archimédiennes). Par le théorème de Kronecker 1.4.2, nous en déduisons que $h(\alpha) = 0$ si et seulement si $\alpha = 0$ ou α est une racine de l'unité.

2. Pour toute place $v \in \mathcal{M}_K$, nous avons

$$\max(1, |\alpha\beta|_v) = \max(1, |\alpha|_v|\beta|_v) \leq \max(1, |\alpha|_v)\max(1, |\beta|_v)$$

et donc $h(\alpha\beta) \leq h(\alpha) + h(\beta)$. De plus, si β est une racine de l'unité, on a $h(\alpha\beta) \leq h(\alpha) + h(\beta) = h(\alpha)$ et $h(\alpha) \leq h(\alpha\beta) + h(\beta^{-1}) = h(\alpha\beta)$, d'où $h(\alpha\beta) = h(\alpha)$.

3. Montrons d'abord que $h(\alpha^{-1}) = h(\alpha)$. Pour toute place $v \in \mathcal{M}_K$, nous avons

$$\frac{\max(1, |\alpha|_v)}{\max(1, |\alpha^{-1}|_v)} = |\alpha|_v \ ,$$

et

$$\log^+|\alpha|_v - \log^+|\alpha^{-1}|_v = \log|\alpha|_v \, .$$

Par la formule du produit, nous obtenons

$$h(\alpha) - h(\alpha^{-1}) = \frac{1}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log|\alpha|_v = 0 \, .$$

Soit maintenant $n \in \mathbb{Z}$. Pour toute place $v \in \mathcal{M}_K$, nous avons

$$\log^+|\alpha^n|_v = \begin{cases} n \log^+|\alpha|_v & \text{si } n \geq 1 \\ |n| \log^+|\alpha^{-1}|_v & \text{si } n < 0. \end{cases}$$

La première égalité donne le résultat si n est positif, tandis que la deuxième (en combinant avec $h(\alpha^{-1}) = h(\alpha)$) donne le résultat si n est négatif.

□

2.5 Hauteur normalisée d'un polynôme

Nous nous proposons d'introduire une hauteur normalisée sur $\overline{\mathbb{Q}}[x]$ qui prolonge la notion de mesure de Mahler d'un polynôme à coefficients entiers. Commençons par la définition suivante :

Définition 2.5.1 *Soit K un corps de nombres, $P \in K[x]$ et $v \in M_K$. Si v est une place archimédienne associée au plongement σ de K dans $\overline{\mathbb{Q}}$, on pose $M_v(P) = M(\sigma P)$. Si v est une place ultramétrique, on définit $M_v(P)$ comme le maximum des valeur absolues v-adiques des coefficients de P.*

Lemme 2.5.2 *Soit K un corps de nombres, $P, Q \in K[x]$ et $v \in \mathcal{M}_K$. On a alors $M_v(PQ) = M_v(P)M_v(Q)$.*

Preuve. L'affirmation découle du fait que la mesure de Mahler est multiplicative si v est archimédienne ; supposons donc v ultramétrique. Soit $P = \sum_i a_i x^i$, $Q = \sum_j b_j x^j$ et $PQ = \sum_l c_l x^l$. Alors :

$$|c_l|_v = \Big| \sum_{i+j=l} a_i b_j \Big|_v \leq \max_{i+j=l} |a_i b_j|_v \leq M_v(P)M_v(Q)$$

et donc $M_v(PQ) \leq M_v(P)M_v(Q)$. Soit maintenant

$$r = \min\{i \text{ t.q. } |a_i|_v = M_v(P)\}$$

et

$$s = \min\{j \text{ t.q. } |b_j|_v = M_v(Q)\}\,.$$

On a alors : $|a_r b_s|_v = M_v(P)M_v(Q)$ et $|a_i b_j|_v < M_v(P)M_v(Q)$ pour $i + j = r + s$ et $(i, j) \neq (r, s)$. D'où :

$$|c_{r+s}|_v = \Big| a_r b_s + \sum_{\substack{i+j=r+s \\ (i,j)\neq(r,s)}} a_i b_j \Big|_v = M_v(P)M_v(Q)$$

et $M_v(PQ) \geq M_v(P)M_v(Q)$.

□

Définition 2.5.3 *Soit $P \in \overline{\mathbb{Q}}[x]$ un polynôme et soit K un corps de nombres contenant ses coefficients. On pose :*

$$\hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log M_v(P)\ .$$

Remarque. On vérifie, exactement comme dans la proposition 2.4.1 que cette définition ne dépend pas du choix du corps K.

Lemme 2.5.4 *La fonction $\hat{h}$ vérifie les propriétés suivantes :*

1. *Pour tout $\lambda \in \overline{\mathbb{Q}}^*$ et $P \in \overline{\mathbb{Q}}[x]$ on a $\hat{h}(\lambda P) = \hat{h}(P)$.*
2. *Pour tout $P, Q \in \overline{\mathbb{Q}}[x]$ on a $\hat{h}(PQ) = \hat{h}(P) + \hat{h}(Q)$.*
3. *Soit $\alpha \in \overline{\mathbb{Q}}^*$; alors : $\hat{h}(x - \alpha) = h(\alpha)$.*

Preuve.

1. On a :
$$\begin{aligned} \hat{h}(\lambda P) - \hat{h}(P) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v (\log M_v(\lambda P) - \log M_v(P)) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log |\lambda|_v = 0 \end{aligned}$$
par la formule du produit.
2. Clair, d'après le lemme 2.5.2.
3. En effet, si σ est un plongement de K dans $\overline{\mathbb{Q}}$ on a $M(x - \sigma\alpha) = \max(1, |\alpha|)$ et donc :
$$\begin{aligned} \hat{h}(x - \alpha) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log M_v(x - \alpha) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+ |\alpha|_v = h(\alpha) \, . \end{aligned}$$

□

On en déduit :

Théorème 2.5.5 *Soit $P \in \overline{\mathbb{Q}}[x]$ et notons $\alpha_1, \ldots, \alpha_D$ ses racines (comptées avec leur multiplicité). On a alors :*

$$\hat{h}(P) = \sum_{j=1}^{n} h(\alpha_j)$$

Preuve. Nous pouvons supposer (lemme précédent, point 1) P unitaire. On a alors (lemme précédent, points 2 et 3) :

$$\hat{h}(P) = \sum_{j=1}^{n} \hat{h}(x - \alpha_j) = \sum_{j=1}^{n} h(\alpha_j) \, .$$

□

On en déduit en particulier :

Corollaire 2.5.6 *Pour tout $P \in \overline{\mathbb{Q}}[x]$ on a $\hat{h}(P) \geq 0$ et $\hat{h}(P) = 0$ si et seulement si toutes les racines de P sont racines de l'unité.*

Corollaire 2.5.7 *Pour tout nombre algébrique α, nous avons*

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

Preuve. On choisit dans le théorème 2.5.5 pour P le polynôme minimal de α sur $\mathbb{Z}$. On a alors

$$M_p(P) = 1$$

pour tout premier rationnel p (car P est primitif) et

$$M_\infty(P) = M(P) .$$

On a donc, en notant $\alpha_1, \ldots, \alpha_D$ les conjugués de α,

$$\log M(P) = \sum_{j=1}^{D} h(\alpha_j) = Dh(\alpha) .$$

□

Corollaire 2.5.8 *Si α et β sont conjugués, alors $h(\alpha) = h(\beta)$.*

Preuve. Le polynôme minimal sur $\mathbb{Z}$ de α et β est le même.

□

Chapitre 3

Théorème de Dobrowolski

3.1 Problème de Lehmer

Soit α un nombre algébrique non nul de degré D, différent d'une racine de l'unité. A la suite du théorème de Kronecker, il est naturel de s'intéresser à minorer $h(\alpha)$. Remarquons tout de suite qu'obtenir une minoration par une constante pour tous les nombres algébriques est impossible. Il suffit en effet de considérer, pour tout entier D, l'entier algébrique $\alpha = 2^{1/D}$ dont la hauteur vaut

$$h(\alpha) = \frac{\log 2}{D};$$

elle est donc arbitrairement petite si son degré D est suffisamment grand.

Le problème de Lehmer (*voir* [6], § 13, page 476 et 477) consiste à déterminer quelle est la minoration optimale (en fonction de son degré D) de la hauteur $h(\alpha)$. Plus précisément, on fait la conjecture suivante :

Conjecture 3.1.1 *Il existe un nombre réel $c > 0$ tel que pour tout $\alpha \in \overline{\mathbb{Q}}^*$, de degré D sur $\mathbb{Q}$, qui n'est pas une racine de l'unité, on ait :*

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

On notera que Lehmer dans son texte était moins catégorique, et formulait plutôt la question en sens inverse.

