Université de Caen
Département de Mathématiques

DEA AAA — Année 2000/2001

Minoration de points de petite hauteur dans une puissance du groupe multiplicatif.

Cours de M. Francesco Amoroso.

Notes de Corentin Pontreau. Version 1.2

Table des matières

1 Hauteurs. 7

I Hauteur d'un nombre algébrique. 7

II Valuations et valeurs absolues. 13

III Généralisation de $\mathbb{Q}$ à un corps de nombres. 18

III.1 Notations et rappels 18

III.2 Valeurs absolues équivalentes. 20

IV Hauteurs et valuations. 23

2 Différents résultats. 29

I Théorème de Loher 29

I.1 Lemmes préliminaires. 31

I.2 Preuve du théorème de Loher (2.2) 33

II Cas particulier d'une extension abélienne 35

II.1 Nombres algébriques contenus dans une extension abélienne 35

II.2 Application à la structure du groupe des classes. 40

II.3 Version faible du théorème de Smyth 43

3 Théorème de Dobrowolski 45

I Lemme clef. 45

II Construction de la fonction auxiliaire. 47

III Démonstration du théorème de Dobrowolski. 50

4 Hauteurs en dimension supérieure. 55

I Hauteur et minimum essentiel. 55

I.1 Minimum essentiel. 55

I.2 Hauteur normalisée. 56

I.3 Etude en dimension 1. 57

II Premiers résultats en dimension supérieure. 58

III Théorème de Zhang. 60

III.1 Enoncé. 60

III.2 Lemme de Siegel sur les variétés. 63
III.3 Fin de la preuve. 65
IV Approches de Lehmer en dimension supérieure. 67
IV.1 Résultats dans $\mathbb{G}_m^n$. 67
IV.2 Résultats pour les hypersurfaces. 68

Notations

$\mathbb{G}_m^n$ — $\mathbb{G}_m^n(\overline{\mathbb{Q}})$, le groupe multiplicatif $(\overline{\mathbb{Q}}^*)^n$.

$H(P)$ — Hauteur de P, *c.f.* p. 10

$h_0(P)$ — *c.f.* p. 25

k — Un corps de nombres.

k_ν — Complété de k pour la topologie induite par ν.

$k[\mathrm{x}_0, \ldots, \mathrm{x}_n]_L$ — Ensemble des polynômes homogènes de degré total L.

$k[\mathrm{x}_1, \ldots, \mathrm{x}_n]_{\leq L}$ — Ensemble des polynômes de degré total $\leq L$.

$\mathcal{L}(P)$ — Longueur de P, *c.f.* p. 10

$\mathcal{M}_k$ — Ensemble des places de k.

$\mathcal{O}_k$ — Anneau des entiers du corps k.

$\overline{S}^{Zar}$ — Adhérence de Zariski de S.

CHAPITRE 1

HAUTEURS.

I HAUTEUR D'UN NOMBRE ALGÉBRIQUE.

Définition 1.1 *Soit $\alpha = p/q \in \mathbb{Q}$, $(p,q) = 1$, $q > 0$, on appelle* ***hauteur*** *de α le nombre :*

$$h(\alpha) := \log \max(|p|, q). \quad (h(0) = 0).$$

Propriétés 1.1 *1.* $h : \mathbb{Q} \longrightarrow \mathbb{R}_+$

2. $\forall h_0 > 0,\ \sharp\{\alpha \in \mathbb{Q}\ ;\ h(\alpha) \leq h_0\} < \infty$

3. $\forall r, s \in \mathbb{Q}^*,\ h(\frac{r}{s}) \leq h(r) + h(s)$

DÉMONSTRATION - *3.* Soient $r = p_1/q_1$, $s = p_2/q_2$, on a :

$$\max(|p_1 \cdot p_2|, q_1 \cdot q_2) \leq \max(|p_1|, q_1) \max(|p_2|, q_2)$$

■

Remarques : • $h(r.r^{-1}) = h(1) = 0$
• $h(r^{-1}) = h(r)$.

Propriétés 1.2 *1.* $\forall r \in \mathbb{Q}^*, \forall n \in \mathbb{Z}, h(r^n) = |n| \cdot h(r)$.

2. $\forall r \in \mathbb{Q}, h(r) = 0 \Leftrightarrow r \in \{-1, 0, 1\}$.

But : Etendre cette définition à $\overline{\mathbb{Q}}$.

Définition 1.2 *Soit $\mathbb{K}$ un corps commutatif. On appelle* ***valeur absolue*** *sur $\mathbb{K}$ toute application $|.|$ de $\mathbb{K}$ dans $\mathbb{R}_+$ vérifiant :*

VA.1 $\forall x \in \mathbb{K}, |x| = 0 \Leftrightarrow x = 0$

VA.2 $\forall x, y \in \mathbb{K}, |x \cdot y| = |x| \cdot |y|$

VA.3 $\forall x, y \in \mathbb{K}, |x+y| \leq |x| + |y|$

VA.3' $\forall x, y \in \mathbb{K}, |x+y| \leq \max\{|x|, |y|\}$ *Dans ce cas, on parle de valeur absolue ultramétrique (ou non archimédienne).*

Remarque : Dans le cas ultramétrique on a même, si $|x| \neq |y|$: $|x+y| = \max\{|x|, |y|\}$. En effet, supposons $|x| < |y|$, on a : $|x+y| \leq \max\{|x|, |y|\} = |y|$ et $|y| \leq \max\{|-x|, |x+y|\} \leq |y|$, d'où $|x+y| = |y|$.

Cas $\mathbb{K} = \mathbb{Q}$: • $|.|$ valeur absolue usuelle : $|.| = |.|_\infty$.
• Soient p premier et $\alpha \in \mathbb{Q}$, $\alpha = p^k \beta$ où $\beta = a/b, p \not| a, p \not| b$, $k \in \mathbb{Z}$.
on pose $|\alpha|_p = p^{-k}$ $\quad (|p|_p = \frac{1}{p})$.
(Valeur absolue ultramétrique.)

Exercice : Si $\alpha \in \mathbb{Q}^*$, $h(\alpha) = \sum_{|.| \cup |.|_\infty} \log\big(\max(|\alpha|, 1)\big)$.

Définition 1.3 *Soit $\alpha \in \overline{\mathbb{Q}}$, on appelle* ***polynôme minimal*** *de α sur $\mathbb{Z}$ le seul polynôme irréductible $F \in \mathbb{Z}$[x] tel que $F(\alpha) = 0$ et $lc(F) > 0$.*

Définition 1.4 *Soit $F \in \mathbb{C}[z]$, $F(z) = a \cdot (z - \alpha_1) \ldots (z - \alpha_d)$.*
On appelle ***mesure de Mahler*** *de F et on note $M(F)$ le nombre :*

$$\begin{aligned} M(0) &:= 0 \\ M(F) &:= |a| \prod_{j=1}^{d} \max(1, |\alpha_j|) \text{ si } F \neq 0. \end{aligned}$$

Remarque : $M(px - q) = q \cdot \max(1, |p/q|) = \max(|p|, q)$ donc $h(p/q) = \log M(qx - p)$.
(*i. e.* si $\alpha \in \mathbb{Q}$, et si F est son polynôme minimal sur $\mathbb{Z}$, alors $h(\alpha) = \log(M(F))$.)

Définition 1.5 *Soient $\alpha \in \overline{\mathbb{Q}}$, F son polynôme minimal sur $\mathbb{Z}$. On appelle* ***hauteur de Weil*** *de α le nombre :*

$$h(\alpha) := \frac{1}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \log M(F).$$

Théorème 1.1 *Soit $F \in \mathbb{C}$[x], $F \neq 0$, on a :*

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

DÉMONSTRATION - Ce résultat est une conséquence directe de la formule de Jensen, néanmoins nous donnons ici la démonstration originale de Mahler.
Notons $\tilde{M}$ l'application :

$$\begin{array}{rccl} \tilde{M}: & \mathbb{C}[\mathrm{x}] & \to & \mathbb{R} \\ & P & \mapsto & \exp\left\{\dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \log|F(e^{it})|dt\right\} \end{array}$$

Le but ici est donc de montrer que pour tout polynôme $F \in \mathbb{C}[\mathrm{x}]$ on a $M(F) = \tilde{M}(F)$.

• Remarquons tout d'abord que les deux applications vérifient

$$\tilde{M}(PQ) = \tilde{M}(P)\tilde{M}(Q) \text{ et } \tilde{M}(\alpha) = |\alpha|$$
$$M(PQ) = M(P)M(Q) \text{ et } M(\alpha) = |\alpha| \quad \forall (P,Q,\alpha) \in \mathbb{C}[\mathrm{x}] \times \mathbb{C}[\mathrm{x}] \times \mathbb{C}$$

On est ainsi ramené à démontrer le théorème pour les polynômes de la forme $x - \alpha$, c'est-à-dire :

$$\forall \alpha \in \mathbb{C}, \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - \alpha|dt = \log\big(\max\{1, |\alpha|\}\big)$$

• En posant $\alpha = re^{i\theta}$ on obtient :

$$\begin{aligned} \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - re^{i\theta}|dt &= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it-\theta} - r|dt \\ &= \frac{1}{2\pi}\int_{-\theta}^{2\pi-\theta} \log|e^{iu} - r|du \\ &= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{iu} - r|du \end{aligned}$$

On peut donc supposer $\alpha \in \mathbb{R}_+$; il suffit donc de montrer :

$$\forall \alpha \in \mathbb{R}_+, \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - r|dt = \log\big(\max\{1, r\}\big). \tag{1.1}$$

• On pose, pour $r \in \mathbb{R}$, $I(r) = \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - r|dt$
FAIT : $I(r^2) = 2I(r)$.

$$\begin{aligned} I(r^2) &= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - r^2|dt \\ &= \frac{1}{4\pi}\int_0^{4\pi} \log|e^{it} - r^2|dt \quad \text{on pose } t = 2s \\ &= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{2is} - r^2|ds \\ &= \frac{1}{2\pi}\int_0^{2\pi} \log|e^{is} - r|ds + \frac{1}{2\pi}\int_0^{2\pi} \log|e^{is} + r|ds \\ &= 2I(r) \quad \text{en posant } u = s - \pi \text{ dans le second membre.} \end{aligned}$$

Montrons à présent (1.1) :

1) Si $r = 1$ d'après ce qui précède $I(1) = 2I(1)$ donc $I(1) = 0 = \log\big(\max\{1,1\}\big)$.

2) Si $r \neq 1$, soient $n \in \mathbb{N}$ et $m = 2^n$, on a

$$I(r^m) = mI(r)$$

On obtient alors :

$$\begin{aligned} |r^m - 1| \leq |e^{it} - r^m| &\leq r^m + 1 \\ \frac{1}{m}\log|r^m - 1| \leq \quad I(r) \quad &\leq \frac{1}{m}\log(r^m + 1) \end{aligned}$$

$I(r)$ est encadrée par deux suites tendant vers 0 si $r < 1$ et $\log r$ si $r > 1$, donc $I(r) = \log\big(\max\{1, r\}\big)$. ■

Théorème 1.2 (de finitude de Northcott) *Soient $d \in \mathbb{N}^*$, $h_0 \in \mathbb{R}_+$.*
Alors $\big\{\, \alpha \in \overline{\mathbb{Q}} \,|\, [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d \text{ et } h(\alpha) \leq h_0 \,\big\}$ est fini.

Remarque : La hauteur d'un nombre algébrique est toujours positive, en effet, si $F \in \mathbb{Z}[\mathrm{x}]$ on a $M(F) \geq |lc(F)| \geq 1$.

On peut alors se demander quels sont ceux de hauteur nulle ; la réponse est donnée par un théorème de Kronecker, que nous verrons plus tard. Avant de démontrer le théorème 1.2, nous allons donner quelques définitions.

Définition 1.6 *Soient $d \in \mathbb{N}$ et $F \in \mathbb{C}[z]_{\leq d}$, $F = a_0 z^d + \ldots + a_d$. On appelle respectivement* ***hauteur*** *H et* ***longueur*** *$\mathcal{L}$ de F les nombres :*

$$\begin{aligned} H(F) &:= \max_{i=0\ldots d} |a_j| \\ \mathcal{L}(F) &:= \sum_{i=0\ldots d} |a_j| \end{aligned}$$

Propriétés 1.3 *Si on note $\|.\|_2$ la norme quadratique sur $\mathbb{C}[z]_{\leq d}$ (associée au produit scalaire $< F, g >= \frac{1}{2\pi}\int_0^{2\pi} F(e^{it})\overline{G(e^{it})}dt$), on rappelle que l'on a, la base $(1, \ldots, z^d)$ étant orthonormée :*

$$\|F\|_2^2 = \sum_{j=0}^{d} |a_j|^2.$$

De plus, si l'on note $|F| := \max_{|z|=1} |F(z)|$, on a les égalités suivantes :

$$H(F) \leq \|F\|_2 \leq |F| \leq \mathcal{L}(F) \leq (d+1) \cdot H(F).$$

Remarque : La mesure de Mahler n'est pas une norme sur $\mathbb{C}[z]$: $M(F+G) \not\leq M(F) + M(G)$. En revanche on peut montrer que l'on a : $M(F+G) \leq M(F) + M(G) + \log 2$.