Remarquons que dans le cadre du problème de Lehmer, on peut toujours supposer que α soit un entier algébrique. En effet, si α n'est pas un entier algébrique, il existe un nombre premier p et une valeur absolue non-

archimédienne $|\cdot|_v$ avec $v \mid p$ tels que $|\alpha|_v > 1$. On a donc

$$h(\alpha) \geq \frac{n_v \log |\alpha|_v}{D} \geq \frac{\log p}{D} \geq \frac{\log 2}{D} .$$

Le meilleur résultat connu à ce jour vers la conjecture 3.1.1 est la minoration de Dobrowolski ([3]) qui obtient (pour $D \geq 2$) :

$$h(\alpha) \geq \frac{1}{1200D} \left(\frac{\log \log D}{\log D} \right)^3 .$$

Pour des raffinements des constantes numériques, on pourra se reporter aux travaux de Louboutin (*voir* [8]), ou plus récemment, de Voutier (*voir* [15]).

Dans ce chapitre nous allons démontrer la version suivante du théorème de Dobrowolski :

Théorème 3.1.2 *Il existe une constante $c > 0$ telle que pour tout nombre algébrique $\alpha \neq 0$ de degré D qui n'est pas une racine de l'unité on a :*

$$h(\alpha) \geq \frac{c}{D} \left(\frac{\log \log 16D}{\log 16D} \right)^3 .$$

3.2 Congruences

La preuve du théorème de Dobrowolski repose sur le lemme clé suivant qui découle du petit théorème de Fermat :

Lemme 3.2.1 *Soient α un entier algébrique, et T un entier strictement positif. Soit $F \in \mathbb{Z}[X]$ un polynôme qui s'annule en α avec un ordre de multiplicité supérieur ou égal à T. Alors, pour tout premier p et toute place $v \in \mathcal{M}_{\mathbb{Q}(\alpha)}$ divisant p, nous avons*

$$|F(\alpha^p)|_v \leq p^{-T}$$

Preuve. Soit α un entier algébrique, et soit $P \in \mathbb{Z}[X]$ le polynôme minimal de α sur $\mathbb{Z}$. Nous avons :

$$P(X)^p \equiv P(X^p) \bmod p\mathbb{Z}[X] ,$$

pour tout premier p, et, en particulier,

$$P(\alpha^p) \equiv P(\alpha)^p \equiv 0 \bmod p\mathbb{Z}[\alpha]$$

et donc p divise $P(\alpha^p)$ dans $\mathcal{O}_{\mathbb{Q}(\alpha)} \supseteq \mathbb{Z}[\alpha]$. Il existe donc $\beta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ tel que $P(\alpha^p) = p\beta$; pour toute place $v \in \mathcal{M}_{\mathbb{Q}(\alpha)}$, nous avons alors :

$$|P(\alpha^p)|_v = |p|_v|\beta|_v = \frac{1}{p}|\beta|_v \leq \frac{1}{p} .$$

Soit $F \in \mathbb{Z}[X]$ un polynôme qui s'annule en α avec un ordre de multiplicité au moins T ; P^T divise F et il existe $G \in \mathbb{Z}[X]$ tel que

$$F(X) = P(X)^T G(X) .$$

Puisque α est un entier algébrique, nous obtenons

$$|F(\alpha^p)|_v = |P(\alpha^p)^T|_v|G(\alpha^p)|_v \leq p^{-T}|G(\alpha^p)|_v \leq p^{-T} .$$

□

Soient α un entier algébrique non nul de degré D et L, T deux entiers strictements positifs. Soit $F = \sum_{j=0}^{L} a_j X^j \in \mathbb{Z}[X]$ un polynôme de degré $\leq L$ qui s'annule en α avec un ordre de multiplicité supérieur ou égal à T. Soit p un nombre premier et soit $v \in \mathcal{M}_{\mathbb{Q}(\alpha)}$. Nous avons alors

$$|F(\alpha^p)|_v \leq p^{-T}$$

si $v \mid p$ (par le lemme précédent),

$$|F(\alpha^p)|_v \leq p^{-T}$$

si $v \nmid \infty$ (car $F(\alpha^p)$ est un entier algébrique), et enfin

$$|F(\alpha^p)|_v \leq \sum_{j=0}^{L} |a_j \alpha^{pj}| \leq \|F\|_1 \max(1, |\alpha|_v)^{pL}$$

si $v \mid \infty$. Si l'on peut construire un tel polynôme F tel que

$$F(\alpha^p) \neq 0 ,$$

alors la formule du produit (théorème 2.3.6) fournit l'inégalité :

$$1 = \prod_{v \in \mathcal{M}_{\mathbb{Q}(\alpha)}} |F(\alpha^p)|_v \leq (p^{-T})^D \|F\|_1^D H(\alpha)^{pDL} ,$$

puisque $\sum_{v|p} n_v = \sum_{v|\infty} n_v = D$. Sous ces hypothèses, nous obtenons :

$$h(\alpha) \geq \frac{T \log p - \log \|F\|_1}{pL}.$$

Par exemple, si α n'est pas une racine de l'unité, pour tout premier p, α^p n'est pas une racine du polynôme minimal P de α, et l'on a

$$h(\alpha) \geq \frac{\log p - \log \|P\|_1}{pD}\ .$$

Malheureusement, la longueur $\|P\|_1$ du polynôme P est difficile à controler (nous pourrions avoir, par exemple, $\log \|P\|_1 \gg D$), et c'est pourquoi, il va falloir construire un polynôme F, de petite longueur qui s'annule en α avec multiplicité (Lemme de Siegel). Il faudra ensuite nous assurer (Lemme de zéro) de l'existance d'un premier p tel que $F(\alpha^p) \neq 0$.

3.3 Lemme de Siegel

La construction de ce polynôme F est obtenue par l'utilisation de la version suivante d'un lemme classique de théorie de la transcendance (lemme de Siegel) :

Théorème 3.3.1 *Soit $\alpha \in \overline{\mathbb{Q}}$, un nombre algébrique de degré D, et soient L et T deux entiers strictement positifs vérifiant $L > DT$. Il existe un polynôme non nul $F \in \mathbb{Z}[X]$ vérifiant*

1. *F est de degré au plus L, et α est une racine de F de multiplicité au moins T.*
2. $\|F\|_\infty \leq 1 + \left(2^T (L+1)^{DT^2} H(\alpha)^{DTL}\right)^{1/(L+1-DT)}$

Nous allons prouver le théorème en considérant les opérateurs de dérivation

$$\partial_j = \frac{1}{j!} \frac{d^j}{dX^j}\ ,$$

et en construisant, à l'aide du principe des tiroirs de Dirichlet (comme dans [16], lemme 4.11), un polynôme F à coefficients entiers petits, tel que $|(\partial_j F)(\alpha)|$ soit petit pour $j = 0, \ldots, T-1$. En appliquant la formule du produit (théorème 2.3.6), nous en déduirons

$$(\partial_j F)(\alpha) = 0$$

pour $j = 0, \ldots, T-1$.

Lemme 3.3.2 *Soit K le corps $\mathbb{R}$ ou $\mathbb{C}$, et notons $n_\infty = [K : \mathbb{C}]$. Soient ensuite L et T deux entiers strictement positifs et $c_{i,j}$ ($i = 0, \ldots, T-1$; $j = 0, \ldots, L-1$) des éléments de K. Notons*

$$C = \max_{i=0,\ldots,T-1} \sum_{j=0}^{L} |c_{i,j}| \; .$$

Soient enfin M et l deux entiers strictement positifs, tels que

$$l^{Tn_\infty} < (M+1)^{L+1} \; .$$

Il existe alors un vecteur non nul $\mathbf{a} = (a_0, \ldots, a_L) \in \mathbb{Z}^L$, tel que

$$\max_{j=0,\ldots,L} |a_j| \leq M$$

et

$$\left| \sum_{j=0}^{L} c_{i,j} a_j \right| \leq \sqrt{n_\infty} \times \frac{CM}{l} \; .$$

Preuve. Nous allons prouver le lemme dans le cas où $K = \mathbb{R}$ (le cas $K = \mathbb{C}$ s'en déduisant alors aisément). La preuve repose sur le principe des tiroirs de Dirichlet. Considérons l'application

$$\begin{array}{rccc} f : & \mathbb{R}^{L+1} & \longrightarrow & \mathbb{R}^T \\ & \mathbf{a} = (a_0, \ldots, a_L) & \longmapsto & \left(\sum_{j=0}^{L} c_{i,j} a_j \right)_{i=0,\ldots,T-1} \end{array} \; ,$$

et posons pour tout $i \in \{0, \ldots, T-1\}$

$$A_i = \sum_{j=0}^{L} \max(0, -c_{i,j}) \text{ et } B_i = \sum_{j=0}^{L} \max(0, c_{i,j}) \; .$$

Nous avons $B_i + A_i \leq C$ pour tout $i \in \{0, \ldots, T-1\}$. Considérons l'hypercube $[0, M]^{L+1}$ et son image par φ :

$$\varphi([0,M]^{L+1}) \subseteq R = [-A_0 M, B_0 M] \times \cdots \times [-A_{T-1} M, B_{T-1} M] \; .$$

Nous allons appliquer le principe des tiroirs de Dirichlet à l'hyperrectangle R découpé en l^T hyperrectangles de $\mathbb{R}^T$ de longueur $M(B_i + A_i)/l$ en la coordonnée $i \in \{0, \ldots, T-1\}$. Puisque $l^T < (M+1)^{L+1}$, il existe deux

$L+1$ uplets distincts $\mathbf{b}$ et $\mathbf{c}$ de $\mathbb{Z}^{L+1}$ tels que $\varphi(\mathbf{b})$ et $\varphi(\mathbf{c})$ sont dans le même petit hyperrectangle. En notant $\mathbf{a} = \mathbf{b} - \mathbf{c}$, nous avons

$$\max_{j=0,\dots,L} |a_j| \leq M$$

et

$$\max_{i=0,\dots,T-1} |\varphi(\mathbf{a})_i| \leq \max_{i=0,\dots,T-1} \frac{M(B_i + A_i)}{l} \leq \frac{MC}{l} .$$

□

Preuve du Théorème 3.3.1 : Soit α un nombre algébrique de degré D et notons $K = \mathbb{Q}(\alpha)$ et $n_\infty = 1$ si α est réel et 2 sinon. Soient L et T deux entiers strictement positifs tels que $L > DT$. On applique le lemme précédent aux nombres complexes

$$c_{i,j} = \binom{j}{i} \alpha^{j-i}, \qquad (i = 0, \dots, T-1;\ j = 0, \dots, L) .$$

On a donc, grâce à la formule $\sum_{j=0}^{L} \binom{j}{i} = \binom{L+1}{i+1} \leq (L+1)^T$,

$$C = \max_{i=0,\dots,T-1} \sum_{j=i}^{L} \binom{j}{i} |\alpha^{j-i}| \leq (L+1)^T \max\{1, |\alpha|\}^L .$$

On choisit

$$M = 1 + \left[\left(2^T (L+1)^{DT^2} H(\alpha)^{DTL} \right)^{1/(L+1-DT)} \right] ,$$

et on choisit pour l un entier satisfaisant l'inégalité :

$$M^{L+1} \leq l^{Tn_\infty} < (M+1)^{L+1}$$

(remarquons qu'un tel entier existe, car $L + 1 \geq Tn_\infty$). Il existe alors un vecteur non nul $\mathbf{a} = (a_0, \dots, a_L) \in \mathbb{Z}^{L+1}$ vérifiant la conclusion du lemme. En posant

$$F(X) = \sum_{j=0}^{L} a_j X^j ,$$

nous avons donc

$$\|F\|_\infty \leq M$$

et

$$|(\partial_i F)(\alpha)| \leq \sqrt{n_\infty} \times \frac{CM}{l} \leq \frac{\sqrt{n_\infty}}{l} (L+1)^T M \max\{1, |\alpha|\}^L .$$

Par ailleurs, pour $i = 0, \dots, T-1$ et $v \in M_{\mathbb{Q}(\alpha)}$, l'inégalité triangulaire donne :

$$|(\partial_i F)(\alpha)|_v = |\sum_{j=i}^{L} \binom{j}{i} \alpha^{j-i} a_j|_v \leq \begin{cases} (L+1)^T M \max\{1, |\alpha|_v\}^L & \text{si } v \mid \infty \\ \max(1, |\alpha|_v)^L & \text{si } v \nmid \infty \end{cases}$$

(utiliser à nouveau $\sum_{j=0}^{L} \binom{j}{i} \leq (L+1)^T$ et l'inégalité ultramétrique).

Supposons $(\partial_i F)(\alpha) \neq 0$ pour un indice i avec $0 \leq i \leq T-1$; la formule du produit (théorème 2.3.6) fournit alors l'inégalité :

$$\begin{aligned} 1 &= \prod_{v \in \mathcal{M}_K} |\partial_i F)(\alpha)|_v^{n_v} \leq \left(\frac{\sqrt{n_\infty}}{l}\right)^{n_\infty} \times \left((L+1)^T M H(\alpha)^L\right)^D \\ &\leq l^{-n_\infty} \times 2(L+1)^{DT} M^D H(\alpha)^{DL} . \end{aligned}$$

On déduit alors du choix de l :

$$M^{L+1} \leq l^{Tn_\infty} \leq 2^T (L+1)^{DT^2} M^{DT} H(\alpha)^{DTL}$$

et

$$M \leq \left(2^T (L+1)^{DT^2} H(\alpha)^{DTL}\right)^{1/(L+1-DT)}$$

qui contredit le choix de M.

□

3.4 Preuve du théorème de Dobrowolski

La preuve suit les étapes classiques d'une démonstration de transcendance :

• *Réductions*

Pour montrer le théorème 3.1.2, on peut d'abord supposer que α soit un entier algébrique. En effet, si α n'est pas un entier algébrique, on a la minoration plus forte :

$$h(\alpha) \geq \frac{\log 2}{D}$$

(*voir* le paragraphe 3.1). Montrons, suivant Rausch [10] que l'on peut, de plus, supposer, par récurrence sur le degré de α, que pour tout entier $n \geq 1$

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

Soit en effet α un entier algébrique qui n'est pas une racine de l'unité et tel que

$$[\mathbb{Q}(\alpha^n) : \mathbb{Q}] < D$$

pour un certain entier $n \geq 1$ et considérons le polynôme

$$Q(X) = X^n - \alpha^n \in \mathbb{Q}(\alpha^n)[X] \; .$$

Nous avons $Q(\alpha) = 0$ et donc les conjugués de α sur $\mathbb{Q}(\alpha^n)$ sont de la forme $\zeta\alpha$, où ζ est une racine n-ième de l'unité. Posons

$$\beta = N_{\mathbb{Q}(\alpha^n)}^{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Q}(\alpha^n) \; ;$$

il existe alors une racine n-ième de l'unité ζ' telle que $\beta = \zeta'\alpha^D$, où l'on a posé $d = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)]$. Nous avons :

$$h(\beta) = h(\zeta'\alpha^D) = h(\alpha^D) = dh(\alpha)$$

et donc :

$$[\mathbb{Q}(\alpha) : \mathbb{Q}]h(\alpha) = \frac{[\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)]}h(\beta) = [\mathbb{Q}(\alpha^n) : \mathbb{Q}]h(\beta) \geq [\mathbb{Q}(\beta) : \mathbb{Q}]h(\beta).$$

Puisque $[\mathbb{Q}(\beta) : \mathbb{Q}] < D$, et puisque

$$\varepsilon(D) = \left(\frac{\log\log 16D}{\log 16D}\right)^3$$

est décroissante, on obtient alors, par hypothèse de récurrence,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}]h(\alpha) \geq [\mathbb{Q}(\beta) : \mathbb{Q}]h(\beta) \geq c\,\varepsilon([\mathbb{Q}(\beta) : \mathbb{Q}]) \geq c\,\varepsilon(D) \; .$$

• *Choix des paramètres*

On choisit trois paramètres L, T et N en fonction du degré D :

$$L = \left[C_0^2 D \left(\frac{\log 16D}{\log\log 16D}\right)\right], \qquad T = \left[C_0 \frac{\log 16D}{\log\log 16D}\right]$$

et

$$N = C_0^3 \frac{(\log 16D)^2}{\log\log 16D} \; .$$

Ci-dessus, C_0 désigne un nombre réel > 0 suffisamment grand : les inégalités que nous serons amenées à écrire seront vraies asymptotiquement en C_0. On notera aussi $c_1, c_2, \ldots$ des nombres réels > 0 (effectivement calculables).

Remarquons que :

$$\log(L+1) \le c_1(\log C_0)(\log 16D) \quad \text{et} \quad \log N \le c_1(\log C_0)(\log 16D) \ .$$

On suppose par l'absurde que

$$h(\alpha) < \frac{C_0^{-5}}{D}\left(\frac{\log\log 16D}{\log 16D}\right)^3 \ .$$

• *Construction de la fonction auxiliaire*

Le lemme de Siegel nous assure l'existance d'un polynôme F non nul à coefficient entier, de degré $\le L$, nul en α avec une multiplicité au moins T et tel que :

$$\|F\|_\infty \le 1 + \left(2^T(L+1)^{DT^2}H(\alpha)^{DTL}\right)^{1/(L+1-DT)} \ .$$

Les inégalités $\|F\|_1 \le (L+1)\|F\|_\infty$ et $L \ge 2DT$ donnent :

$$\begin{aligned} \|F\|_1 &\le (L+1)\left(1+(L+1)^{4DT^2/L}H(\alpha)^{2DT}\right) \\ &\le (L+1)^{2+4DT^2/L}H(\alpha)^{2DT} \end{aligned}$$

et donc :

$$\begin{aligned} \log\|F\|_1 &\le \left(2+\tfrac{4DT^2}{L}\right)\log(L+1) + 2DTh(\alpha) \\ &\le c_2 \log 16D \end{aligned}$$

• *Extrapolation*

Comme nous l'avons déjà signalé, nous avons, pour tout premier p et toute place $v \in \mathcal{M}_{\mathbb{Q}(\alpha)}$:

$$|F(\alpha^p)|_v \le \begin{cases} p^{-T} & \text{si } v \nmid \infty \text{ et } v \mid p \\ 1 & \text{si } v \nmid \infty \\ \|F\|_1 \max(1,|\alpha|_v)^{pL} & \text{si } v \mid \infty \end{cases}$$

Supposons qu'il existe un premier $p \in [\log 16D, N]$ tel que $F(\alpha^p) \neq 0$. En appliquant la formule du produit, nous obtenons

$$1 = \prod_{v\in\mathcal{M}_{\mathbb{Q}(\alpha)}} |F(\alpha^p)|_v^{n_v} \le p^{-TD}\|F\|_1^D H(\alpha)^{DpL} \ ,$$

et

$$\begin{aligned} T \log\log 16D &\leq \log \|F\|_1 + NLh(\alpha) \\ &\leq c_3 \log 16D \ . \end{aligned}$$

Par ailleurs :

$$T \log\log 16D \geq \frac{C_0}{2} \log 16D \ ,$$

contradiction. Le polynôme F s'annule donc en α^p pour tout premier $p \in [\log 16D, N]$.