Lemme 1.1 *Soit $F \in \mathbb{C}[z]$, on a : $M(F) \leq |F|$ (conséquence du théorème 1.1). De plus $M(F) \leq \|F\|_2$.*

Lemme 1.2 *Soit $F \in \mathbb{C}[z]$ de degré n, on a :*

$$\mathcal{L}(F) \leq 2^n M(F).$$

Remarque : Cette majoration est optimale, en effet, si $F = (z-1)^n$ on a :

$$\begin{aligned} M(F) &= 1 \\ \mathcal{L}(F) &= \sum_{h=0}^{n} \binom{n}{h} = 2^n = 2^n \cdot M(F). \end{aligned}$$

DÉMONSTRATION - On écrit $F(z) = a_0 + \ldots + a_n z^n = a_n \prod_{j=1}^{n} (z - \alpha_j)$, on a :

$$\begin{aligned} a_{n-1} &= -a_n \cdot \sum_{j=0}^{n} \alpha_j \\ a_{n-2} &= a_n \cdot \sum_{j<k} \alpha_j \alpha_k \\ \vdots \quad &= \\ a_0 \quad &= (-1)^n a_n \prod_{j=0}^{n} \alpha_j \end{aligned}$$

$$\begin{aligned} |a_{n-k}| &\leq |a_n| \binom{n}{k} \prod_{j=1}^{n} \max(1, |\alpha_j|) \\ &\leq \binom{n}{k} M(F) \quad k = 0, 1, \ldots, n. \end{aligned}$$

d'où $\mathcal{L}(F) = \sum_{k=0} |a_{n-k}| \leq 2^n \cdot (F)$. ■

Nous pouvons maintenant démontrer le théorème 1.2 :

DÉMONSTRATION - Soit $\alpha \in \overline{\mathbb{Q}}^*$, $h(\alpha) \leq h_0$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d$. Soit F_α le polynôme minimal de α sur $\mathbb{Z}$, on a :

$$h(\alpha) = \frac{M(F_\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \leq h_0,$$

soit $M(F_\alpha) \leq e^{d \cdot h_0}$. Ainsi, d'après la proposition précédente :

$$L(F_\alpha) \leq 2^n e^{d \cdot h_0}.$$

Comme $L(F_\alpha)$ est majorée par une fonction de d et h_0, F_α étant à coefficients entiers, il n'existe qu'un nombre fini de polynômes possibles, donc qu'un nombre fini de α. ■

Notation : On note $\overline{\mathbb{Q}}^*_{tors}$ le module de torsion du $\mathbb{Z}$-module $\overline{\mathbb{Q}}^*$, *i. e.* l'ensemble des racines de l'unité.

Corollaire 1.1 (Kronecker) *Soit $\alpha \in \overline{\mathbb{Q}}^*$, on a l'équivalence suivante :*

$$h(\alpha) = 0 \Longleftrightarrow \alpha \in \overline{\mathbb{Q}}^*_{tors}.$$

Démonstration -

$\Leftarrow$. Si α est une racine de l'unité alors F_α est un polynôme cyclotomique. En particulier il est de la forme $F_\alpha(\mathrm{x}) = \prod(\mathrm{x} - \alpha_j)$ où α_j est une racine de l'unité, donc de module 1. ainsi $M(F) = 1$ et $h(\alpha) = 0$.

$\Rightarrow$. Supposons $h(\alpha) = 0$ ($\alpha \neq 0$). Comme $M(F_\alpha) = 1$, tous les conjugués de α sont de module plus petit que 1, il en est de même pour ceux de α^n, pour tout $n \in \mathbb{N}$, ainsi $h(\alpha^n) = 0$.

Fixons $h_0 > 0$ quelconque, posons $d := [\mathbb{Q}(\alpha) : \mathbb{Q}]$, on obtient alors l'inclusion suivante :

$$\{\alpha^n \mid n \in \mathbb{N}^*\} \subseteq \{\beta \in \overline{\mathbb{Q}}^* \mid h(\beta) \leq h_0, [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq q\}.$$

Donc, d'après le théorème 1.2 de finitude de Northcott, l'ensemble $\{\alpha^n \mid n \in \mathbb{N}^*\}$ est fini, c'est-à-dire qu'il existe deux entiers distinct n et m tels que $\alpha^n = \alpha^m$. ■

Conséquence : Si $\alpha \in \overline{\mathbb{Q}}^*$ n'est pas une racine de l'unité, alors $h(\alpha) > 0$.

Exemple : $\alpha := 2^{1/d} > 1$.
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, $F_\alpha(\mathrm{x}) = \mathrm{x}^d - 2$, $M(F) = 2$ et $h(\alpha) = \frac{\log 2}{d}$.

L'exemple précédent montre que la hauteur d'un nombre algébrique peut tendre vers 0 quand son degré tend vers l'infini. Mais le problème a été étudié plus en détail par Lehmer, voir [Leh], il pose la question :

Conjecture 1.1 *Il existe un nombre réel une constante $c > 0$ telle que, pour tout $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{tors}$, on ait :*

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

Ceci reste aujourd'hui un problème ouvert, l'exemple précédent nous dit que si une telle constante c existe, alors $c \leq \log 2$.

Remarque : Il suffit en fait d'étudier le cas des entiers algébriques. En effet si $\alpha \in \overline{\mathbb{Q}}$ n'est pas un entier, alors son polynôme minimal sur $\mathbb{Z}$ a un coefficient dominant ≥ 2, en conséquence : $h(\alpha) \geq \log 2/[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Il est remarquable qu'après bien des années et calculs, le polynôme de plus petite mesure de Mahler connu reste celui donné par Lehmer lui-même :

$$F(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1, \quad M(F) \cong 1,176\ldots.$$

II Valuations et valeurs absolues.

Dans la suite, k désigne un corps commutatif.

Définition 1.7 *On appelle **valuation** sur k une application $v : k \longrightarrow \mathbb{R} \cup \{\infty\}$ vérifiant :*

(V1) $\forall x \in k,\ v(x) = \infty \Leftrightarrow x = 0.$

(V2) $\forall x, y \in k,\ v(xy) = v(x) + v(y).$

(V3) $\forall x, y \in k,\ v(x + y) \geq \min\{v(x), v(y)\}.$

Exemple important : Valuation sur $\mathbb{Q}$ ($k = \mathbb{Q}$) :
Soient p premier, et $x = y \cdot p^\alpha \in \mathbb{Q}$, avec $y = a/b,\ (a, p) = (b, p) = 1$, on note $v_p(x) := \alpha \in \mathbb{Z}$.

Exemple : $v_3(\frac{5}{18}) = -2\ :\ \frac{5}{18} = 3^{-2}\frac{5}{2}$.

Remarque : $v : (k^*, .) \longrightarrow (\mathbb{R}, +)$ est un morphisme de groupes.

Exercice : Soit $|.|$ une valeur absolue sur k.

1. $|1| = 1$.
2. $\forall (w, n) \in k \times \mathbb{N}^*,\ w^n \Rightarrow |w| = 1$.

3. Si $|.|$ est non archimédienne, on a $\forall x, y \in k,\ |x| \neq |y| \Rightarrow \max\{|x|, |y|\} = |x+y|$.

Remarque : Si k est le corps des fractions d'un anneau A et si $|.|$ est une application de $A - \{0\}$ dans $\mathbb{R}_+^*$ qui satisfait (VA2) et (VA3), alors elle définit de façon unique une valeur absolue sur k.

Remarques :

• Si v est une valuation sur k et $a \in]0,1[$, on peut lui associer une valeur absolue $|.|$ sur k :

$$|x| = \begin{cases} 0 & \text{si } x = 0 \\ a^{v(x)} & \text{si } x \neq 0 \end{cases} \quad \text{est une valeur absolue ultramétrique.}$$

• Si $|.|$ est une valeur absolue ultramétrique sur k et $b \in \mathbb{R}_+^*$, on peut lui associer une valuation v sur k :

$$v(x) = \begin{cases} +\infty & \text{si } x = 0 \\ -b \log |x| & \text{si } x \neq 0 \end{cases}$$

Proposition 1.1 *Soit (k, v) un corps valué.*

1. *$A := \{x \in k \mid v(x) \geq 0\}$ est un sous-anneau de k.*
2. *Pour tout $x \in k^*$, on a $x \in A$ ou $x^{-1} \in A$.*
3. *k est le corps de fraction de A.*
4. *$\mathfrak{m} := \{x \in k \mid v(x) > 0\}$ est le seul idéal maximal de A.*

DÉMONSTRATION - Exercice. ■

Définition 1.8 *Le corps $A/\mathfrak{m}$ est appelé **corps résiduel** de (K, v).*

Remarque : Si $|.|$ est une valeur absolue associée à v (*i.e* s'il existe $a \in]0,1[$ tel que : pour tout $x \in k$, $|x| = a^{v(x)}$), alors : $A = \{x \in k \mid |x| \leq 1\}$ et $\mathfrak{m} = \{x \in k \mid |x| < 1\}$ (cela est indépendant de a.)

Définition 1.9 *Deux valeurs absolues $|.|_1$ et $|.|_2$ sont dites **équivalentes** si elles définissent la même topologie, on note alors $|.|_1 \sim |.|_2$.*

Proposition 1.2 *Soient $|.|_1$ et $|.|_2$ deux valeurs absolues sur k, les 3 assertions suivantes sont équivalentes :*

1. $|.|_1 \sim |.|_2$.
2. $\{x \in k \mid |x|_1 < 1\} = \{x \in k \mid |x|_1 < 1\}$.
3. $\exists b > 0 \mid \forall x \in k,\ |x|_1 = |x|_2^b$.

Démonstration -

3. $\Rightarrow$ 2. $\Rightarrow$ 1. Facile.

1. $\Rightarrow$ 2. $M_j = \{x \in k \mid |x|_j < 1\}$ $(j = 1, 2)$. On a : $x \in M_j \Leftrightarrow x^n \underset{|.|_j}{\longrightarrow} 0$.

2. $\Rightarrow$ 3. Supposons $M_1 = M_2 =: M$, on a $M = \{0\}$ si et seulement si les $|.|_j$ sont triviales, dans ce cas on obtient 3. en prenant $b = 1$; on peut donc supposer $|.|_1$ et $|.|_2$ non triviales.
Soit $y \in M - \{0\}$, on pose $b := \frac{\log |y|_1}{\log |y|_2}$; on a $b > 0$ car $|y|_1 < 1$ et $|y|_2 < 1$.
On veut montrer que b ne dépend pas de y c'est-à-dire :

$$\forall x \in k^*,\ \frac{\log |x|_1}{\log |y|_1} = \frac{\log |x|_2}{\log |y|_2}.$$

Soit $x \in k^*$. Si $|x|_1 = 1$, alors $|x|_2 = 1$; en effet, si $|x|_2 < 1$ (resp. $|1/x|_2 < 1$) alors $|x|_1 < 1$ (resp. $|1/x|_1 < 1$), car $M_1 = M_2$.
On peut maintenant supposer $x \in M$, *i.e* $|x|_j < 1$ $(j = 1, 2)$, quitte à considérer $1/x$.
Supposons par exemple $\frac{\log |x|_1}{\log |y|_1} < \frac{\log |x|_2}{\log |y|_2}$.
Soient $m, n \in \mathbb{N}^*$ tels que

$$0 < \frac{\log |x|_1}{\log |y|_1} < \frac{m}{n} < \frac{\log |x|_2}{\log |y|_2},$$

en paticulier :

$$n \log |x|_2 < m \log |y|_2 \text{ et } n \log |x|_1 > m \log |y|_1,$$

or, pour $j = 1, 2$ nous avons :

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

d'où une contradiction. ■

Corollaire 1.2 *Si $|.|_1$ et $|.|_2$ sont associées à la même valuation v (i. e. $|.|_1 = a_1^{v(x)}$ et $|.|_2 = a_2^{v(x)}$), alors elles sont équivalentes.*

Définition 1.10 *Soient v_1 et v_2 deux valuations, $|.|_1 = a_1^{v_1(x)}$, $|.|_2 = a_2^{v_2(x)}$, $a_i \in]0,1[$. On dit que v_1 et v_2 sont* ***équivalentes*** *si $|.|_1 =$ et $|.|_2$ le sont, dans ce cas on note de même : $v_1 \sim v_2$.*

Corollaire 1.3 *Soient v_1 et v_2 deux valuations sur k.*
Alors

$$\begin{aligned} v_1 \sim v_2 &\Longleftrightarrow \{x \in k \mid v_1(x) > 0\} = \{x \in k \mid v_2(x) > 0\} \\ &\Longleftrightarrow \exists b > 0 \ ; \ v_1 = b \cdot v_2 \end{aligned}$$

Notation : Soit $x \in \mathbb{Q}$, on note $|x|_p := p^{-\alpha} = p^{-v_p(x)}$, on l'appelle valeur absolue normalisée ($a = \frac{1}{p}$), et $|x|_\infty := |x|$.

En fait, en dehors de la valeur absolue triviale, il n'existe que 2 types de valeurs absolues sur $\mathbb{Q}$, résultat montré par Ostrowsky :

Théorème 1.3 (Ostrowsky) *Soit $|.|$ une valeur absolue non triviale sur $\mathbb{Q}$, alors :*

1. *S'il existe $n \in \mathbb{N}^*$ tel que $|n| < 1$, alors il existe $(p, a) \in \mathcal{P} \times]0,1[$ tel que $|.| = a^{v_p(.)}$.*
2. *Sinon il existe $\alpha \in]0,1]$ tel que $|.| = |.|_\infty^\alpha$.*

DÉMONSTRATION -

1. Soit $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers, on a :

$$\forall i \in \{1, \ldots, r\}, \ |p_i| \geq 1 \Rightarrow |n| \geq 1,$$

donc il existe un nombre premier p tel que $|p| < 1$.

• Montrons que pour tout entier m, $|m| \leq 1$.
Soient $m \in \mathbb{Z}$ et $k \in \mathbb{N}^*$, on a :

$$m^k = c_{k,0} + c_{k,1}p + \ldots + c_{k,h_k}p^{h_k} \quad \text{où} \ \ c_{k,j} \in \{0, \ldots, p-1\}, \ c_{k,h_k} \neq 0.$$

En particulier

$$h_k \leq \frac{\log(m^k)}{\log p} = \frac{k \log m}{\log p} \quad (p^{h_k} \leq m^k).$$

Par ailleurs, si on pose $M := \max\{|1|, |2|, \ldots, |p-1|\}$, alors :

$$\begin{aligned} |m|^k &= |m^k| \leq (1 + h_k) \cdot M \quad \text{car } |p| < 1 \text{ d'où :} \\ |m| &\leq \left(1 + \tfrac{k \log m}{\log p}\right)^{1/k} \cdot M^{1/k} \xrightarrow[k \to +\infty]{} 1 \end{aligned}$$

• Montrons maintenant que pour tout nombre premier q distinct de p, on a $|q| = 1$. Soient q premier $q \neq p$ et $k \in \mathbb{N}^*$, supposons $|q| < 1$. D'après Bézout, il existe des entiers λ_k et μ_k tels que $\lambda_k p^k + \mu_k q^k =$, d'où :

$$\begin{aligned} |1| &\leq |\lambda_k||p|^k + |\mu_k||q|^k \\ &\leq |p|^k + |q|^k \xrightarrow[k\to+\infty]{} 0 \quad \text{absurde.} \end{aligned}$$

• Pour finir, posons $a := |p| < 1$. Soit $x \in \mathbb{N}^*$ et écrivons $x = p^{v_p(x)} \cdot x'$, où $(x', p) = 1$. D'après ce qui précède, $|x'| = 1$, donc $|x| = a^{v_p(x)}$.