• *Lemme de zéros*

Puisque α n'est pas une racine de l'unité, α^p et α^q ne sont pas conjugués pour $p \neq q$ (car sinon on aurait en particulier $ph(\alpha) = h(\alpha^p) = h(\alpha^q) = qh(\alpha)$ et donc $h(\alpha) = 0$). De plus, on a supposé $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] = D$ pour tout entier $n \geq 1$. Soit

$$\Sigma = \{\sigma(\alpha^p), \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\ p \text{ premier},\ \log 16D \leq p \leq N\} \ .$$

On a alors, en utilisant le théorème des nombres premiers,

$$\begin{aligned} \#\Sigma = \sum_{\log 16D \leq p \leq N} D &\geq D\left(c_4 \frac{N}{\log N} - c_5 \frac{\log 16D}{\log\log 16D}\right) \\ &\geq D \frac{c_6 C_0^3}{\log C_0} \frac{\log 16D}{\log\log 16D} > L \ , \end{aligned}$$

ce qui contredit le fait que le polynôme F est nul sur Σ.

□

Chapitre 4

Minorations de la hauteur dans une extension abélienne

4.1 Résultats

Dans la direction du problème de Lehmer, d'autres résultats partiels existent. On sait en particulier que si $\mathbb{Q}(\alpha)$ est totalement réel ou est un corps CM (c'est-à dire, une extension quadratique imaginaire d'un corps totalement réel), on sait obtenir des minorations bien plus fortes que celle de la conjecture 3.1.1 :

Théorème 4.1.1 (Schinzel [12]) *Soit K un corps totalement réel ou CM et soit $\alpha \in K^*$ un nombre algébrique tel que $|\alpha| \neq 1$; alors*

$$H(\alpha) \geq \sqrt{\frac{1+\sqrt{5}}{2}} = 1.272\ldots\ .$$

Même si l'hypothèse $|\alpha| \neq 1$ n'est pas restrictive si α est un entier algébrique (en effet, si K est un corps totalement réel ou CM et $|\alpha| = 1$, alors tous les conjugués de α sont de module 1, et donc α est une racine de l'unité par le théorème de Kronecker) elle devient contraignante dès que l'on cherche à minorer la hauteur de nombres algébriques qui ne sont pas forcément entiers. C'est donc intéressant de savoir si l'hypothèse $|\alpha| \neq 1$ peut être affaiblie en supposant seulement que α ne soit pas une racine de l'unité. Dans ce chapitre, nous allons donner une réponse affirmative à cette question dans le cas particulier des extensions abéliennes (une extension galoisienne $K \subset L$ est abélienne si le groupe de Galois $\mathrm{Gal}(L/K)$ est abélien; il est facile

de montrer qu'un corps de nombres L tel que $\mathbb{Q} \subset L$ est abélienne est en particulier un corps totalement réel ou CM). Plus précisément (*voir* [1]) :

Théorème 4.1.2 *Soit $L/\mathbb{Q}$ une extension abélienne et soit $\alpha \in L^*$, avec $\alpha \neq$ racine de l'unité, alors*

$$H(\alpha) \geq 5^{1/12} = 1.143\ldots$$

Pour simplifier la preuve, nous nous contenterons ici de montrer la minoration plus faible :

$$H(\alpha) \geq (5/2)^{1/10} = 1.095\ldots$$

Nous déduirons de cette minoration une nouvelle preuve du théorème de Smyth concernant les nombres algébriques non réciproques, et nous l'appliquerons également à la détermination du nombre de classes d'idéaux dans une extension abélienne.

4.2 Lemmes préliminaires

Notons dans toute la suite (m entier naturel, $m \not\equiv 2 \bmod 4$) $K_m = \mathbb{Q}(\xi_m)$, où ξ_m est une racine primitive m-ième de l'unité. Nous allons donner dans la proposition 4.3.1, une minoration de la hauteur d'un nombre algébrique $\alpha \in K_m^*$ qui n'est pas une racine de l'unité. L'idée de la preuve repose sur le lemme suivant :

Lemme 4.2.1 *Soit p un nombre premier ≥ 3. Il existe alors un morphisme $\sigma_p \in Gal(K_m/\mathbb{Q})$ ayant les propriétés suivantes :*

- *Si p ne divise pas m, alors $\gamma^p \equiv \sigma_p(\gamma) \bmod p\mathcal{O}_{K_m}$ pour tout $\gamma \in \mathcal{O}_{K_m}$.*
- *Si p divise m, alors $\gamma^p \equiv \sigma_p(\gamma^p) \bmod p\mathcal{O}_{K_m}$ pour tout $\gamma \in \mathcal{O}_{K_m}$. De plus, pour tout $\alpha \in \mathcal{O}_{K_m}$ vérifiant $\sigma_p(\alpha^p) = \alpha^p$, il existe une racine de l'unité $\xi \in K_m$ tel que $\xi\alpha \in K'$, où K' est une extension cyclotomique de $\mathbb{Q}$ strictement contenue dans K_m.*

Preuve. Supposons tout d'abord que p ne divise pas m, et soit $\sigma_p \in \mathrm{Gal}(K_m/\mathbb{Q})$ l'unique morphisme vérifiant $\sigma_p(\xi_m) = \xi_m^p$. Soit $\gamma \in \mathcal{O}_{K_m}$, il existe alors $F \in \mathbb{Z}[X]$ tel que $\gamma = F(\xi_m)$ (car l'anneau des entiers $\mathcal{O}_{K_m}$ de K_m est égal à $\mathbb{Z}[\xi_m]$). Or, pour tout polynôme $F \in \mathbb{Z}[X]$, il existe (par le petit théorème de Fermat) un polynôme $G \in \mathbb{Z}[X]$ tel que $F(X)^p = F(X^p) + pG(X)$. Nous avons donc :

$$\gamma^p = F(\xi_m)^p = F(\xi_m^p) + pG(\xi_m) \equiv \sigma_p(\gamma) \bmod p\mathcal{O}_{K_m}.$$

Supposons désormais que p divise m, et considérons cette fois σ_p un générateur du groupe $\mathrm{Gal}(K_m/K_{m/p})$ (qui est cyclique d'ordre p si p^2 divise m, et d'ordre $p-1$ sinon). Soit $\gamma \in \mathcal{O}_{K_m}$, il existe $F \in \mathbb{Z}[X]$ tel que $\gamma = F(\xi_m)$, et comme précédemment il existe un polynôme $G \in \mathbb{Z}[X]$ tel que $F(X)^p = F(X^p) + pG(X)$. On a alors :

$$\gamma^p = F(\xi_m)^p \equiv F(\xi_m^p) \bmod p\mathcal{O}_{K_m}$$

et

$$\sigma_p(\gamma^p) = \sigma_p\big(F(\xi_m)^p\big) \equiv \sigma_p\big(F(\xi_m^p)\big) \bmod p\mathcal{O}_{K_m}\,.$$

Par ailleurs, puisque $\xi_m^p \in K_{m/p}$, on a $\sigma_p(\xi_m^p) = \xi_m^p$, et par suite $F(\xi_m^p) = \sigma_p F(\xi_m^p)$. On a donc $\gamma^p \equiv \sigma_p(\gamma^p) \bmod p\mathcal{O}_{K_m}$.

Supposons enfin qu'il existe $\alpha \in K_m$ tel que $\sigma_p(\alpha^p) = \alpha^p$. Puisque $\sigma_p(\xi_m)^p = \xi_m^p$ et puisque σ_p est un générateur de $\mathrm{Gal}(K_m/K_{m/p})$, nous avons

$$\sigma_p(\xi_m) = \xi_p \xi_m,$$

où ξ_p est une racine p-ième primitive de l'unité. Par le même argument, il existe un entier u tel que $\sigma_p(\alpha) = \xi_p^u \alpha$. Nous en déduisons

$$\sigma_p\left(\frac{\alpha}{\xi_m^u}\right) = \frac{\xi_p^u \alpha}{\xi_p^u \xi_m^u} = \frac{\alpha}{\xi_m^u},$$

Donc σ_p est générateur de $\mathrm{Gal}(K_m/K_{m/p})$, et laisse fixe α/ξ_m^u ; on en déduit que $\alpha/\xi_m^u \in K_{m/p}$, ce qui achève la preuve du lemme.

□

Nous aurons aussi besoin du lemme suivant, qui nous assure de l'esistance d'un dénominateur local dans un corps de nombres.