2. Par hypothèse on a : $\forall n \in \mathbb{N}^*, |n| \leq 1$. Soit $n \in \mathbb{N}^*$ tel que $|n| > 1$ (il existe car $|.|$ est supposé non trivial).

• Montrons l'assertion suivante :

$$\forall x \in \mathbb{N}^*, \frac{\log|x|}{\log x} \leq \frac{\log|n|}{\log n}.$$

Soient $x, k \in \mathbb{N}^*$, on a :

$$r^k = c_{k,0} + c_{k,1}n + \ldots + c_{k,h_k}n^{h_k} \quad \text{où} \;\; c_{k,j} \in \{0, \ldots, n-1\},\; c_{k,h_k} \neq 0.$$

En particulier

$$h_k \leq \frac{\log(x^k)}{\log n} = \frac{k \log x}{\log n}.$$

Par ailleurs, si on pose $M := \max\{|1|, |2|, \ldots, |n-1|\}$, alors :

$$\begin{aligned} |x|^k &= |x^k| \leq (1 + h_k) \cdot M(|1| + |n| + \ldots + |n|^{h_k}) = M\frac{|n|^{h_k} - 1}{|n| - 1} \\ |x| &\leq \left(\frac{|n|^{k(\log x)/(\log n)+1} - 1}{|n| - 1}\right)^{1/k} \cdot M^{1/k} \xrightarrow[k\to+\infty]{} |n|^{(\log x)/\log n}. \end{aligned}$$

Il suffit alors de remarquer que $\frac{\log|n|}{\log n} \in]0, 1]$ car $|n| \leq |1| + \ldots + |1| \leq n$.

• Posons $\alpha := \frac{\log|n|}{\log n}$, il faut maintenant vérifier que

$$\forall x \in \mathbb{N}^*,\; |x| = x^\alpha.$$

Soit $x \in \mathbb{N}^*$, si $|x| \geq 1$ on obtient, en appliquant 2 fois le point précédent (en intervertissant le rôle de x et n la seconde fois) :

$$\frac{\log|x|}{\log x} = \frac{\log|n|}{\log n} = \alpha,$$

d'où $|x| = x^\alpha$.

Si $|x| = 1$, on a $|nx| = |n| > 1$ donc $|nx| = |nx|_\infty^\alpha = |n|_\infty^\alpha |x|_\infty^\alpha$. De plus, comme $\alpha = \frac{\log|n|}{\log n}$, on a $|n| = |n|_\infty^\alpha$ donc $|x| = |x|^\alpha$. ■

Proposition 1.3 (Formule du produit) *Soit $x \in \mathbb{Q}^*$, on a :*

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

DÉMONSTRATION - On peut supposer $x \in \mathbb{N}^*$; soit $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en nombres premiers, on a :

$$|x|_\infty = p_1^{\alpha_1} \dots p_r^{\alpha_r} = |x|_{p_1}^{-\alpha_1} \dots |x|_{p_r}^{-\alpha_r}.$$

■

III Généralisation de $\mathbb{Q}$ à un corps de nombres.

III.1 Notations et rappels

Pour plus de détail, on pourra consulter ici [Ma].

Soient k un corps de nombres et $\mathcal{O}_k$ son anneau des entiers, on a :
$[k : \mathbb{Q}] = \#\{\sigma : k \hookrightarrow \overline{\mathbb{Q}}\} = r + 2s$ où $r = \#\{\sigma : k \hookrightarrow \mathbb{R} \cap \overline{\mathbb{Q}}\}$.

$$\begin{aligned} \sigma_1, \dots, \sigma_r &: k \hookrightarrow \mathbb{R} \cap \overline{\mathbb{Q}} \\ \sigma_{r+1}, \dots, \sigma_{r+s} &: k \hookrightarrow \overline{\mathbb{Q}} \\ \underbrace{\sigma_{r+s+1}}_{\overline{\sigma_{r+1}}}, \dots, \underbrace{\sigma_{2s}}_{\overline{\sigma_{r+s}}} &: k \hookrightarrow \overline{\mathbb{Q}} \end{aligned}$$

Décomposition des idéaux.

Proposition 1.4 *Soient I, J des idéaux de $\mathcal{O}_k$, alors $I|J$ si et seulement si $J \subseteq I$.*

Théorème 1.4 *Tout idéal I de $\mathcal{O}_k$ possède une unique décomposition en produits d'idéaux premiers $\mathcal{P}_1^{\lambda_1} \dots \mathcal{P}_l^{\lambda_l}$ ($\lambda_j \in \mathbb{N}$).*

Définition 1.11

- *Soit I un idéal de $\mathcal{O}_k$, on appelle* ***norme*** *de I le nombre $\|I\| = [\mathcal{O}_k : I]$.*
- *Soient $\mathbb{Q} \subseteq k \subseteq F$ des corps de nombres, $\mathcal{Q}$ un idéal premier de $\mathcal{O}_F$ et $\mathcal{P} := \mathcal{Q} \cap \mathcal{O}_k$.*

On appelle indice de ramification *de $\mathcal{Q}$ sur $\mathcal{P}$ et on note $e(\mathcal{Q}|\mathcal{P})$ la puissance de $\mathcal{Q}$ intervenant dans la décomposition de $\mathcal{P}$.*

Propriétés 1.4 *Soient $\mathbb{Q} \subseteq k \subseteq F$ des corps de nombres, $\mathcal{Q}$ un idéal premier de $\mathcal{O}_F$, $\mathcal{P} := \mathcal{Q} \cap \mathcal{O}_k$ et $P := \mathcal{Q} \cap \mathbb{Z}$, on a :*

$$e(\mathcal{Q}|P) = e(\mathcal{Q}|\mathcal{P}) \cdot e(\mathcal{P}|P)$$

Définition 1.12 *Avec les mêmes notations, on appelle* ***degré d'inertie*** *de $\mathcal{Q}$ sur $\mathcal{P}$ et on note $f(\mathcal{Q}|\mathcal{P})$ la dimension $[\mathcal{O}_F/\mathcal{Q} : \mathcal{O}_k/\mathcal{P}]$.*

Définition 1.13 *Soient $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k)$, et $d := [F : k]$, on dit que :*

- *$\mathcal{P}$ est* ***inerte*** *dans $\mathcal{O}_F$ si $\mathcal{P}\mathcal{O}_F$ est premier.*
- *$\mathcal{P}$* ***décomposé*** *sinon.*
- *$\mathcal{P}$ est* ***totalement décomposé*** *dans $\mathcal{O}_F$ si $\mathcal{P}\mathcal{O}_F = \mathcal{Q}_1 \dots \mathcal{Q}_d$.*
- *$\mathcal{P}$ est* ***ramifié*** *dans $\mathcal{O}_F$ s'il existe $\mathcal{Q} \in \mathrm{Spec}(\mathcal{O}_F)$, $\mathcal{Q}|\mathcal{P}$ tel que $e(\mathcal{Q}|\mathcal{P}) > 1$.*
- *$\mathcal{P}$ est* ***totalement ramifié*** *dans $\mathcal{O}_F$ $\mathcal{P}\mathcal{O}_F = \mathcal{Q}^d$.*

Propriétés 1.5 *Avec les mêmes notations, on a :*

$$f(\mathcal{Q}|P) = f(\mathcal{Q}|\mathcal{P}) \cdot f(\mathcal{P}|P)$$

Théorème 1.5 *Soient $\mathbb{Q} \subseteq k \subseteq F$ des corps de nombres, $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k)$.*
Soit $\mathcal{Q}_1^{e_1} \dots \mathcal{Q}_r^{e_r}$ $(e_j > 0)$ la décomposition en idéaux premiers de l'idéal $\mathcal{P}\mathcal{O}_F$, on a :

$$\sum_{j=1}^{r} e(\mathcal{Q}_j|\mathcal{P}) \cdot f(\mathcal{Q}_j|\mathcal{P}) = [F : k]$$

- *Valeurs absolues archimédiennes.*

Soit k un corps de nombres. Les plongements σ_j, $j = 1, \dots, r+s$ définissent des valeurs absolues archimédiennes sur $\mathbb{Q}$:

$$\forall x \in k, \quad |x|_{\sigma_j} = |\sigma(x)|_\infty \qquad (\text{on a } |\overline{\sigma}(x)| = |\sigma(x)|)$$

- *Valeurs absolues ultramétriques.*

Définition 1.14 *Soit k un corps de nombres, soient I un idéal fractionnaire et $\mathcal{P}$ un idéal premier non nul. On note $P := \mathcal{P} \cap \mathbb{Z}$ et λ la puissance de $\mathcal{P}$ intervenant dans la décomposition en idéaux premiers de I ($\lambda \in \mathbb{Z}$).*

On définit la ***valuation $\mathcal{P}$-adique*** *de I :*

$$v_{\mathcal{P}}(I) := \frac{\lambda}{e(\mathcal{P}|P)}.$$

Définition 1.15 *Soit $x \in k$, avec les mêmes notations, on définit la* ***valeur absolue $\mathcal{P}$-adique*** *(normalisée) :*

$$|x|_{\mathcal{P}} := p^{v_{\mathcal{P}}(\ (x)\ )},$$

où $p \in \mathbb{Z}$ est le générateur positif de $\mathcal{P} \cap \mathbb{Z}$.

III.2 Valeurs absolues équivalentes.

Notations : $\mathcal{M}_{k,\infty} = \{\sigma_1, \ldots, \sigma_{r+s}\}$
$\mathcal{M}_k := \mathcal{M}_{k,\infty} \cup \{\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k) - \{(0)\}\}$

Nous l'avons vu, à chaque élément de $\mathcal{M}_k$ on peut associer une valeur absolue. Nous allons voir qu'en fait celles-ci sont 2 à 2 non équivalentes et qu'elles sont les seules sur k ; on parle de "place", c'est à dire de classe d'équivalence de valeur absolue.

Théorème 1.6 *1. Les valeurs absolues définies par les plongements σ, $\sigma \in \mathcal{M}_{k,\infty}$ sont deux à deux non équivalentes.*

2. Si $|.|$ est une valeur absolue sur k archimédienne, alors :

$$\exists\, \sigma \in \mathcal{M}_{k,\infty}\ ;\ |.| \sim |.|_{\sigma}.$$

Théorème 1.7 *1. Soient $\mathcal{P}, \mathcal{Q} \in \mathrm{Spec}(\mathcal{O}_k)$ non nuls et distincts, alors $|.|_{\mathcal{P}} \neq |.|_{\mathcal{Q}}$.*

2. Si $|.|$ est une valeur absolue ultramétrique sur k alors :

$$\exists \mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k)\ ;\ |.| \sim |.|_{\mathcal{P}}.$$

Notations : Soit $v \in \mathcal{M}_k$, on note :

$$n_v (= [k_v : \mathbb{Q}_v]) := \begin{cases} 1 & \text{si } v \in \mathcal{M}_{k,\infty}\ (v|\infty) \text{ et si } v = \sigma,\ \sigma(k) \subseteq \mathbb{R}\ (K_v = \mathbb{R}) \\ 2 & \text{si } v \in \mathcal{M}_{k,\infty}\ (v|\infty) \text{ et si } v = \sigma,\ \sigma(k) \nsubseteq \mathbb{R}\ (K_v = \mathbb{C}) \\ e(\mathcal{P}|P) \cdot f(\mathcal{P}|P) & \text{si } v \sim \mathcal{P} \text{ et } P := \mathcal{P} \cap \mathbb{Z} \end{cases}$$

Théorème 1.8 (formule du produit) *Soit $\alpha \in k^*$, on a :*

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

DÉMONSTRATION - Soit $\alpha \in k^*$, on a :

$$(\alpha) = \mathcal{P}_1^{a_1} \dots \mathcal{P}_l^{a_l} \quad a_j \in \mathbb{Z},\ \mathcal{P}_j \in \mathrm{Spec}(\mathcal{O}_k) - \{(0)\}.$$

Pour tout j on note $(p_j) := \mathcal{P}_j \cap \mathbb{Z}$.

$$\begin{aligned} \prod_{\substack{v \in \mathcal{M}_k \\ v|\infty}} |\alpha|_v^{n_v} &= \prod_{\sigma\,:\,k \hookrightarrow \mathbb{C}} |\sigma(\alpha)| = |N_{\mathbb{Q}}^k(\alpha)| \\ &= \prod_{j=1}^{l} \|\mathcal{P}_j\|^{a_j} \quad \text{(voir [Ma] p.66)} \\ &= \prod_{j=1}^{l} p_j^{a_j f(\mathcal{P}_j|(p_j))} \end{aligned}$$

or $v_{\mathcal{P}_j}(\alpha) := \frac{a_j}{e(\mathcal{P}_j|(p_j))}$ donc

$$\begin{aligned} \prod_{\substack{v \in \mathcal{M}_k \\ v|\infty}} |\alpha|_v^{n_v} &= \prod_{j=1}^{l} p_j^{f(\mathcal{P}_j|(p_j))e(\mathcal{P}_j|(p_j))v_{\mathcal{P}_j}(\alpha)} = \prod_{j=1}^{l} p_j^{v_{\mathcal{P}_j}(\alpha)n_{\mathcal{P}_j}} \\ &= \prod_{j=1}^{l} |\alpha|_{\mathcal{P}_j}^{-n_{\mathcal{P}_j}} = \prod_{\substack{v \in \mathcal{M}_k \\ v \nmid \infty}} |\alpha|_v^{-n_v} \end{aligned}$$

■

On s'intéresse maintenant au prolongements des valeurs absolues.

Définition 1.16 *Soient $\mathbb{Q} \subseteq k \subseteq F$ des corps de nombres, $v \in \mathcal{M}_k$ et $w \in \mathcal{M}_F$. On dit que w **divise** v et on note $w|v$ si pour tout α dans k, on a $|\alpha|_v = |\alpha|_w$.*

Proposition 1.5 *On reprend les mêmes notations.*

1. *Si $v, w|\infty$, associés respectivement aux plongements $\sigma : k \hookrightarrow \mathbb{C}$ et $\tau : F \hookrightarrow \mathbb{C}$ alors on a :*

$$w|v \iff \tau_{|k} = \sigma.$$

2. *Si $v, w \nmid \infty$, associés respectivement aux idéaux $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k) - \{(0)\}$ et $\mathcal{Q} \in \mathrm{Spec}(\mathcal{O}_F) - \{(0)\}$ alors on a :*

$$w|v \iff \mathcal{Q}|\mathcal{P}\mathcal{O}_F.$$

Démonstration -

1. Supposons $w|v$, on a par définition : $\forall \alpha \in k,\ |\sigma(\alpha)| = |\tau(\alpha)|$. Ainsi $\tau_{|k}$ est un plongement de k dans $\mathbb{C}$ qui définit la même valeur absolue que σ donc $\tau_{|k} = \sigma$, car il n'y a qu'un représentant de chaque classe dans $\mathcal{M}_k$.
   L'autre sens est facile.
2. Supposons $\mathcal{Q} \nmid \mathcal{P}\mathcal{O}_F$, on a alors $\mathcal{P}\mathcal{O}_F \nsubseteq \mathcal{Q}$ d'après 1.4 et a fortiori $\mathcal{P} \nsubseteq \mathcal{Q}$. Ainsi il existe $\alpha \in \mathcal{P} - \mathcal{Q}$, on a : $|\alpha|_{\mathcal{P}} < 1$ et $|\alpha|_{\mathcal{Q}} = 1$, donc $w \nmid v$.
   Supposons maintenant $\mathcal{Q} \mid \mathcal{P}\mathcal{O}_F$, et soit $\alpha \in \mathcal{O}_k - \{0\}$. Considérons les décompositions de (α) dans $\mathcal{O}_k$ et $\mathcal{O}_F$:

$$\begin{aligned} \alpha\mathcal{O}_k &= \mathcal{P}^{v_{\mathcal{P}}(\alpha)e(\mathcal{P}|P)} \\ \alpha\mathcal{O}_F &= \mathcal{P}\mathcal{O}_F^{v_{\mathcal{P}}(\alpha)e(\mathcal{P}|P)} \\ \alpha\mathcal{O}_F &= \mathcal{Q}_F^{e(\mathcal{Q}|\mathcal{P})v_{\mathcal{P}}(\alpha)e(\mathcal{P}|P)} \quad \text{or} \\ \alpha\mathcal{O}_F &= \mathcal{Q}_F^{e(\mathcal{Q}|P)v_{\mathcal{Q}}(\alpha)} \end{aligned}$$

   donc $v_{\mathcal{P}}(\alpha) = v_{\mathcal{Q}}(\alpha)$ et $|\alpha|_{\mathcal{P}} = |\alpha|_{\mathcal{Q}}$.

■

Lemme 1.3 *Soient $k \subseteq F$ deux corps de nombres, on a :*

$$\forall v \in \mathcal{M}_k,\ \sum_{\substack{w \in \mathcal{M}_F \\ w|v}} \frac{n_w}{n_v} = [F : k].$$

Démonstration -

• Supposons $v|\infty$, on a :

$$\sum_{\substack{w \in \mathcal{M}_F \\ w|v}} \frac{n_w}{n_v} = [F : k]_{\text{sep}}.$$

• Supposons $v \nmid \infty$, associé à un idéal $\mathcal{P}$, $\mathcal{P}\mathcal{O}_F = \mathcal{Q}_1^{e(\mathcal{Q}_1|\mathcal{P})} \dots \mathcal{Q}_l^{e(\mathcal{Q}_l|\mathcal{P})}$, on a :

$$\begin{aligned} \sum_{\substack{w \in \mathcal{M}_F \\ w|v}} \frac{n_w}{n_v} &= \sum_{j=1}^{l} \frac{n_{\mathcal{Q}_j}}{n_{\mathcal{P}}} \\ &= \sum_{j=1}^{l} \frac{e(\mathcal{Q}_j|\mathcal{P})f(\mathcal{Q}_j|\mathcal{P})}{e(\mathcal{P}|P)f(\mathcal{P}|P)} \\ &= \sum_{j=1}^{l} e(\mathcal{Q}_j|P)f(\mathcal{Q}_j|P) \\ &= [F : k]. \end{aligned}$$

■

IV Hauteurs et valuations.

Nous donnons ici une nouvelle définition de la hauteur d'un nombre algébrique, celle ci ayant l'avantage de se généraliser facilement en dimension supérieure, nous verrons plus tard que les 2 coïncident bien.

Définition 1.17 *Soient $\alpha \in \overline{\mathbb{Q}}$ et k un corps de nombres contenant α, on définit la* ***hauteur*** *de α :*

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

où $\log^+(|\alpha|)$ désigne $\log(\max\{1, |\alpha|\})$.

Ceci est une "bonne" définition (*i. e.* indépendante de k) : considérons un corps de nombres F contenant k ;

$$\begin{aligned}
\frac{1}{[F:\mathbb{Q}]} \sum_{w \in \mathcal{M}_F} n_v \log^+ |\alpha|_w &= \frac{1}{[F:\mathbb{Q}]} \sum_{v \in \mathcal{M}_k} \sum_{\substack{w \in \mathcal{M}_F \\ w|v}} n_w \log^+ |\alpha|_v \\
&= \frac{1}{[F:\mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log^+ |\alpha|_v \sum_{\substack{w \in \mathcal{M}_F \\ w|v}} \frac{n_w}{n_v} \\
&= \frac{[F:k]}{[F:\mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log^+ |\alpha|_v \\
&= \frac{1}{[k:\mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log^+ |\alpha|_v.
\end{aligned}$$

Propriétés 1.6 *Soient $\alpha, \beta \in k$ et $n \in \mathbb{Z}$, on a :*

1. $h(\alpha\beta) \leq h(\alpha) + h(\beta)$
2. $h(\alpha^n) = |n| \cdot h(\alpha)$
3. $h(\alpha) \geq 0$
4. $h(\alpha) = 0 \Longleftrightarrow \alpha \in \overline{\mathbb{Q}}^*_{tors}$ *(ou $\alpha = 0$)*
5. $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2$

Démonstration - Soient $\alpha, \beta \in k$

1. Soit $v \in \mathcal{M}_k$, on a $\max\{|\alpha\beta|, 1\} \leq \max\{|\alpha|, 1\} \max\{|\beta|, 1\}$, donc

$$\log^+ |\alpha\beta| \leq \log^+ |\alpha| + \log^+ |\beta|,$$

et a fortiori $h(\alpha\beta) \leq h(\alpha) + h(\beta)$.

2. Soit $n \in \mathbb{Z}$, on a :

$$\begin{aligned}\log^+ |\alpha|_v^n &= \log \max\{1, |\alpha|_v^n\} \\ &= |n| \log \max\{1, |\alpha|_v\} \text{ si } n \geq 1 \\ &= |n| \log \max\{1, |\alpha^{-1}|_v\} \text{ si } n < 1,\end{aligned}$$

il reste donc à montrer que $h(\alpha) = h(\alpha^{-1})$.

On a $\max\{1, |\alpha|_v\} / \max\{1, |\alpha|_v^{-1}\} = |\alpha|_v$ d'où :

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

Ainsi, d'après la formule du produit (1.3) :

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

3. Il suffit ici de remarquer que pour tout $x \in \mathbb{R}$, $\log^+(x) \geq 0$.

4. On a $h(\alpha) = 0 \Leftrightarrow \forall v \in \mathcal{M}_k,\ |\alpha|_v \leq 1$.

   En particulier : Pour tout $v \in \mathcal{M}_k, v \nmid \infty$, $|\alpha|_v \leq 1$ donc pour tout $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k)$, $v_{\mathcal{P}}(\alpha) \leq 0$ et $\alpha \in \mathcal{O}_k$, on a :

$$\begin{aligned}h(\alpha) = 0 &\Leftrightarrow \alpha \in \mathcal{O}_k \text{ et } |\sigma(\alpha)| \leq 1,\ \forall \sigma : k \hookrightarrow \mathbb{C} \\ &\Leftrightarrow \alpha = 0 \text{ ou } |\sigma(\alpha)| = 1,\ \forall \sigma : k \hookrightarrow \mathbb{C}, i.\ e.\ \alpha \in \mathcal{O}_k^*.\end{aligned}$$

   Donc si $h(\alpha) = 0$ alors α est un entier algébrique dont tous les conjugués sont de module inférieur à 1, donc, d'après un théorème de Kronecker (voir par exemple [Go] p.90), α est nul ou une racine de l'unité, *i. e.* un élément de $\overline{\mathbb{Q}}^*_{\mathrm{tors}}$.

5. On a :

$$\begin{aligned}\max\{1, |\alpha + \beta|_v\} &\leq \max\{1, |\alpha|_v + |\beta|_v\} \\ &\leq 2 \cdot \max\{1, |\alpha|_v, |\beta|_v\} \\ &\leq 2 \cdot \max\{1, |\alpha|_v\} \max\{1, |\beta|_v\}\end{aligned}$$

   d'où la dernière assertion de la propriété.

■

On sait que, pour tout entier x, $|x| \geq 1$, généralisons cela :

Théorème 1.9 (Inégalité de Liouville) *Soit $\alpha \in \overline{\mathbb{Q}}^*$, on pose :*

$$n_\infty := \begin{cases} 1 \ si \ \mathbb{Q}(\alpha) \subseteq \mathbb{R} \\ 2 \ si \ \mathbb{Q}(\alpha) \nsubseteq \mathbb{R}. \end{cases}$$

Alors,

$$n_\infty \log(\alpha) \geq -[\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha) \quad (= -\log M(\alpha)).$$

DÉMONSTRATION - On pose $k := \mathbb{Q}(\alpha) \subset \mathbb{C}$, on a :

$$\begin{aligned} 0 &= \sum_{v \in \mathcal{M}_k} n_v \log |\alpha|_v \\ &\leq n_\infty \log |\alpha| + \sum_{v \in \mathcal{M}_k} n_v \log^+ |\alpha|_v \\ &\leq n_\infty \log |\alpha| + [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha). \end{aligned}$$

■

Pour finir ce chapitre, nous allons montrer que les 2 hauteurs coïncident, commençons par introduire une nouvelle hauteur sur les polynômes :

Définition 1.18 *Soit $P \in \overline{\mathbb{Q}}[\mathrm{x}]$, $P = \sum_{j=0}^{d} a_j x^j$ et soit k un corps de nombres tel que $P \in k[\mathrm{x}]$, on pose :*

$$h_0(P) := \frac{1}{[k : \mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log |P|_v,$$

où

$$|P|_v := \begin{cases} \max_j |a_j|_v & si \ v \nmid \infty \\ M(\sigma(P)) & si \ v \mid \infty, \ v \sim \sigma \end{cases}$$

Remarque : Comme pour la hauteur d'un nombre algébrique, cette définition a bien un sens : elle ne dépend pas du corps k (même raisonnement).

Exemple : Soit $P \in \mathbb{Z}[\mathrm{x}]$ primitif (*i. e.* $\mathrm{pgcd}(a_j) = 1$), on a, pour tout p premier de $\mathbb{Z}$: $\max_j |a_j|_p = 1$, donc $h_0(P) = \log M(P)$.

Propriétés 1.7 *Soient $P, Q \in \overline{\mathbb{Q}}[\mathrm{x}]$ et $\lambda \in \overline{\mathbb{Q}}^*$, on a :*

1. $h_0(P \cdot Q) = h_0(P) + h_0(Q)$
2. $h_0(\lambda P) = h_0(P)$
3. $h_0(x - \lambda) = h(\lambda)$

DÉMONSTRATION -

1. Exercice.
2. Il suffit ici d'appliquer la formule du produit.
3. On a :

$$|x-\lambda|_v := \begin{cases} \max_j\{1,|\lambda|_v\} & \text{si } v \nmid \infty \\ M(\mathrm{x}-\sigma(\lambda)) & = \max\{1,|\sigma(\lambda)|\} \quad \text{si } v \mid \infty,\ v \sim \sigma \\ & = \max\{1,|\lambda|_v\} \end{cases}$$

d'où le résultat.

■

Lemme 1.4 *Soient $\alpha \in \overline{\mathbb{Q}}^*$, et $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.*
Alors $h(\sigma(\alpha)) = h(\alpha)$.

DÉMONSTRATION - Soient d le degré de α et $\alpha_1, \ldots, \alpha_d$ ses conjugués.
On pose $k := \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$, la clôture normale de $\mathbb{Q}(\alpha)$. Notre but ici est de montrer l'égalité :

$$\frac{1}{[k:\mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log \max\{1,|\alpha|_v\} = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log \max\{1,|\sigma(\alpha)|_v\}.$$

• Si $v|\infty$, $v \sim \tau : k \hookrightarrow$, on a :
$|\sigma(\alpha)|_v = |\tau \circ \sigma(\alpha)| = |\alpha|_{v'}$ où $v' \sim \tau \circ \sigma$.

• Si $v \nmid \infty$, $v \sim \mathcal{P}$, $(p) := \mathcal{P} \cap \mathbb{Z}$ on a :

$$\alpha\mathcal{O}_k = \mathcal{P}^a \ldots \text{ et } \sigma(\alpha)\mathcal{O}_k = (\sigma\mathcal{P})^a \ldots$$

De plus, (p) étant stable sous l'action de $\mathrm{Gal}(k/\mathbb{Q})$, si $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k)$ divise (p), alors $\sigma\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k)$ et divise (p) également. En appliquant le le corollaire de théorème 23 de [Ma] par exemple, on obtient :

$$e(\mathcal{P}|p) = e(\sigma\mathcal{P}|p),$$

d'où :

$$\forall \mathcal{P} \in \mathrm{Spec}(\mathcal{O}_k),\ |\alpha|_{\mathcal{P}} = p^{-\frac{1}{e(\mathcal{P}|p)}} = |\alpha|_{\sigma\mathcal{P}}.$$

■

Comme annoncé plus tôt, nous montrons ici que les 2 définitions de hauteur d'un nombe algébrique coïncident :

Théorème 1.10 *Soient $\alpha \in \overline{\mathbb{Q}}^*$, et P son polynôme minimal sur $\mathbb{Z}$, alors :*

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

DÉMONSTRATION - Soit d le degré de α, et notons $\alpha_1, \ldots, \alpha_d$ les conjugués de α, on a, d'après 1.7 :

$$\begin{aligned} \log M(P) &= \sum_{j=1}^{d} h_0(\mathrm{x} - \alpha_j) \\ &= \sum_{j=1}^{d} h(\alpha_j) \end{aligned}$$

Il suffit alors d'appliquer le lemme pour conclure. ■

Chapitre 2

Différents résultats.