Lemme 4.2.2 *Soient K un corps de nombres, α un élément de K^*, et $v \in \mathcal{M}_K$ une valeur absolue ultramétrique sur K, alors il existe un entier algébrique $\beta \in \mathcal{O}_K$, tel que $\beta\alpha \in \mathcal{O}_K$, et $|\beta|_v = \max(1, |\alpha|_v)^{-1}$*

Preuve. Fixons une place archimédienne quelconque w_0, et notons Σ l'ensemble fini de places ultramétriques suivantes :

$$\Sigma = \{w \in \mathcal{M}_K,\, w \nmid \infty,\ \text{et } |\alpha|_w > 1\} \cup \{v\}.$$

Notons ensuite, pour $w \in \Sigma$,

$$\theta_w = \begin{cases} \alpha, & \text{si } |\alpha|_w > 1\ ; \\ \\ 1, & \text{si } |\alpha|_w \leq 1 \end{cases}$$

de telle sorte que $|\theta_w|_w = \max(1, |\alpha|_w)$.

D'après le théorème d'approximation forte [2, Chapter II, Section 15, p. 67] il existe un élément $\beta \in K$ tel que :

$$\begin{cases} |\beta - \theta_w^{-1}|_w < |\theta_w|_w^{-1}, & \text{pour tout } w \in \Sigma\ ; \\ |\beta|_w \leq 1, & \text{si } w \notin \Sigma \text{ et } w \neq w_0\ . \end{cases}$$

En utilisant l'inégalité ultramétrique, on en déduit donc :

$$\begin{cases} |\beta|_w = \max(1, |\alpha|_w)^{-1}, & \text{pour tout } w \in \Sigma\ ; \\ |\beta|_w \leq 1, & \text{si } w \notin \Sigma \text{ et } w \nmid \infty\ . \end{cases}$$

En particulier, pour toute place finie w de K on a $|\beta|_w \leq 1$ et $|\beta\alpha|_w \leq 1$ (et donc β, $\beta\alpha \in \mathcal{O}_K$). Enfin, on a bien

$$|\beta|_v = \max(1, |\alpha|_v)^{-1}$$

(car $v \in \Sigma$). Le lemme 4.2.2 est donc établi.

□

4.3 Preuve du résultat principal

Proposition 4.3.1 *Soit α un nombre algébrique non nul appartenant à un corps cyclotomique K_m. Supposons que α ne soit pas une racine de l'unité.*

- *Si p est un nombre premier ne divisant pas m, on a :*

$$h(\alpha) \geq \frac{\log(p/2)}{p+1}\,.$$

- *Supposons de plus que pour toute racine de l'unité ζ le corps $\mathbb{Q}(\zeta\alpha)$ ne soit pas contenu dans un corps cyclotomique K' avec $K' \subsetneq K_m$. On a alors, pour tout nombre premier p divisant m,*

$$h(\alpha) \geq \frac{\log(p/2)}{2p}\,.$$

Preuve. Supposons tout d'abord que p ne divise pas m. Nous allons chercher à majorer $|\alpha^p - \sigma_p(\alpha)|_v$, pour toute place v afin d'obtenir, en utilisant la formule du produit(théorème 2.3.6), l'inégalité reliant la hauteur logarithmique de α à p. Soit $v \in \mathcal{M}_{K_m}$, $v \mid p$. Par le lemme 4.2.2, il existe $\beta \in \mathcal{O}_{K_m}$,

tel que $\beta\alpha \in \mathcal{O}_{K_m}$, et $|\beta|_v = \max\{1, |\alpha|_v)^{-1}$, et par le lemme 4.2.1, il existe un morphisme $\sigma_p \in \mathrm{Gal}(K_m/\mathbb{Q})$ tel que $(\alpha\beta)^p - \sigma_p(\alpha\beta)$, $\beta^p - \sigma_p(\beta) \in p\mathcal{O}_{K_m}$ et donc :

$$|(\alpha\beta)^p - \sigma_p(\alpha\beta)|_v \leq \frac{1}{p}$$

et de même :

$$|\beta^p - \sigma_p(\beta)|_v \leq \frac{1}{p}\,.$$

Nous avons alors :

$$\begin{aligned}
|\alpha^p - \sigma_p(\alpha)|_v &= |\beta|_v^{-p}|(\alpha\beta)^p - \sigma_p(\alpha\beta) + (\sigma_p(\beta) - \beta^p)\sigma_p(\alpha)|_v \\
&\leq |\beta|_v^{-p} \max\left(|(\alpha\beta)^p - \sigma_p(\alpha\beta)|_v, |\sigma_p(\beta) - \beta^p|_v |\sigma_p(\alpha)|_v\right) \\
&\leq \frac{1}{p}|\beta|_v^p \max\left(1, |\sigma_p(\alpha)|_v\right) \\
&= \frac{1}{p}\max\left(1, |\alpha|_v\right)^p \max\left(1, |\sigma_p(\alpha)|_v\right)
\end{aligned}$$

Pour les autres valeurs absolues ultramétriques, nous obtenons en utilisant l'inégalité ultramétrique :

$$|\alpha^p - \sigma_p(\alpha)|_v \leq \max\left(1, |\alpha|_v\right)^p \max\left(1, |\sigma_p(\alpha)|_v\right).$$

Et enfin pour les valeurs absolues archimédiennes, nous obtenons par l'inégalité triangulaire :

$$|\alpha^p - \sigma_p(\alpha)|_v \leq 2\max\left(1, |\alpha|_v\right)^p \max\left(1, |\sigma_p(\alpha)|_v\right).$$

Puisque par hypothèse, $\alpha \neq 0$ et α n'est pas une racine de l'unité, nous avons $\alpha^p - \sigma_p(\alpha) \neq 0$. En effet, l'hypothèse contraire impliquerait $ph(\alpha) = h(\alpha^p) = h(\sigma_p(\alpha)) = h(\alpha)$, et donc $h(\alpha) = 0$, ce qui d'après le théorème de Kronecker 1.4.2 entraînerait une contradiction. Nous pouvons donc appliquer la formule du produit à $\alpha - \sigma_p(\alpha)$, et nous obtenons, grâce à la

proposition 2.3.9,

$$\begin{aligned}
0 &= \sum_{v\in\mathcal{M}_{K_m}} n_v \log|\alpha-\sigma_p(\alpha)|_v \\
&\leq \sum_{\substack{v\in\mathcal{M}_{K_m}\\ v|p}} n_v \log\frac{1}{p} + \sum_{\substack{v\in\mathcal{M}_{K_m}\\ v|\infty}} n_v \log 2 \\
&\qquad + p\sum_{v\in\mathcal{M}_{K_m}} n_v \log\max(1,|\alpha|_v) + \sum_{v\in\mathcal{M}_{K_m}} n_v \log\max(1,|\sigma_p(\alpha)|_v) \\
&= [K_m:\mathbb{Q}]\left(\log\frac{2}{p} + ph(\alpha) + h(\sigma_p(\alpha))\right) \\
&= [K_m:\mathbb{Q}]\left(-\log\frac{p}{2} + (p+1)h(\alpha)\right)
\end{aligned}$$

qui donne bien l'inégalité recherchée.

Dans le cas où p divise m, nous pouvons montrer *mutatis mutandis* la seconde inégalité en remplaçant naturellement $\sigma_p(\alpha)$ par $\sigma_p(\alpha^p)$, en utilisant les lemmes 4.2.1 et 4.2.2. Nous avons alors les inégalités

$$|\alpha^p-\sigma_p(\alpha^p)|_v \leq \begin{cases} \dfrac{1}{p}\max(1,|\alpha|_v)^p \max(1,|\sigma_p(\alpha)|_v)^p & \text{si } v|p \\ \max(1,|\alpha|_v)^p \max(1,|\sigma_p(\alpha)|_v)^p & \text{si } v\nmid p \text{ et } v\nmid\infty \\ 2\max(1,|\alpha|_v)^p \max(1,|\sigma_p(\alpha)|_v)^p & \text{si } v|\infty \end{cases}$$

à partir desquelles, en appliquant la formule du produit [1] à $\alpha^p-\sigma_p(\alpha)^p$, nous déduisons

$$0 \leq [K_m:\mathbb{Q}]\left(-\log\frac{p}{2} + 2ph(\alpha)\right)$$

qui fournit là encore l'inégalité attendue.

□

Preuve du théorème 4.1.2 : Soit α un nombre algébrique ($\alpha\neq 0$, $\alpha\neq$ racine de l'unité) appartenant à une extension abélienne de $\overline{\mathbb{Q}}$. Notons K_m le plus petit corps cyclotomique tel qu'il existe une racine de l'unité ζ

1. On remarquera que $\alpha^p-\sigma_p(\alpha)^p$ est différent de 0 par le choix du morphisme σ_p (*cf* lemme 4.2.1) et par l'hypothèse faite sur K_m

pour laquelle $\zeta\alpha \in K_m$ (ce corps existe par le théorème de Kronecker-Weber : toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique). La proposition précédente, avec $p = 5$, donne alors :

$$h(\alpha) = h(\zeta\alpha) \geq \min\left(\frac{\log(5/2)}{6}, \frac{\log(5/2)}{10}\right) = \frac{\log(5/2)}{10}\,.$$

□

4.4 Minoration de la norme dans une extension abélienne et applications.

Nous allons tout d'abord énoncer un lemme reliant la norme d'un entier algébrique $\gamma \in \mathcal{O}_L$ à la hauteur logarithmique absolue de $\gamma/\overline{\gamma}$, valable dans toute extension $L/\mathbb{Q}$ abélienne.