I Théorème de Loher

On utilisera dans cette section la hauteur non logarithmique :

Définition 2.1 *Soit $\alpha \in \overline{\mathbb{Q}}$, on appelle hauteur non logarithmique et on note $H(\alpha)$ le nombre :*

$$H(\alpha) := \exp(h(\alpha)).$$

Remarque : Pour tout $\alpha \in \overline{\mathbb{Q}}^*$ et tout $n \in \mathbb{Z}$ on a : $H(\alpha^n) = H(\alpha)^{|n|}$ (voir propriétés 1.6).

Dans cette section nous allons donner un résultat effectif renforçant le théorème de Northcott 1.2. Rappellons que ce théorème énonce, que, étant donnés un entier naturel non nul D et un réel $H \geq 1$ on a :

$$\#\left\{\alpha \in \overline{\mathbb{Q}} \mid H(\alpha) \leq H, [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D\right\} < \infty,$$

et, par conséquent, si on fixe un corps de nombres k fixé, l'ensemble :

$$k(H) := \{\alpha \in k | H(\alpha) \leq H\}$$

est aussi de cardinal fini. Notre but est de donner une majoration de $\#k(H)$.

Un résultat de 1979 de S. Schanuel donne une première estimation du cardinal de $k(H)$.

Théorème 2.1 (Schanuel [Sch]) *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 et s le nombre de plongements réels et complexes (respectivement), et ζ_k la fonction zêta de k, nous avons*

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

avec

$$S_k(1) = \frac{h_k R_k/\omega_k}{\zeta_k(2)} \left(\frac{2^r(2\pi)^s}{\sqrt{|d_k|}}\right)^2 2^{r+s-1}.$$

Malheureusement, le terme d'erreur, qui provient d'un comptage de points entiers, semble difficile à rendre explicite. Le théorème suivant donne une majoration explicite du cardinal, avec une dépendance quasi-linéaire en le degré de k (en dehors du terme H^{2D}, inévitable d'après le théorème de Schanuel) :

Théorème 2.2 (Loher) *Soit k un corps de nombres, et soit $H > 0$, nous avons :*

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

Remarque : D'après le théorème de Kronecker 1.1, nous avons avec ces notations

$$k(1) = \mathcal{O}_k \cap \overline{\mathbb{Q}}^*_{\text{tors}} \cup \{0\},$$

et

$$\#k(1) = 1 + \omega_k,$$

pour tout corps de nombres k. En considérant un corps cyclotomique $k = \mathbb{Q}(\exp(2i\pi/n))$, nous avons $\omega_k = n$ et

$$[k : \mathbb{Q}] = \phi(n) \gg \frac{n}{\log \log n} \quad ([\text{HW, Theorem 328}]).$$

Nous en déduisons

$$\#k(1) = n + 1 \gg D \log \log D,$$

ce qui montre que, même pour une petite hauteur, l'estimation du théorème de Loher est étonamment précise.

Corollaire 2.1 *Pour tout corps de nombres k de degré $D \geq 2$, nous avons*

$$S_k(1) \leq 37 d \log d.$$

Corollaire 2.2 *Soit $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{tors}$ de degré D, alors :*

$$h(\alpha) \geq (74e)^{-1} D^{-2} (\log D)^{-1}.$$

DÉMONSTRATION - Soit $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{\text{tors}}$, de degré D et soit $H \geq 1$ un paramètre qui dépend de D.
Posons $N := \#k(H) + 1$; on a nécessairement :

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{N-1}\} \not\subseteq k(H),$$

il existe donc un entier $n \in \{0, \ldots, N-1\}$, tel que :

$$H(\alpha^N) > H \quad \text{et} \quad (N-1)h(\alpha) \geq nh(\alpha) > \log H.$$

Par ailleurs, le théorème de Loher assure que $N \leq 37(D \log D)H^{2D} + 1$, il vient donc

$$37(D \log D)H^{2D}h(\alpha) > \log H,$$

et

$$h(\alpha) > \frac{\log H}{37(D \log D)H^{2D}}.$$

En étudiant le terme de droite de cette inégalité, il est facile de voir que le bon choix pour la valeur du paramètre H est $H = e^{1/2D}$ pour laquelle nous obtenons

$$h(\alpha) > \frac{1/2D}{37(D \log D)e} = (74e)^{-1}D^{-2}(\log D)^{-1}.$$

■

Le reste de cette section est consacrée à la preuve du théorème de Loher. Elle repose sur l'utilisation de l'inégalité d'Hadamard (lemme 2.1), de la formule du produit (Théorème 1.3) et sur le principe des tiroirs de Dirichlet.

I.1 Lemmes préliminaires.

Lemme 2.1 (Inégalité de Hadamard) , *Soient $N \in \mathbb{N}^*$ et $A \in M_N(\mathbb{C})$, $A = (z_{i,j})_{i,j}$, on pose $\Delta := \det A$, on a :*

$$|\Delta| \leq \prod_{i=1}^{N} \Big(\sum_{j=1}^{N} |z_{i,j}|^2\Big)^{1/2}$$
$$|\Delta| \leq \sum_{j=1}^{N} \Big(\prod_{i=1}^{N} |z_{i,j}|^2\Big)^{1/2}.$$

On va appliquer ce lemme au Van Der Monde de N points $\alpha_1, \ldots, \alpha_N$, *i. e.* :

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{N-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{N-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_N & \alpha_N^2 & \ldots & \alpha_N^{N-1} \end{pmatrix}$$

Notation : Dans la suite, $B(z, r)$ désigne la boule fermée de centre z et de rayon r.

Lemme 2.2 *Soient $z \in \mathbb{C}$, $r > 0$, $n \in \mathbb{N}^*$ et $\alpha_1, \ldots, \alpha_n \in B(z,r)$, alors*

$$|\det(\alpha_i^{j-1})| \leq N^{N/2} r^{N(N-1)/2}.$$

DÉMONSTRATION - Le determinant étant une application multilinéaire alternée, quitte à composer par l'application $\alpha_j \mapsto (\alpha_j - z)/r$, on peut supposer $z = 0$ et $r = 1$, *i. e.* pour tout $(i,j) \in \{1, \ldots, N\}^2$, $|\alpha_i^{j-1}| \leq 1$.

On applique alors l'inégalité d'Hadamard du lemme 2.1 au Van Der Monde des α_i :

$$\begin{aligned} |\det(\alpha_i^{j-1})|^2 &\leq \prod_{i=1}^{N} \left(\sum_{j=1}^{N} |\alpha_i|^{2(j-1)} \right) \\ &\leq \prod_{i=1}^{N} N \\ &\leq N^N. \end{aligned}$$

■

Lemme 2.3 *Soient $r \in \mathbb{R}_+^*$, $n \in \mathbb{N}$ et $S \subset \mathbb{R}^N$; on pose $M := \#\big(S \cap B(0,1)\big)$ et on suppose $M \geq 1$.*

Alors, il existe $z \in B(0,1)$ tel que

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

DÉMONSTRATION - Soit $z \in B(0, 1+r)$, on pose

$$M(z) := \#\big(S \cap B(z,r)\big).$$

Pour tout sous-ensemble A de $\mathbb{R}^N$, on note χ_A sa fonction indicatrice ; remarquons que pour tout $z, w \in \mathbb{R}^N$ on a $\chi_{B(z,r)}(w) = \chi_{B(w,r)}(z)$.

Quitte à considérer $S \cap B(0,1)$, on peut supposer $S \subseteq B(0,1)$, on obtient alors :

$$\begin{aligned} \sum_{w \in S} \int_{B(0,1+r)} \chi_{B(w,r)}(z) dz &= \int_{B(0,1+r)} \sum_{w \in S} \chi_{B(w,r)}(z) dz \\ &= \int_{B(0,1+r)} \underbrace{\sum_{w \in S'} \chi_{B(z,r)}(w)}_{M(z)} dz \end{aligned}$$

Pour $w \in S$, on a $B(w,r) \subseteq B(0, 1+r)$, donc $\int_{B(0,1+r)} \chi_{B(w,r)}(z) dz$ est égale à la mesure de Lebesgue de $B(w,r)$, c'est à dire à $\gamma_n r^N$, pour un certain γ_n, donc

$$\sum_{w \in S} \int_{B(0,1+r)} \chi_{B(w,r)}(z) dz = \sum_{w \in S} \gamma_n r^N = M \gamma_n r^N.$$

La valeur moyenne de $M(z)$ sur la boule $B(0,1+r)$ vaut alors :

$$\int_{B(0,1+r)} M(z)dz = \frac{1}{\gamma_n(1+r)^N} \int B(0,1+r)M(z)dz = M\left(\frac{r}{1+r}\right)^N.$$

Il existe donc $z \in B(0,1+r)$ tel que

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

■

I.2 Preuve du théorème de Loher (2.2)

On montrera ici simplement l'estimation :

$$\#k(H) \ll (D\log D)H^{2D}.$$

Par le théorème de Northcott 1.2, nous savons que le cardinal de $k(H)$ est fini. De plus $k(H)$ contient 0, 1, et -1, et, comme $H(\alpha) = H(\alpha^{-1})$ pour tout $\alpha \neq 0$, les autres éléments de $k(H)$ se regroupe en couple (α, α^{-1}) avec $\alpha \neq \alpha^{-1}$; soit M l'entier tel que $\#k(H) = 2M+1$. Il existe alors M éléments non nuls $\alpha_1, \ldots, \alpha_M$ dans $k(H)$ de module inférieur ou égal à 1.

Pour tout $N \in \{1, \ldots, M-1\}$, notons

$$r_N := \frac{1}{\left(\frac{M}{N}\right)^{1/n_\infty} - 1},$$

où $n_\infty = 1$ si $k \subset \mathbb{R}$ et $n_\infty = 2$ sinon. Pour tout $N < M/4$, on a $r_N < 1$ et

$$N := \left(\frac{r_N}{1+r_N}\right)^{n_\infty} M \geq \left(\frac{r_N}{1+r_N}\right)^2 M.$$

Nous considérerons dans la suite un entier $N < M/4$.

Quitte à renuméroter les α_j, d'après le lemme 2.3, avec $S = k(H)$, il existe un complexe $z \in \mathbb{C}$ tel que $\alpha_1, \ldots, \alpha_N \in B(z, r_N)$. Par le lemme 2.2, le déterminant de Van der Monde $\Delta_N := \det(\alpha_i^{j-1})$ qui est non nul (puisque les α_i sont distincts), vérifie :

$$|\Delta_N| \leq N^{N/2} r_N^{N(N-1)/2}.$$

Evaluons $|\Delta_N|_v$ pour toute place v du corps k.
Tout d'abord, pour une place archimédienne v associé à un plongement σ de k dans $\mathbb{C}$,

nous avons, par l'inégalité de Hadamard :

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

donc

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

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

$$\forall (i,j) \in \{1, \ldots, N\}^2, \ |\alpha_i - \alpha_j|_v \leq \max(1, |\alpha_i|_v) \times \max(1, |\alpha_j|_v),$$

il vient

$$\begin{aligned} |\Delta_N|_v &\leq \prod_{i=1}^{N} \max(1, |\alpha_i|_v)^{N-1} \qquad \text{si } v \nmid \infty \\ |\Delta_N|_\infty &\leq N^{N/2} \cdot r_N^{N(N-1)/2} \\ |\Delta_N|_v &\leq N^{N/2} \prod_{i=1}^{N} \max(1, |\alpha_i|_v)^{N-1} \quad \text{si } v \mid \infty, \ |.|_v \neq |.|_\infty \end{aligned}$$

En appliquant la formule du produit au déterminant $\Delta_N \neq 0$, on obtient :

$$\begin{aligned} 1 &= \prod_{v \in \mathcal{M}_k} |\Delta_N|_v \\ &\leq (N^{N/2})^{\sum_{\substack{v \in \mathcal{M}_k \\ v \mid \infty}} n_v} \left(r_N^{N(N-1)/2} \right)^{n_\infty} \left[\prod_{v \in \mathcal{M}_k} \prod_{i=1}^{N} \max(1, |\alpha_i|_v)^{n_v} \right]^{N-1} \\ &\leq N^{DN/2} \cdot r_N^{n_\infty N(N-1)/2} \cdot \prod_{i=1}^{N} H(\alpha_i)^{D(N-1)} \\ &\leq N^{DN/2} \cdot r_N^{n_\infty N(N-1)/2} \cdot H^{DN(N-1)}, \end{aligned}$$

d'où

$$\left(\left(\frac{M}{N} \right)^{1/n_\infty} - 1 \right)^{n_\infty N(N-1)/2} \leq N^{DN/2} H^{DN(N-1)}.$$

On en déduit :

$$\left(\frac{M}{N} \right)^{1/n_\infty} \leq 1 + N^{D/((N-1)n_\infty)} H^{2D/n_\infty} \leq \sqrt{2} \cdot (1 + N^{D/(N-1)} H^{2D})^{1/n_\infty},$$

et

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

Enfin, par hypothèse, nous avons $\#k(H) = 2M+1$. Si $M \ll D\log D$, alors le résultat de Loher est immédiatement montré.

Dans le cas contraire, le choix de paramètre $N = O(D\log D)$, avec $N < M/4$, donne l'estimation attendue, $1 + N^{D/(N-1)}$ étant alors borné :

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

pour une certaine constante c. ■

II Cas particulier d'une extension abélienne

Bien que la conjecture de Lehmer reste encore non démontrée, on peut dans certains cas obtenir de meilleurs résultats, c'est le cas notamment dans le cas d'une extension abélienne de $\mathbb{Q}$, *i. e.* galoisienne de groupe de galois abélien. Plus précisément, F. Amoroso et R. Dvornicich [AmDv1] ont montré le résultat suivant :

Théorème 2.3 *Soit $L/\mathbb{Q}$ une extension abélienne et soit $\alpha \in L*$, $\alpha \notin \overline{\mathbb{Q}}^*_{tors}$, alors*

$$h(\alpha) \geq \frac{\log(5/2)}{10}.$$

Par des arguments un peu plus fins, [AmDv1] ont même montré $h(\alpha) \geq \frac{\log(5)}{12}$.

Comme nous le verrons, de cette minoration découle une nouvelle preuve du théorème de Smyth concernant les nombres algébriques non réciproques, et la détermination du nombre de classes d'ideaux dans une extension abélienne.

II.1 Nombres algébriques contenus dans une extension abélienne

L'argumentation est basée sur un résultat classique de théorie de Galois, le théorème de Kronecker-Weber, dont on pourra trouver une preuve dans [Wa].

Théorème 2.4 (Kronecker-Weber) *Toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique.*

La hauteur d'un nombre algébrique étant indépendante du corps de nombres le contenant que l'on considère, le théorème de Kronecker-Weber nous permet donc de nous limiter à l'étude de la hauteur d'un nombre algébrique d'une extension cyclotomique de $\mathbb{Q}$.

Notons, pour toute la suite, ζ_m une racine primitive m-ième de l'unité et $k_m := \mathbb{Q}(\zeta_m)$, le corps cyclotomique de degré $\phi(m)$. Comme $k_m = k_{2m}$ pour m impair, on peut supposer $m \not\equiv 2 \pmod 4$. Nous allons donner, dans la proposition 2.1, une minoration de la hauteur de $\alpha \in k_m^* \setminus \overline{\mathbb{Q}}^*_{\text{tors}}$, et pour cela nous aurons besoin des deux lemmes suivants :

Lemme 2.4 *Soit p un nombre premier impair, alors il existe $\sigma_p \in Gal(k_m/\mathbb{Q})$ tel que :*

- *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 ne divise pas 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, si $\sigma_p(\alpha^p) = \alpha^p$ pour un certain $\alpha \in k_m$, alors il existe $\zeta \in k_m$, une racine de l'unité, tel que $\zeta\alpha$, appartienne à une sous extension cyclotomique stricte de k_m.

DÉMONSTRATION -

• Supposons tout d'abord que $p \nmid m$, et soit $\sigma_p : k_m \longrightarrow \mathbb{Q}$ le morphisme de corps défini par $\sigma_p(\zeta_m) = \zeta_m^p$ et $\mathbb{Q}$-linéarité.
Soit $\gamma \in \mathcal{O}_{k_m} (= \mathbb{Z}[\zeta_m])$ et soit $F \in \mathbb{Z}[\mathrm{x}]$ tel que $\gamma = F[\zeta_m]$.

Or, pour tout $F \in \mathbb{Z}[\mathrm{x}]$, il existe $G \in \mathbb{Z}[\mathrm{x}]$ tel que $F(\mathrm{x})^p = F(\mathrm{x}^p) + pG(\mathrm{x})$. En effet, par le petit théorème de Fermat, le résultat est immédiat pour un monôme, et de plus si cette propriété est vraie pour F_1 et F_2, elle est immédiatement vérifiée pour $F_1 + F_2$ (par le fait classique que $\binom{n}{p}$ est divisible par p pour $n \in \{1, \ldots, p-1\}$).
Nous avons donc :

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

• Supposons désormais que $p|m$, et considérons cette fois σ_p un générateur du groupe $\mathrm{Gal}(k_m/k_{m/p})$ (qui est cyclique car sous-groupe de $\mathrm{Gal}(k_m/\mathbb{Q})$, d'ordre p si p^2 divise m, et d'ordre $p-1$ sinon ; regarder $\phi(m)$ et $\phi(m/p)$).
Soit $\gamma \in \mathcal{O}_{k_m}$, soit $F \in \mathbb{Z}[\mathrm{x}]$ tel que $\gamma = F[\zeta_m]$; comme précédemment il existe $G \in \mathbb{Z}[\mathrm{x}]$ tel que $F(\mathrm{x})^p = F(\mathrm{x}^p) + pG(\mathrm{x})$. Puisque $\zeta_m^p \in k_{m/p}$, il vient $\sigma_p(\zeta_m^p) = \zeta_m^p$, et par suite :

$$\begin{aligned} \gamma^p = F(\zeta_m)^p &\equiv F(\zeta_m^p) \bmod p\mathcal{O}_{k_m} \\ &\equiv F(\sigma_p(\zeta_m^p)) \bmod p\mathcal{O}_{k_m} \\ &\equiv \sigma_p(\gamma^p) \bmod p\mathcal{O}_{k_m}. \end{aligned}$$

Enfin, puisque $\sigma_p(\zeta_m)^p = \sigma_p(\zeta_m^p) = \zeta_m^p$ et puisque σ_p est générateur de $\mathrm{Gal}(k_m/k_{m/p})$, nous avons

$$\sigma_p(\zeta_m) = \zeta_p\zeta_m,$$

où ζ_p est une racine p-ième primitive de l'unité.
Supposons qu'il existe $\alpha \in k_m$ tel que $\sigma_p(\alpha^p) = \alpha^p$, alors par le même argument, il existe un entier u tel que $\sigma_p(\alpha) = \zeta_p^u\alpha$, nous en déduisons :

$$\sigma_p\left(\frac{\alpha}{\zeta_m^u}\right) = \frac{\zeta_p^u\alpha}{\zeta_p^u\zeta_m^u} = \frac{\alpha}{\zeta_m^u},$$

Comme σ_p est générateur de $\mathrm{Gal}(k_m/k_{m/p})$, et laisse fixe α/ζ_m^u, et il vient $\alpha/\zeta_m^u \in k_{m/p}$, ce qui achève la preuve du lemme, si l'on pose $\zeta := \zeta_m^{-u}$. ■

Lemme 2.5 *Soient k un corps de nombres, α un élément de k, et $v \in \mathcal{M}_k$ une valuation ultramétrique sur k (i. e. $v \nmid \infty$), alors il existe $\beta \in \mathcal{O}_k$, tel que $\beta\alpha \in \mathcal{O}_k$, et*

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

DÉMONSTRATION - Fixons une valuation w_0 ultramétrique quelconque et posons :

$$\Sigma := \left\{ w \in \mathcal{M}_k,\ w \nmid \infty \mid \max\{1, |\alpha|_w\} > 1 \right\} \cup \{v\}.$$

Pour toute place $w \in \Sigma$, notons aussi notons :

$$\begin{cases} 0_w := 1 & \text{si } \ w = v \text{ et si } \ |\alpha|_v \leq 1, \\ 0_w := \alpha^{-1} & \text{sinon .} \end{cases}$$

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

$$\begin{cases} |\beta - 0_w|_w < \max\{1, |\alpha|_w\}^{-1}, & \text{pour tout } w \in \Sigma, \\ |\beta|_w \leq 1, & \text{si } w \notin \Sigma \cup \{w_0\}. \end{cases}$$

Sachant que $|0_w|_w = \max\{1, |\alpha|_w\}^{-1}$ pour tout $w \in \Sigma$ et en utilisant l'inégalité ultramétrique à $\beta = \beta - (\beta - 0_w)$, on en déduit :

$$\begin{cases} |\beta|_w = \max\{1, |\alpha|_w\}^{-1}, & \text{pour tout } w \in \Sigma, \\ |\beta|_w \leq 1, & \text{si } w \notin \Sigma \cup \{w_0\}. \end{cases}$$

En particulier, pour toute place finie w de k on a $|\beta|_w \leq 1$ (et donc $\beta \in \mathcal{O}_k$) ; de même, $|\beta\alpha|_w \leq |\beta|_w \max\{1, |\alpha|_w\} \leq 1$ (et donc $\beta\alpha \in \mathcal{O}_k$).
Enfin, on a bien $|\beta|_v = \max\{1, |\alpha|_v\}^{-1}$ (car $v \in \Sigma$). Le lemme est donc établi. ■

Remarque : Le β du lemme peut être qualifié de dénominateur « local » de α.

Proposition 2.1 *Soit p un nombre premier, $p \geq 3$, et soit $\alpha \in k_m^*$, $\alpha \notin \overline{\mathbb{Q}}^*_{tors}$, alors*

$$h(\alpha) \geq \begin{cases} \dfrac{\log(p/2)}{p+1} & \text{si } p \nmid m \\ \\ \dfrac{\log(p/2)}{2p} & \text{si } p \mid m \end{cases}$$

DÉMONSTRATION -

• Supposons tout d'abord que p ne divise pas m. Soit $v \in \mathcal{M}_{k_m}$, $v \mid p$. Par le lemme 2.5, il existe $\beta \in \mathcal{O}_{k_m}$, tel que $\beta\alpha \in \mathcal{O}_{k_m}$, , et $\mid \beta \mid_v = \max(1, \mid \alpha \mid_v)^{-1}$, et par le lemme 2.4, il existe un morphisme $\sigma_p \in \mathrm{Gal}(k_m/\mathbb{Q})$ tel que

$$\mid (\alpha\beta)^p - \sigma_p(\alpha\beta) \mid_v \leq \frac{1}{p}.$$

En effet, $(\alpha\beta) - \sigma_p(\alpha\beta) \in p\mathcal{O}_{k_m}$, et de même :

$$\mid \beta^p - \sigma_p(\beta) \mid_v \leq \frac{1}{p}.$$

Nous allons chercher à évaluer $\mid \alpha^p - \sigma_p(\alpha) \mid_v$, pour toute place v afin d'obtenir en utilisant la formule du produit, l'inégalité reliant la hauteur logarithmique de α à p.

Pour toute valeur absolue ultramétrique $v \mid p$, nous avons

$$\begin{aligned}
\mid \alpha^p - \sigma_p(\alpha) \mid_v &= \mid \beta \mid_v^{-p} \mid (\alpha\beta)^p - \sigma_p(\alpha\beta) + (\sigma_p(\beta) - \beta^p)\sigma_p(\alpha) \mid_v \\
&\leq \mid \beta \mid_v^{-p} \max\{\mid (\alpha\beta)^p - \sigma_p(\alpha\beta) \mid_v, \mid \sigma_p(\beta) - \beta^p \mid_v \mid \sigma_p(\alpha) \mid_v\} \\
&\leq \frac{1}{p} \mid \beta \mid_v^p \max\{1, \mid \sigma_p(\alpha) \mid_v\} \\
&= \frac{1}{p} \max\{1, \mid \alpha \mid_v\} \max\{1, \mid \sigma_p(\alpha) \mid_v\}
\end{aligned}$$

Pour les autres valeurs absolues ultramétriques $v \nmid p$, $v \nmid \infty$, nous obtenons en utilisant l'inégalité ultramétrique :

$$\mid \alpha^p - \sigma_p(\alpha) \mid_v \leq \max\{1, \mid \alpha \mid_v\} \max\{1, \mid \sigma_p(\alpha) \mid_v\}.$$

Et enfin pour les valeurs absolues archimédiennes $v \mid \infty$, nous obtenons par l'inégalité triangulaire :

$$\mid \alpha^p - \sigma_p(\alpha) \mid_v \leq 2 \max\{1, \mid \alpha \mid_v\} \max\{1, \mid \sigma_p(\alpha) \mid_v\}.$$

Puisque par hypothèse, $\alpha \notin \overline{\mathbb{Q}}^*_{\mathrm{tors}}$, nous avons $\alpha^p - \sigma_p(\alpha) \neq 0$. En effet, l'hypothèse contraire impliquerait $h(\alpha^p) = h(\sigma_p(\alpha)) = h(\alpha)$, et donc $h(\alpha) = 0$, ce qui d'après le théorème de Kronecker 1.1 entrainerait $\alpha = 0$ ou $\alpha \in \overline{\mathbb{Q}}^*_{\mathrm{tors}}$.

Nous pouvons donc appliquer la formule du produit à $\alpha - \sigma_p(\alpha)$, et nous obtenons :

$$\begin{aligned} 0 &= \sum_{v\in\mathcal{M}_{k_m}} n_v \log|\alpha-\sigma_p(\alpha)|_v \\ &\leq \sum_{\substack{v\in\mathcal{M}_{k_m}\\ v|p}} n_v \log\Big(\frac{1}{p}\max\{1,|\alpha^p|_v\}\max\{1,|\sigma_p(\alpha)|_v\}\Big) \\ &\quad + \sum_{\substack{v\in\mathcal{M}_{k_m}\\ v|\infty}} n_v \log\Big(2\max\{1,|\alpha^p|_v\}\max\{1,|\sigma_p(\alpha)|_v\}\Big) \\ &\quad + \sum_{\substack{v\in\mathcal{M}_{k_m}\\ v\nmid p, v\nmid\infty}} n_v \log\Big(\max\{1,|\alpha^p|_v\}\max\{1,|\sigma_p(\alpha)|_v\}\Big) \end{aligned}$$

Nous en déduisons

$$\begin{aligned} 0 &\leq -\log p \sum_{\substack{v\in\mathcal{M}_{k_m}\\ v|p}} n_v + \log 2 \sum_{\substack{v\in\mathcal{M}_{k_m}\\ v|\infty}} n_v \\ &\quad + \sum_{v\in\mathcal{M}_{k_m}} n_v \log\Big(\max\{1,|\alpha^p|_v\}\max\{1,|\sigma_p(\alpha)|_v\}\Big) \end{aligned}$$

Et en relachant les deux premières sommes, il vient l'inégalité

$$[k_m:\mathbb{Q}](\log 2-\log p)+\sum_{v\in\mathcal{M}_{k_m}} n_v \log(\max(1,|\ \alpha\ |_v))^p+\sum_{v\in\mathcal{M}_{k_m}} n_v \log(\max(1,\sigma_p(\alpha)\ |_v))\geq 0$$

d'où :

$$0\leq\Big(-\log\frac{p}{2}+ph(\alpha)+h(\sigma(\alpha))\Big)\,[k_m:\mathbb{Q}]$$

qui donne bien l'inégalité recherchée.

• Dans le cas où p divise m, nous pouvons montrer *mutatis mutandis* la seconde inégalité en remplacant naturellement $\sigma_p(\alpha)$ par $\sigma_p(\alpha^p)$, en utilisant les lemmes 2.4 et 2.5.