Lemme 4.4.1 *Soit L une extension abélienne de $\mathbb{Q}$, et soit $\gamma \in \mathcal{O}_L \setminus \{0\}$, alors*

$$\log|N_{\mathbb{Q}}^{L}(\gamma)| \geq [L:\mathbb{Q}]\ h(\overline{\gamma}/\gamma)\,.$$

Preuve. Soit $\gamma \in \mathcal{O}_L \setminus \{0\}$, posons $\alpha = \overline{\gamma}/\gamma$. Pour toute valeur absolue archimédienne v, nous avons $|\alpha|_v = 1$. En effet, associée à une telle valeur absolue, il existe un morphisme $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $|\alpha|_v = |\sigma(\alpha)|_\infty$, et

$$|\alpha|_v^2 = \sigma(\alpha)\overline{\sigma(\alpha)} = \sigma(\alpha)\sigma(\overline{\alpha}) = \sigma(|\alpha|^2) = 1\,,$$

car la conjugation complexe commute avec σ. D'où, en appliquant la formule du produit 2.3.6 à γ , nous obtenons :

$$\begin{aligned}
[L:\mathbb{Q}]h(\alpha) &= \sum_{\substack{v\in\mathcal{M}_L\\ v\nmid\infty}} n_v \log^+|\alpha|_v \\
&= \sum_{\substack{v\in\mathcal{M}_L\\ v\nmid\infty}} n_v \log^+|\alpha|_v + \sum_{v\in\mathcal{M}_L} n_v \log|\gamma|_v \\
&= \sum_{\substack{v\in\mathcal{M}_L\\ v\nmid\infty}} n_v \log\max\left(|\overline{\gamma}|_v\,,|\gamma|_v\right) + \sum_{\substack{v\in\mathcal{M}_L\\ v|\infty}} n_v \log|\gamma|_v \\
&\leq \sum_{\substack{v\in\mathcal{M}_L\\ v|\infty}} n_v \log|\gamma|_v
\end{aligned}$$

puisque γ et $\overline{\gamma}$ sont des entiers algébriques, et donc $|\gamma|_v \leq 1$ et $|\overline{\gamma}|_v \leq 1$ pour toute valeur absolue $|\cdot|_v$ ultramétrique.

Or,

$$N_{\mathbb{Q}}^{L}(\gamma) = \prod_{\substack{v \in \mathcal{M}_L \\ v|\infty}} |\gamma|_v^{n_v} ,$$

nous en déduisons l'inégalité annoncée

$$\log |N_{\mathbb{Q}}^{L}(\gamma)| \geq [L : \mathbb{Q}]\ h\left(\frac{\gamma}{\overline{\gamma}}\right).$$

□

4.4.1 Corps cyclotomiques principaux.

En utilisant les techniques précédentes, on peut montrer qu'il y a exactement 29 corps cyclotomiques K_m dont l'anneau des entiers est principal[2]. Nous nous contenterons ici de donner quelques exemples.

Lemme 4.4.2 *Supposons que l'anneau des entiers du corps cyclotomique K_m soit principal, alors pour tout premier $p \equiv 1 \bmod m$, il existe un entier algébrique $\gamma \in K_m$ tel que $N_{\mathbb{Q}}^{K_m}\gamma = p$ et tel que $\gamma/\overline{\gamma}$ ne soit pas une racine de l'unité.*

Preuve. L'hypothèse sur p nous assure que ce premier est totalement décomposé dans l'anneau des entiers de K_m. Soit $\wp$ un premier au dessus de p et soit γ un générateur de $\wp$; on a donc $N_{\mathbb{Q}}^{K_m}\gamma = p$. De plus $\wp \neq \overline{\wp}$ (car p est totalement décomposé) et donc $\gamma/\overline{\gamma}$ n'est pas une racine de l'unité.

□

Corollaire 4.4.3 *Il n'existe qu'un nombre fini de corps cyclotomiques dont l'anneau des entiers est principal.*

Preuve. Le théorème de Linnik, un résultat profond de théorie analytique des nombres, montre qu'il existe une constante $L > 0$ tel que pour tout entier $m \geq 2$, il existe un nombre premier p vérifiant $p \equiv 1, \bmod m$ et $p < m^L$. Soit donc m un entier ≥ 2 et supposons que l'anneau des entiers du corps cyclotomique K_m soit principal ; le lemme précédent donne alors un entier algébrique $\gamma \in K_m$ tel que $N_{\mathbb{Q}}^{K_m}\gamma < m^L$ et tel que $\gamma/\overline{\gamma}$ ne soit pas une racine

2. En fait, ce résultat est connu depuis 1976 [9].

de l'unité. En appliquant le lemme 4.4.1 et le théorème 4.1.2, on en déduit la minoration :

$$L \log m \geq \varphi(m) c_1$$

où φ désigne la fonction indicatrice d'Euler et c_1 est une constante absolue. Par le théorème de Mertens [4, Theorem 429], il existe une constante absolue $c_2 > 0$, telle que

$$\varphi(m) \geq c_2 \frac{m}{\log m}$$

Les inégalités précédentes entraînent :

$$L \log m \geq c_1 c_2 \frac{m}{\log m} .$$

Nous en déduisons que m est majoré par une constante (effectivement calculable en fonction de L, c_1 et c_2).

□

Corollaire 4.4.4 *L'anneau des entiers de K_{100} n'est pas principal.*

Preuve. Supposons par l'absurde que l'anneau des entiers $\mathcal{O}$ de K_{100} soit principal. Le premier $p = 101$ est totalement décomposé dans $\mathcal{O}$; d'après les lemmes 4.4.1 et 4.4.2, on en déduit l'existance d'un certain $\alpha \in K_{100}^*$ tel que

$$h(\alpha) \leq \frac{\log 101}{\varphi(100)} \leq 0.12$$

et tel que α n'est pas une racine de l'unité. Pour la proposition 4.3.1 (avec $m = 100$ et $p = 7$), on a :

$$h(\alpha) \geq \frac{\log (7/2)}{8} \geq 0.15 .$$

□

Par des raisonnements analogues, il est possible d'obtenir une estimation de l'exposant du groupe de classes d'une extension cyclotomique sur $\mathbb{Q}$. Enfin, sous l'hypothèse de Riemann généralisée, on peut encore plus généralement minorer l'exposant du groupe de classes d'une extension CM quelconque.

4.4.2 Hauteur d'un entier algébrique non réciproque

Le théorème 4.1.2 permet d'obtenir une nouvelle démonstration d'un théorème de Smyth sur les nombres algébriques non réciproques (avec cependant une constante moins bonne). Rappelons qu'un polynôme $F \in \mathbb{C}[X]$ est dit réciproque si son ensemble de racines est invariant sous l'action de l'involution $z \longmapsto z^{-1}$ (*i.e.* si $F =$ constante $\times F^*$, où $F^*(X) = X^{\deg F} F(1/X)$ est le polynôme réciproque de F) et qu'un nombre algébrique est réciproque si son ensemble de conjugués est invariant sous l'action de cette même involution.

Théorème 4.4.5 *Soit $\alpha \neq 0$ un nombre algébrique non réciproque de degré D, alors*

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

où $c = \frac{\log(7/2)}{8} \approx 0.15659....$

Ce théorème a été démontré pour la première fois en 1971 par C. J. Smyth (*voir* [14]) avec la constante $c = \log\theta \approx 0.281199...$, où θ est la racine réelle de $X^3 - X - 1 = 0$. Remarquons que $h(\theta) = (\log\theta)/3$ (car les autres racines de $X^3 - X - 1$ ont module < 1) ; le resultat de Smyth est donc optimal.

Lemme 4.4.6 *Soit α un entier algébrique non réciproque de degré D et notons F son polynôme minimal sur $\mathbb{Z}$. Soit aussi p un nombre premier, $p \geq 3$. Notons $\gamma_p = F(\xi_p)$ où $\xi_p = \exp(2\pi i/p)$. Alors $\gamma_p/\overline{\gamma_p}$ n'est pas une racine de l'unité.*

Remarque. L'hypothèse de non réciprocité de α est nécessaire ; en effet, dans le cas contraire, nous avons $\gamma_p = F(\xi_p)$ et $F(X) = X^D F(\frac{1}{X})$ entraîne $\overline{\gamma_p} = F(\overline{\xi_p}) = F(\xi_p^{-1}) = \xi_p^{-D} F(\xi_p)$ et $\gamma_p/\overline{\gamma_p} = \xi_p^{-D}$.

Preuve. Par construction, $\gamma_p/\overline{\gamma_p} \in K_p$. Supposons par l'absurde que $\gamma_p/\overline{\gamma_p}$ soit une racine de l'unité. Alors nécessairement $\gamma_p/\overline{\gamma_p}$ est soit une racine p-ième, soit une racine $2p$-ième de l'unité. Il existe donc $i \in \{0, 1\}$ et $j = -1, \ldots, p-2$ tel que

$$\gamma_p/\overline{\gamma_p} = (-1)^i \xi_p^j \, .$$

Puisque $\overline{\gamma_p} = F(\xi_p^{-1})$, on a $F(\xi_p) = (-1)^i \xi_p^j F(\xi_p^{-1})$, et :

$$\xi_p^D F(\xi_p) = (-1)^i \xi_p^j F^*(\xi_p) \, .$$

Posons

$$G(X) = X^{\max(D-j,0)} F(X) + (-1)^{i+1} X^{\max(j-D,0)} F^*(X) \, .$$

D'après la remarque précédente, nous avons $G(\xi_p) = 0$. De plus, $G \neq 0$, puisque F ne divise ni X, ni F^* (car F et F^* sont de même degré, et α est non réciproque). Donc le p-ième polynôme cyclotomique divise G, et comme G est non nul, $\deg G \geq p-1$. Or

$$\deg G \leq |D-j| + D \leq \max(2D-j, j) \leq \max(2D+1, p-2)$$

par le choix de j, et pour $p \geq 2D+3$ nous obtenons une contradiction.

Donc $\gamma_p/\overline{\gamma_p}$ n'est pas une racine de l'unité pour tout premier $p \geq 2D+3$. □

Preuve du théorème 4.4.5. Nous pouvons supposer que α est un entier algébrique non réciproque (en effet, dans le cas contraire, nous avons déjà vu (paragraphe 3.1) que $h(\alpha) \geq (\log 2)/D$). Avec les notations du lemme précédent, pour tout premier $l \geq \max(2D+3, 11)$, nous avons $\gamma_l/\overline{\gamma_l} \in K_l^*$, et de plus $\gamma_l/\overline{\gamma_l}$ n'est pas une racine de l'unité ; donc d'après la proposition 4.3.1 (avec $m = l$ et $p = 7$) et le lemme 4.4.1 :

$$\frac{1}{l-1} \log \left| N_{\mathbb{Q}}^{K_l}(\gamma_l) \right| \geq h(\gamma_l/\overline{\gamma_l}) \geq \frac{\log(7/2)}{8} .$$

Par ailleurs,

$$\left| N_{\mathbb{Q}}^{K_l}(\gamma_l) \right| = \left| \prod_{j=1}^{l-1} F(\xi_l^j) \right| ,$$

et en notant $\alpha_1, \ldots, \alpha_D$ les conjugués de α, on obtient

$$\left| N_{\mathbb{Q}}^{K_l}(\gamma_l) \right| = \left| \prod_{j=1}^{l-1} \prod_{i=1}^{D} \left(\alpha_i - \xi_l^j \right) \right| = \left| \prod_{i=1}^{D} \prod_{j=1}^{l-1} \left(\alpha_i - \xi_l^j \right) \right| .$$

D'autre part, nous avons $\prod_{j=1}^{l-1} \left(X - \xi_l^j \right) = X^{l-1} + X^{l-2} + \cdots + X + 1$, d'où

$$\begin{aligned} \left| N_{\mathbb{Q}}^{K_l}(\gamma_l) \right| &= \left| \prod_{i=1}^{D} (1 + \alpha_i + \cdots + \alpha_i^{l-1}) \right| \\ &\leq \prod_{i=1}^{D} \left(l \max(1, |\alpha_i|)^{l-1} \right) \\ &\leq l^D H(\alpha)^{D(l-1)} \end{aligned}$$

et

$$\frac{D\log l + D(l-1)h(\alpha)}{l-1} \geq h(\gamma_l/\overline{\gamma_l}) \geq \frac{\log(7/2)}{8} \ .$$

En faisant tendre l vers l'infini, nous obtenons le résultat.

□

Chapitre 5

Théorèmes de comptage

5.1 Résultats

Soit K un corps de nombres et soit H un nombre réel. Le théorème de Northcott 1.4.1 montre en particulier que l'ensemble

$$K(H) = \{\alpha \in K \mid H(\alpha) \leq H\}$$

est fini. Un résultat de 1979 de S. Schanuel donne une estimation asymptotique du cardinal de $K(H)$.

Théorème 5.1.1 (Schanuel [11]) *Soit K un corps de nombres de degré D et soient h_K le nombre de classes, R_K le régulateur, ω_K le nombre de racines de l'unité, d_K le discriminant, r_1 et $2r_2$ le nombre de plongements réels et complexes (respectivement), et ζ_K la fonction zeta de K. Notons $K(H)$ l'ensemble des éléments α de K dont la hauteur absolue $H(\alpha)$ est majorée par H. On a alors, pour $H \to \infty$,*

$$\#K(H) = S_K(1)H^{2D} + O\left(H^{2D-1}\right) ,$$

avec

$$S_K(1) = \frac{h_K R_K/\omega_K}{\zeta_K(2)} \left(\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_K|}}\right)^2 2^{r_1+r_2-1} .$$

□

Malheureusement, le terme d'erreur semble difficile à rendre explicite. En 1993, W. M. Schmidt a donné une majoration explicite du cardinal de

$K(H)$:

Théorème 5.1.2 (Schmidt [13]) *Soit K un corps de nombres de degré D, et soit $H > 0$. En notant $K(H)$ l'ensemble des éléments α de K dont la hauteur absolue $H(\alpha)$ est majorée par H, nous avons*

$$\#K(H) \leq 32 \cdot 2^D H^{2D} .$$

□

Pour de petites valeurs de H, la dépendance exponentielle en le degré du corps K n'est pas satisfaisante, comme nous le verrons dans la prochaine remarque. Le théorème suivant donne une majoration explicite du cardinal de $K(H)$, avec une dépendance quasi-linéaire en le degré de K (en dehors du terme H^{2D}, inévitable d'après le théorème de Schanuel) :

Théorème 5.1.3 (Loher [7]) *Soit K un corps de nombres de degré $D \geq 2$, et soit $H > 0$. En notant $K(H)$ l'ensemble des éléments α de K dont la hauteur absolue $H(\alpha)$ est majorée par H, nous avons*

$$\#K(H) \leq 37 \cdot (D \log D) H^{2D}.$$

Remarque. D'après le théorème de Kronecker 1.4.2, nous avons

$$\#K(1) = 1 + \omega_K ,$$

pour tout corps de nombres K, où ω_K est le nombre de racines de l'unité dans K. En considérant un corps cyclotomique $K = \mathbb{Q}(\xi_n)$, où $\xi_n = \exp(2i\pi/n)$, nous avons $\omega_K \geq n$ et $D = \varphi(n)$. Donc

$$\#K(1) > n \geq \text{constante} \times D \log\log D$$

(utiliser l'estimation asymptotique de Mertens $\varphi(n) \sim e^{-\gamma} n (\log\log n)^{-1}$, *voir* [4, Theorem 328]) ce qui montre que, même pour une petite hauteur, l'estimation du théorème de Loher est étonnamment précise.

Nous nous contenterons de montrer l'estimation

$$\#K(H) \leq c(D \log D) H^{2D},$$

où $c > 0$ est une constante positive. Nous utiliserons ensuite ce résultat pour obtenir (à nouveau) une minoration de la hauteur logarithmique absolue d'un nombre algébrique, ni nul, ni racine de l'unité.

5.2 Lemmes préliminaires

L'idée nouvelle de la preuve de Loher consiste à utiliser un principe de localisation :

Lemme 5.2.1 *Pour tout sous-ensemble S de $\mathbb{R}^f$, vérifiant $\#(S\cap B(0,1)) = N \geq 1$, et pour tout $r > 0$, il existe $x \in \mathbb{R}^f$ tel que*

$$\#(S \cap B(x,r)) \geq \left(\frac{r}{1+r}\right)^f N \, .$$

Preuve. Soit $x \in B(0,1+r)$, et soit $N(x) = \#(S \cap B(x,r))$. Pour tout sous-ensemble A de $\mathbb{R}^f$ notons χ_A la fonction indicatrice de A. On vérifie alors que

$$\chi_{B(x_1,r)}(x_2) = \chi_{B(x_2,r)}(x_1)$$

pour x_1, $x_2 \in \mathbb{R}^f$. En notant $S' = S \cap B(0,1)$, nous avons donc :

$$\begin{aligned}
\sum_{w\in S'} \int_{B(0,1+r)} \chi_{B(w,r)}(x)dx &= \int_{B(0,1+r)} \sum_{w\in S'} \chi_{B(w,r)}(x)dx \\
&= \int_{B(0,1+r)} \sum_{w\in S'} \chi_{B(x,r)}(w)dx \\
&= \mathrm{Vol}(B(0,1+r))N(x) \\
&= \gamma_f (1+r)^f N(x)
\end{aligned}$$

où l'on a noté γ_f la mesure de la boule unitaire dans $\mathbb{R}^f$. Par ailleurs, pour $w \in S'$ on a $B(w,r) \subseteq B(0,1+r)$, donc $\int_{B(0,1+r)} \chi_{B(w,r)}(x)dx$ est égale à la mesure de Lebesgue de $B(w,r)$, c'est-à-dire à $\gamma_f r^f$. D'où :

$$\sum_{w\in S'} \int_{B(0,1+r)} \chi_{B(w,r)}(x)dx = \sum_{w\in S'} \gamma_f r^f = N\gamma_f r^f \, .$$