Nous avons alors les inégalités

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

à partir desquelles, en appliquant la formule du produit à $\alpha^p-\sigma_p(\alpha)^p\neq 0$, nous déduisons

$$0\leq\Big(\log\frac{1}{p}+\log 2+ph(\alpha)+ph(\sigma_p(\alpha))\Big)\,[k_m:\mathbb{Q}]$$

qui fournit là encore l'inégalité attendue. ■

DÉMONSTRATION - (du théorème 2.3.)

La proposition précédente, avec $p = 5$, *via* Kronecker-Weber, nous donne le résultat.

■

II.2 Application à la structure du groupe des classes.

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

Rappellons qu'une extension $k/\mathbb{Q}$ est CM lorsque k est une extension quadratique imaginaire d'un corps k' totallement réel, c'est-à-dire $k \not\subseteq \mathbb{R}$ et

$$\forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\ \sigma(k') \subset \mathbb{R}.$$

En particulier, si $k/\mathbb{Q}$ est galoisienne, on a :

$$k/\mathbb{Q} \text{ CM} \iff \sigma \in \mathcal{Z}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})), \sigma \neq \mathrm{id}$$

où σ désigne la conjugaison complexe et $\mathcal{Z}$ le centre du groupe ; le résultat sera donc vérifié dans toute extension abélienne de $\mathbb{Q}$, non réelle.

Lemme 2.6 *Soit k un corps de nombres tel que l'extension $k/\mathbb{Q}$ soit galoisienne CM, et soit $\gamma \in \mathcal{O}_k \setminus \{0\}$, alors*

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

DÉMONSTRATION - Soit $\gamma \in \mathcal{O}_k \setminus \{0\}$, posons $\alpha := \gamma/\overline{\gamma}$; pour tout $v \in \mathcal{M}_{k,\infty}$, nous avons $|\alpha|_v = 1$. En effet, si $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ est associée v, on a :

$$|\sigma(\alpha)|_\infty = \left|\frac{\sigma(\gamma)}{\sigma(\overline{\gamma})}\right|_\infty = \left|\frac{\sigma(\gamma)}{\overline{\sigma(\gamma)}}\right|_\infty = 1.$$

où l'hypothèse que l'extension est CM est indispensable pour la seconde égalité.

La hauteur logarithmique absolue de α vérifie donc :

$$[k : \mathbb{Q}]h(\alpha) = \sum_{v \in \mathcal{M}_k} n_v \log^+ \left|\frac{\gamma}{\overline{\gamma}}\right|_v = \sum_{\substack{v \in \mathcal{M}_k \\ v \nmid \infty}} n_v \log^+ \left|\frac{\gamma}{\overline{\gamma}}\right|_v.$$

D'où, en appliquant la formule du produit 1.3 à $\overline{\gamma}$, nous obtenons

$$[k : \mathbb{Q}]h(\alpha) = \sum_{\substack{v \in \mathcal{M}_k \\ v \nmid \infty}} n_v \log^+ \left|\frac{\gamma}{\overline{\gamma}}\right|_v + \sum_{v \in \mathcal{M}_k} n_v \log |\overline{\gamma}|_v,$$

et

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

puisque γ et $\overline{\gamma}$ sont des entiers algébriques, et vérifient $\mid \gamma \mid_v \leq 1$ et $\mid \overline{\gamma} \mid_v \leq 1$ pour toute valeur absolue $|\cdot|_v$ ultramétrique.
Or, $N_{\mathbb{Q}}^k(\gamma) = N_{\mathbb{Q}}^k(\overline{\gamma}) = \prod_{\substack{v\in\mathcal{M}_k\\ v|\infty}} |\overline{\gamma}|_v^{n_v}$, nous en déduisons l'inégalité annoncée

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

■

Proposition 2.2 *Soit $m \in \mathbb{N}^*$, tel que l'anneau des entiers $\mathcal{O}_{k_m}$ de k_m soit principal, alors pour tout premier $p \equiv 1 \pmod m$, nous avons*

$$\log p \geq \frac{\log 5}{12} \cdot \phi(m).$$

DÉMONSTRATION - Il est bien connu que le degré $[k_m : \mathbb{Q}]$ vaut $\phi(m)$, où ϕ désigne la fonction indicatrice d'Euler. Nous admettrons que dans k_m, pour qu'un premier p soit totalement décomposé, il faut et il suffit que m divise $p-1$.

L'anneau des entiers $\mathcal{O}_{k_m}$ étant principal, et le nombre premier p considéré vérifiant la congruence $p \equiv 1 \bmod m$, il existe un entier algébrique $\gamma \in \mathcal{O}_{k_m}$, tel que :

$$p = u\gamma_1 \ldots \gamma_{\phi(m)},$$

où u est une unité de $\mathcal{O}_{k_m}$, et les γ_j pour $j \in \{1, \ldots, \phi(m)\}$, sont les conjugués de γ.
Par le lemme précédent, et la forme renforcée du théorème 2.3, nous trouvons

$$\log \mid N_{\mathbb{Q}}^k(\gamma) \mid \geq \phi(m) h(\gamma/\overline{\gamma}) \geq \frac{\log 5}{12}\phi(m).$$

De plus, nous avons

$$p^{\phi(m)} = \mid N_{\mathbb{Q}}^k(p) \mid = \mid N_{\mathbb{Q}}^k(u) \mid\mid N_{\mathbb{Q}}^k(\gamma_1) \mid \ldots \mid N_{\mathbb{Q}}^k(\gamma_{\phi(m)}) \mid = \mid N_{\mathbb{Q}}^k(\gamma) \mid^{\phi(m)},$$

donc $p = \mid N_{\mathbb{Q}}^{k}(\gamma) \mid$, et finalement, nous obtenons l'inégalité cherchée

$$\log p \geq \frac{\log 5}{12}\phi(m).$$

■

Application : L'anneau des entiers de $\mathbb{Q}(\zeta_{100})$ n'est pas principal.
En effet, supposons par l'absurde le contraire, alors $p = 101 \equiv 1 \pmod{100}$ est totalement décomposé dans $\mathcal{O}_{\mathbb{Q}(\zeta_{100})}$, et d'après ce qui précède nous avons

$$\log 101 \geq \frac{\log 5}{12}\phi(100),$$

or $\phi(100) = \phi(25)\phi(4) = 20$ et nous obtenons $101^3 \geq 5^{10}$, ce qui n'est pas.

A partir du théorème de Linnik, un résultat difficile de théorie analytique des nombres, nous allons pouvoir généraliser ce qui précède aux extensions cyclotomiques de $\mathbb{Q}$.

Théorème 2.5 (Linnik) *Il existe $L > 0$ tel que pour tout entier $m \geq 2$, il existe un nombre premier p vérifiant $p \equiv 1 \pmod{m}$ et $p < m^L$.*

Corollaire 2.3 *Il n'existe qu'un nombre fini de corps cyclotomiques dont l'anneau des entiers est principal.*

Remarque : En fait, ce résultat est connu depuis 1976 [MM], et l'on sait même qu'il y a exactement 29 corps cyclotomiques k_m dont l'anneau des entiers est principal (pour $m = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$).

DÉMONSTRATION - Par le théorème de Mertens [HW, Theorem 429], il existe une constante absolue $c > 0$, telle que

$$\phi(m) \geq c\frac{m}{\log m}$$

pour tout entier $m \in \mathbb{N}^*$.
Supposons qu'il existe une infinité de corps cyclotomiques dont l'anneau des entiers est principal. Soit m un entier tel que l'anneau des entiers $\mathcal{O}_{k_m}$ de k_m est principal, et soit p le plus petit premier totalement décomposé dans $\mathcal{O}_{k_m}$. En appliquant les théorèmes de Linnik et de Mertens, la proposition précédente entraine

$$\frac{\log 5}{12} \leq \frac{\log p}{\phi(m)} \leq \frac{\log m}{L\phi(m)} \leq \frac{(\log m)^2}{cLm},$$

et puisque le terme de droite tend vers 0 lorsque m tend vers $+\infty$, nous obtenons une contradiction pour m suffisamment grand. ■

Par un raisonnement analogue, 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 galoisienne CM quelconque.

II.3 Version faible du théorème de Smyth

Le théorème d'Amoroso-Dvornicich 2.3 permet d'obtenir une nouvelle démonstration du théorème de Smyth sur les nombres algébriques non réciproques, avec cependant une constante moins bonne.

Lemme 2.7 *Soit α un entier algébrique non réciproque, de polynôme minimal F de degré D sur $\mathbb{Z}$. Pour tout premier p, notons $\gamma_p = F(\zeta_p)$ où $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$, alors pour tout premier $p \geq 2D+3$, nous avons $\gamma_p/\overline{\gamma_p} \notin \overline{\mathbb{Q}}^*_{tors}$.*

Remarque : L'hypothèse de non reciprocité de α est nécessaire, en effet, dans le cas contraire, nous avons $\gamma_p = F(\zeta_p)$ et $F(\mathrm{x}) = \mathrm{x}^D F(\frac{1}{\mathrm{x}})$ entraine $\overline{\gamma_p} = F(\overline{\zeta_p}) = F(\zeta_p^{-1}) = \zeta_p^{-D} F(\zeta_p)$ et $\gamma_p/\overline{\gamma_p} = \zeta_p^{-D} \in \overline{\mathbb{Q}}^*_{\mathrm{tors}}$.

DÉMONSTRATION - Par construction, $\gamma_p/\overline{\gamma_p} \in \mathbb{Q}(\zeta_p)$. Supposons par l'absurde que $\gamma_p/\overline{\gamma_p} \in \overline{\mathbb{Q}}^*_{\mathrm{tors}}$, 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 $j \in \{-1, p-2\}$ tel que

$$\gamma_p/\overline{\gamma_p} = (-1)^i \zeta_p^j$$

Puisque $\overline{\gamma_p} = F(\zeta_p^{-1})$, il vient $F(\zeta_p) = (-1)^i \zeta_p^j F(\zeta_p^{-1})$, et $\zeta_p^D F(\zeta_p) = (-1)^i \zeta_p^j F^*(\zeta_p)$.
Posons $G(\mathrm{x}) := \mathrm{x}^{\max\{D-j,0\}} F(\mathrm{x}) + (-1)^{i+1} \mathrm{x}^{max\{j-D,0\}} F^*(\mathrm{x})$. D'après la remarque précédente, nous avons $G(\zeta_p) = 0$.
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 polynôme cyclotomique Φ_p de degré $p-1$ divise G, et comme G est non nul, $\deg G \geq p-1$.
Or $\deg G \leq \mid D-j \mid + D \leq \max\{2D-j, j\} \leq \max\{2D+1, p-2\}$ par le choix de j, et pour $p \geq 2D+3$ nous obtenons une contradiction.
Donc $\gamma_p/\overline{\gamma_p} \notin \overline{\mathbb{Q}}^*_{\mathrm{tors}}$, pour tout premier $p \geq 2D+3$. ■

Théorème 2.6 (Version faible du théorème de Smyth) *Soit α un nombre algébrique non réciproque de degré D, alors*

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

DÉMONSTRATION - Nous pouvons supposer que α est un entier algébrique non réciproque (en effet, dans le cas contraire, nous avons déjà vu que $h(\alpha) \geq (\log 2)/D$. Avec les notations du lemme précédent, pour tout premier $p \geq 2D+3$, nous avons $\gamma_p/\overline{\gamma_p} \in \mathbb{Q}[\zeta_p]$, et $\gamma_p/\overline{\gamma_p} \notin \overline{\mathbb{Q}}^*_{\text{tors}}$, donc d'après le théorème d'Amoroso-Dvornicich 2.3,

$$h(\gamma_p/\overline{\gamma_p}) \geq \frac{\log 5}{12},$$

et d'après le lemme 2.6, nous avons de plus

$$h(\gamma_p/\overline{\gamma_p}) \leq \frac{\log |N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\gamma_p)|}{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}.$$

Or la norme $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\gamma_p)$ de γ_p est le produit des conjugués de γ_p, donc

$$\left| N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\gamma_p) \right| = \left| \prod_{j=1}^{p-1} F(\zeta_p^j) \right|,$$

et en notant $\alpha_1, \ldots, \alpha_D$ les conjugués de α, il vient

$$\begin{aligned} \left| N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\gamma_p) \right| &= \left| \prod_{j=1}^{p-1} \prod_{i=1}^{D} \left(\alpha_i - \zeta_p^j\right) \right| \\ &= \left| \prod_{i=1}^{D} \prod_{j=1}^{p-1} \left(\alpha_i - \zeta_p^j\right) \right|. \end{aligned}$$

D'autre part, nous avons $\prod_{j=1}^{p-1} \left(\mathrm{x} - \zeta_p^j\right) = \mathrm{x}^{p-1} + \mathrm{x}^{p-2} + \cdots + \mathrm{x} + 1$, d'où

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

D'où

$$\frac{D \log p + D(p-1)h(\alpha)}{p-1} \geq h(\gamma_p/\overline{\gamma_p}) \geq \frac{\log 5}{12},$$

et faisant tendre p vers l'infini, nous obtenons le résultat. ■

Chapitre 3

Théorème de Dobrowolski

Théorème 3.1 (Dobrowolski [Do]) *Il existe une constante $c > 0$ telle que, pour tout $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{tors}$ de degré D,*

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

Comme nous l'avons déjà dit, il suffit de montrer le théorème de Dobrowolski pour α un entier algébrique (*c.f.* remarque suivant la conjecture 1.1). De plus, grâce au théorème de finitude de Northcott 1.2, on pourra supposer D aussi grand que l'on veut. La preuve du théorème de Dobrowolski repose sur le lemme suivant, qui découle du petit théorème de Fermat :

I Lemme clef.