On en déduit que la valeur moyenne de $N(x)$ sur le disque $B(0,1+r)$ vaut $N(r/(1+r))^f$; il existe donc $x \in B(0,1+r)$ tel que

$$\#(S \cap B(x,r)) \geq \left(\frac{r}{1+r}\right)^f N \, .$$

□

Lemme 5.2.2 *Soit $z \in \mathbb{C}$, soit $r > 0$, soit $n \in \mathbb{N}^*$ et soient $\alpha_1, \dots, \alpha_n$ des complexes de la boule fermée $\overline{B}(z,r)$ de centre z et de rayon r. Alors le déterminant de Van der Monde*

$$\Delta = \mathrm{Det}\big((\alpha_i^j)_{1\le i,j\le n}\big)$$

vérifie

$$|\Delta| \le n^{n/2} r^{n(n-1)/2} .$$

Preuve. Nous pouvons supposer sans perte de généralité que $z = 0$ (en effet, la translation $\alpha_j \mapsto \alpha_j - z$ ne change pas la valeur de Δ), et $r = 1$ par homogénéité. Nous avons alors $|\alpha_i^{j-1}| \le 1$ pour tout couple (i,j). En appliquant l'inégalité de Hadamard (qui permet de majorer la valeur absolue d'un déterminant par le produit des moyens quadratiques de ses lignes), nous obtenons

$$|\Delta| \le \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\alpha_i|^{2(j-1)} \right)^{1/2} \le \prod_{i=1}^{n} n \le n^n$$

d'où le résultat.

□

5.3 Preuve du théorème de Loher

L'ensemble $K(H)$ contient 0, 1, et -1, et puisque $H(\alpha) = H(\alpha^{-1})$ pour tout $\alpha \neq 0$, les autres éléments de $K(H)$ se regroupe en couple (α, α^{-1}) avec $\alpha \neq \alpha^{-1}$. Notons N l'entier tel que $\#K(H) = 2N+1$. Il existe alors N éléments non nuls $\alpha_1, \dots, \alpha_N \in K(H)$ de module inférieur ou égal à 1. Soit maintenant $n \in [1, N-1]$ un paramètre entier qui sera choisi à la fin de la preuve et notons

$$r = \frac{1}{\left(\frac{N}{n}\right)^{1/f} - 1},$$

où $f = 1$ si $K \subset \mathbb{R}$ et $f = 2$ sinon; nous avons donc $r < 1$ et

$$\left(\frac{r}{1+r}\right)^f N = n.$$

Quitte à renuméroter les α_j, d'après le lemme de localisation 5.2.1, il existe un complexe $z \in \mathbb{C}$ tel que $\alpha_1, \dots, \alpha_n \in B(z,r)$. Par le lemme 5.2.2, le déterminant de Van der Monde

$$\Delta = \mathrm{Det}\big((\alpha_i^j)_{1\le i,j\le n}\big)$$

qui est non nul (puisque les α_i sont distincts), vérifie

$$|\Delta| \leq n^{n/2} r^{n(n-1)/2}.$$

Evaluons $|\Delta|_v$ pour toute place v du corps K. Tout d'abord, pour une place archimédienne v associée au plongement σ de K dans $\mathbb{C}$, nous avons par l'inégalité de Hadamard :

$$|\Delta|_v = |\sigma(\Delta)| \leq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma(\alpha_i)|^{2(j-1)} \right)^{1/2},$$

donc

$$\begin{aligned} |\Delta|_v &\leq \prod_{i=1}^{n} \left(n \max(1, |\sigma(\alpha_i)|)^{2(n-1)} \right)^{1/2} \\ &= n^{n/2} \prod_{i=1}^{n} \max(1, |\alpha_i|_v)^{n-1} \\ &\leq n^{n/2} \prod_{i=1}^{n} \max(1, |\alpha_i|_v)^{n} \end{aligned}.$$

Par ailleurs, pour une place ultramétrique v, puisque nous avons

$$|\alpha_i - \alpha_j|_v \leq \max(1, |\alpha_i|_v) \times \max(1, |\alpha_j|_v).$$

On obtient :

$$|\Delta|_v \leq \prod_{i=1}^{n} \max(1, |\alpha_i|_v)^n.$$

En appliquant la formule du produit au déterminant $\Delta \neq 0$, nous obtenons (compte tenue de la formule $\sum_{v \in \mathcal{M}_K, v|\infty} n_v = D$) :

$$1 = \prod_{v \in \mathcal{M}_K} |\Delta|_v^{n_v} \leq r^{fn(n-1)/2} n^{Dn/2} \prod_{i=1}^{n} H(\alpha_i)^{Dn} \leq r^{fn^2/2} n^{Dn/2} H^{Dn^2},$$

et

$$\left(\left(\frac{N}{n} \right)^{1/f} - 1 \right)^{fn^2/2} = r^{-fn^2/2} \leq n^{Dn/2} H^{Dn^2}.$$

Nous en déduisons

$$\left(\frac{N}{n} \right)^{1/f} \leq 1 + n^{D/2nf} H^{D/f} \leq (1 + n^{D/2n} H^D)^{1/f},$$

et

$$N \leq n(1+n^{D/2n}H^D)^2 \leq n(1+n^{D/n})^2H^{2D}.$$

Si $N \leq D\log D$, alors

$$\#K(H) = 2N+1 \leq \big(2(D\log D)+1\big)H^{2D} \leq 3D(\log D)H^{2D}\ .$$

Dans le cas contraire, le choix de paramètre $n = [D\log D] \leq N-1$ donne à nouveau l'estimation attendue :

$$\#K(H) \leq c(D\log D)H^{2D}\ ,$$

pour une certain constante $c > 0$.

□

Corollaire 5.3.1 *Il existe une constante $c > 0$, telle que pour tout nombre algébrique α de degré $D \geq 2$ qui n'est pas une racine de l'unité, nous avons*

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

Preuve. Soit $H \geq 1$ un paramètre réel qui sera choisi à la fin de la preuve. Posons $N = \#K(H)$. L'ensemble des $N+1$ premières puissances de α

$$\{1, \alpha, \alpha^2, \ldots, \alpha^N\}$$

est de cardinal $N+1$ (car α n'est pas une racine de l'unité) et il n'est donc pas contenu dans $K(H)$. Il existe alors un entier $n \in \{0, \ldots N\}$, tel que

$$H(\alpha^n) > H,$$

et

$$Nh(\alpha) \geq nh(\alpha) > \log H\ .$$

Par ailleurs, le théorème de Loher assure que $N \leq c(D\log D)H^{2D}$; on en déduit donc :

$$cD\log DH^{2D}h(\alpha) \geq \log H$$

et

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

Pour obtenir le résultat annoncé, il suffit maintenant de choisir $H = e^{1/D}$.

□

Bibliographie

[1] F. Amoroso et R. Dvornicich – A lower bound for the height in abelian extensions., *J. Number Theory* **80** (2000), no. 2, p. 260–272.

[2] J. W. S. Cassels et A. Fröhlich – *Algebraic number theory; Proceedings of an instructional conference organized by the London Mathematical Society.*, Academic Press. London–New-York (1967).

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

[4] Hardy et Wright – *An introduction to the theory of numbers.* Clarendon Press. Oxford (1979).

[5] L. Kronecker – Zwei sätze über gleichungen mit ganzzahligen coefficienten, *J. Reine Angew. Math.* **53** (1857), p. 173–175.

[6] D. H. Lehmer – Factorization of certain cyclotomic functions, *Ann. of Math.* **34** (1933), p. 461–479.

[7] T. Loher – Counting points of bounded height., *Ph.D. Thesis* , Basel (2002).

[8] R. Louboutin – Sur la mesure de mahler d'un nombre algébrique., *C. R. Acad. Sci. Paris Sér. I Math.* **296** (1983), no. 16, p. 707–708.

[9] J.M. Masley, H.L Montgomery – Cyclotomic fields with unique factorization, *J. Reine Angew. Math.* **286/287** (1976), p. 248–256.

[10] U. Rausch – On a theorem of Dobrowolski about the product of conjugate numbers., *Colloq. Math* **50** (1985), p. 137–142.

[11] S. Schanuel – Heights in number fields., *Bull. Soc. Math. France* **107** (1979), p. 433–449.

[12] A. Schinzel – On the product of the conjugates outside the unit circle of an algebraic number., *Acta Arith.* **24** (1973), p. 385–399.

[13] W. M. Schmidt – Northcott's theorem on heights I., *Monatsch. Math.* **115** (1993), p. 169–181.

[14] C. Smyth – On the product of the conjugates outside the unit circle of an algebraic integer., *Bull. Lond. Math. Soc.* **3** (1971), p. 169–175.

[15] P. M. Voutier – An effective lower bound for the height of algebraic numbers., *Acta Arith.* **74** (1996), no. 1, p. 81–95.

[16] M. Waldschmidt – *Diophantine approximation on linear algebraic group*. Springer. Berlin - Heidelberg - New York - Oxford (2000).