Lemme 3.1 (Lemme clef.) *Soient α un entier algébrique, et $T \in \mathbb{N}^*$. Soit $F \in \mathbb{Z}[\mathrm{x}]$ un polynôme qui s'annule en α avec un ordre de multiplicité supérieur ou égal à T.*

Alors, pour tout nombre premier p et toute place $v \in \mathcal{M}_{\mathbb{Q}(\alpha)}$ divisant p, nous avons

$$\mid F(\alpha^p) \mid_v \leq p^{-T}$$

Démonstration - Soit α un entier algébrique, et soit $P \in \mathbb{Z}[\mathrm{x}]$ le polynôme minimal de α sur $\mathbb{Z}$. Par le petit théorème de Fermat, nous avons :

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

pour tout premier $p \in \mathcal{P}$, et ,en particulier,

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

ainsi p divise $P(\alpha^p)$ dans $\mathcal{O}_{\mathbb{Q}(\alpha)} \supseteq \mathbb{Z}[\alpha]$, *i.e.* il existe $\beta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ tel que $P(\alpha^p) = p\beta$. Pour toute place $v \in M_{\mathbb{Q}(\alpha)}$, nous avons :

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

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

$$F(\mathrm{x}) = P(\mathrm{x})^T \times G(\mathrm{x}).$$

Puisque α est un entier algébrique, nous obtenons

$$\mid F(\alpha^p) \mid_v = \mid P(\alpha^p)^T \mid_v \mid G(\alpha^p) \mid_v \leq p^{-T} \mid G(\alpha^p) \mid_v \leq p^{-T},$$

car $G(\alpha^p) \in \mathcal{O}_k$. ■

Remarque : Si α n'est pas une racine de l'unité, α^p n'est pas un conjugué de α, en effet, dans le cas contraire, $h(\alpha^p) = ph(\alpha) = h(\alpha)$ et alors $h(\alpha) = 0$, d'où une contradiction d'après 1.1. De même, si p et q sont des nombres premiers distincts, α^p et α^q ne sont pas conjugués.

On va utiliser la formule du produit et le lemme clef précédent.
Soient α un entier algébrique, et $L, T \in \mathbb{N}^*$ deux paramètres. Soit $F \in \mathbb{Z}[\mathrm{x}]$ un polynôme de degré L qui s'annule en α avec un ordre de multiplicité supérieur ou égal à T. Pour tout premier p et toute place $v \in \mathcal{M}_{\mathbb{Q}(\alpha)}$, nous avons

$$\mid F(\alpha^p) \mid_v \leq \begin{cases} p^{-T} & \text{si } v \mid p \quad (\rightarrow \text{Lemme précédent}) \\ 1 & \text{si } v \nmid \infty \quad (\rightarrow F(\alpha^p) \text{ est un entier algébrique}) \\ \mathcal{L}(F) \max(1, \mid \alpha_v \mid)^{pL} & \text{si } v \mid \infty \quad (\rightarrow \text{Inégalité triangulaire}) \end{cases}$$

Si l'on peut construire un tel polynôme F tel que $F(\alpha^p) \neq 0$, alors la formule du produit, du théorème 1.3, fournit l'inégalité

$$1 = \prod_{v \in \mathbb{Q}(\alpha)} \mid F(\alpha^p) \mid_v \leq (p^{-T})^D \mathcal{L}(F)^D H(\alpha)^{pDL},$$

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

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

Par exemple, si on choisit $F := P$, le polynôme minimal de α sur $\mathbb{Z}$ (avec $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{\text{tors}}$), pour tout premier $p \in \mathcal{P}$, α^p n'est pas une racine du polynôme minimal P de α, d'après la remarque précédente, on a alors $L = D$, $T = 1$ et :

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

Problème : On peut avoir $\log \mathcal{L}(P) \gg D$, auquel cas il faut prendre $p \sim \exp D$ et la minoration obtenue est catastrophique. C'est pourquoi, il va falloir construire un polynôme F, de degré pas trop grand, de petite longueur (en fait de petite hauteur car $\mathcal{L}(F) \leq \deg(F)H(F)$), qui s'annule en α avec une grande multiplicité , et nous choisirons un premier $p \in \mathcal{P}$ de sorte que $F(\alpha^p) \neq 0$.

La construction de ce polynôme F est obtenue par l'utilisation d'un lemme classique de théorie de la transcendance, dont le principe repose sur le principe des tiroirs de Dirichlet. Nous allons alors en fait raisonner lègèrement différemment ; nous allons montrer par l'absurbe que si la hauteur de α est petite, alors F n'annule en "trop" de puissance α^p de α.

II Construction de la fonction auxiliaire.

Le théorème suivant va nous donner un polynôme (*i.e.* fonction auxiliaire) non nul de hauteur majorée par M, de degré majoré par L et qui va s'annuler en α avec une grande multiplicité (au moins T), où L, T et M seront des paramètres controlés.

Notations : Soient $L, T \in \mathbb{N}$, on note $E(\alpha, L, T)$ l'espace vectoriel des polynômes de degré $\leq L$ à coefficients dans $\mathbb{Q}$ nul en α avec multiplicité au moins T.

Pour $j \in \mathbb{N}^*$, $\partial_j := \frac{1}{j!}\frac{d^j}{dx^j}$.

Théorème 3.2 (Lemme de Siegel) *Soit $\alpha \in \overline{\mathbb{Q}}^*$, de degré D, et soient $L, T \in \mathbb{N}^*$ vérifiant $L > DT$. Alors il existe $F \in E(\alpha, L, T) \cap \mathbb{Z}[\mathrm{x}]$ tel que :*

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

Si l'on assimile $\mathbb{Q}[\mathrm{x}]_{\leq L}$ à $\mathbb{Q}^{L+1}$, alors $E(\alpha, L, T)$ est simplement un sous-espace vectoriel de $\mathbb{Q}^{L+1}$, et le polynôme F n'est rien d'autre qu'un élément du noyau d'une certaine matrice C. Notons que si F est associé au vecteur $\mathbf{a} \in \mathbb{Z}^{L+1}$ on a

$$H(F) = \|\mathbf{a}\|_\infty.$$

Rappelons avant tout quelques notations sur les normes matricielles :

Soient $T, L \in \mathbb{N}^*$ et $C \in M_{T,L}(k)$ une matrice à T lignes et L colonnes à coefficients dans un corps k. On $\|C\|_\infty$ la norme de la matrice C subordonnée à la norme $\|.\|_\infty$, *i.e.* :

$$\|C\|_\infty := \sup_{\mathbf{x} \in k^L \setminus \{0\}} \frac{\|C.\mathbf{x}\|_\infty}{\|\mathbf{x}\|_\infty} = \max_{i \in \{1,\ldots,T\}} \sum_{j=1}^{L} |c_{i,j}|.$$

où $\|\mathbf{x}\|_\infty := \max |x_j|$.

Lemme 3.2 *Soit $k = \mathbb{R}$ ou $\mathbb{C}$, et soient $L, T \in \mathbb{N}^*$. On considère $C := (c_{i,j}) \in M_{T,L+1}(k)$ et $M > 0$, $l > 0$ deux entiers.*

Si $l^{Tn_\infty} < (M+1)^{L+1}$, alors il existe un élément $\mathbf{a} \in \mathbb{Z}^{L+1}$ non nul tel que

$$\|\mathbf{a}\|_\infty \leq M \quad et \quad \|C.\mathbf{a}\|_\infty \leq \frac{\sqrt{n_\infty}}{l} M \|C\|_\infty$$

où $n_\infty := [k : \mathbb{R}]$.

DÉMONSTRATION - Nous allons prouver le lemme dans le cas où $k = \mathbb{R}$ (le cas $k = \mathbb{C}$ s'en déduisant alors aisément). Le principe de la preuve repose sur le principe des tiroirs de Dirichlet.

Soit f l'application linéaire associé à C :

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

Posons

$$A_i := \sum_{j=0}^{L} \min(0, c_{i,j}) \quad \text{et} \quad B_i := \sum_{j=0}^{L} \max(0, c_{i,j}),$$

en particulier $B_i - A_i \leq \|C\|_\infty$. De plus, si $\mathbf{x} \in (\mathbb{R}_+)^{L+1}$ on a :

$$A_i \|\mathbf{x}\|_\infty \leq \sum_{j=0}^{L} c_{i,j} x_j \leq B_i \|\mathbf{x}\|_\infty \quad i = 0, \ldots, T-1,$$

d'où :

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

On applique le principe des tiroirs de Dirichlet à ce dernier ensemble découpé en l^T pavés de i-ème côté de longueur $(B_i - A_i)/l$. Comme $l^T < (M+1)^{L+1}$, il existe deux $(L+1)$-uplets distincts $\mathbf{b}$ et $\mathbf{c}$ de $\mathbb{Z}^{L+1} \cap [0,M]^{L+1}$ tels que $f(\mathbf{b})$ et $f(\mathbf{c})$ soient dans le même pavé. En notant $\mathbf{a} := \mathbf{b} - \mathbf{c}$, on a :

$$\|\mathbf{a}\|_\infty \leq M$$

et

$$\|f(\mathbf{a})\|_\infty \leq M \frac{\max_{i \in \{0,\ldots,T-1\}}(B_i - A_i)}{l} \leq \frac{M}{l} \|C\|_\infty.$$

d'où le lemme. ■

DÉMONSTRATION - (Théorème 3.2)
Notons F_α le polyôme minimal de α sur $\mathbb{Z}$, en particulier $\deg(F_\alpha) = D$. Puisque $L > DT$, l'espace vectoriel $E(\alpha, L, T)$ contient F_α^T, notamment il est non vide. Si l'on associe $\mathbb{Q}[\mathrm{x}]_{\leq L}$ à $\mathbb{Q}^{L+1}$ nous avons

$$E(\alpha, L, T) = \{\mathbf{a} \in \mathbb{Q}^{L+1} \mid C \cdot \mathbf{a} = \mathbf{0}\}$$

où C est la matrice définie, pour $i \in \{0, \ldots, T-1\}$ et $j \in \{0, L\}$ par

$$c_{i,j} := \begin{pmatrix} j \\ i \end{pmatrix} \alpha^{j-i}.$$

En effet si F est un polynôme :

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

nous avons pour tout $i \in \{0, \ldots, T-1\}$,

$$(\partial_i F)(\alpha) = \sum_{j=i}^{L} \binom{j}{i} \alpha^{j-i} a_j = \sum_{j=i}^{L} c_{i,j} a_j = (C \cdot \mathbf{a})_i \,,$$

de plus $H(F) = \|\mathbf{a}\|_\infty$. Notre but est donc de trouver un élément $\mathbf{a} \in \mathbb{Q}^{L+1}$ tel que $\|\mathbf{a}\|_\infty \leq M$ et $C \cdot \mathbf{a} = \mathbf{0}$.
Soient $M \geq 1$ et l deux entiers tels que $M^{L+1} \leq l^{Tn_\infty} < (M+1)^{L+1}$ (on précisera ces entiers plus tard[1]). D'après le lemme 3.2, il existe alors $\mathbf{a} = (a_0, \ldots, a_L) \in \mathbb{Z}^{L+1} \setminus \{(0, \ldots, 0)\}$ tel que

$$H(F) = \|\mathbf{a}\|_\infty \leq M \quad \text{et} \quad \max_{i=0\ldots T-1} |(\partial_i F)(\alpha)| = \|C \cdot \mathbf{a}\|_\infty \leq \frac{\sqrt{n_\infty}}{l} M \|C\|_\infty, \quad (3.1)$$

où F est le polynôme associé à $\mathbf{a}$. Par l'absurde supposons qu'il existe $i_0 \in \{0, \ldots, T-1\}$ tel que $(\partial_{i_0} F)(\alpha) \neq 0$, la formule du produit nous donne alors

$$1 = \prod_{v \in \mathcal{M}_{\mathbb{Q}(\alpha)}} |(\partial_{i_0} F)(\alpha)|_v^{n_v}. \quad (3.2)$$

Soit v une place de $\mathbb{Q}(\alpha)$, majorons $|(\partial_{i_0} F)(\alpha)|_v$.
• Si v est archimédienne, pour tout i nous avons :

$$\begin{aligned} \sum_{j=0}^{L} |c_{i,j}|_v &= \sum_{j=0}^{L} \binom{j}{i} |\alpha|_v^{j-i} \leq \sum_{j=0}^{L} \binom{j}{i} \max(1, |\alpha|_v)^L \\ &\leq \binom{L+1}{i+1} \max(1, |\alpha|_v)^L \leq (L+1)^{i+1} \max(1, |\alpha|_v)^L. \end{aligned}$$

[1] un tel l existe bien puisque $L + 1 > DT \geq n_\infty T$.

en particulier $\|C\|_\infty \leq (L+1)^T \max(1, |\alpha|_v)^L$. On déduit de ceci et de (3.1)

$$|(\partial_{i_0} F)(\alpha)|_v = |\sum_{j=0}^{L} c_{i_0,j} a_j|_v \leq \sum_{j=0}^{L} |c_{i_0,j}|_v \|\mathbf{a}\|_\infty \leq M(L+1)^{i_0+1} \max(1, |\alpha|_v)^L$$

et (dans le cas où v est associé au plongement identité)

$$|(\partial_{i_0} F)(\alpha)| \leq \frac{\sqrt{n_\infty}}{l} M(L+1)^T \max(1, |\alpha|_v)^L$$

• Si $v \nmid \infty$, alors $\left|\binom{j}{i_0}\right|_v \leq 0$ et $|a_j|_v \leq 0$ pour tout j, car ce sont des entiers, ainsi,

$$|(\partial_{i_0} F)(\alpha)|_v \leq \max(1, |\alpha|_v)^L.$$

En reportant tout ceci dans (3.2) on trouve

$$1 \leq \left(\frac{\sqrt{n_\infty}}{l}\right)^{n_\infty} \cdot \left(M(L+1)^T\right)^D H(\alpha)^{LD}$$

De part de notre choix de l on en déduit :

$$M^{L+1} \leq l^{Tn_\infty} \leq 2^T M^{TD} (L+1)^{T^2 D} H(\alpha)^{LTD}$$

d'où

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

Il suffit alors de poser

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

pour arriver à une contradiction, d'où le théorème. ■

III Démonstration du théorème de Dobrowolski.

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

• *Réduction.*

Montrons que l'on peut se ramener au cas où

$$\forall p \in \mathcal{P}, [\mathbb{Q}(\alpha^p) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

Soit $p \in \mathcal{P}$ un premier tel que $[\mathbb{Q}(\alpha^p) : \mathbb{Q}] < D$, *i.e.* $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^p)] > 1$.
Le polynôme minimal de α sur $\mathbb{Q}(\alpha^p)$ divise $\mathrm{x}^p - \alpha^p$, en particulier les conjugués de

α sur $\mathbb{Q}(\alpha^p)$ sont de la forme $\zeta\alpha$, où ζ est une racine p-ième de l'unité. Considérons $\beta := N_{\mathbb{Q}(\alpha^p)}^{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Q}(\alpha^p)$, il existe une racine p-ième de l'unité ζ', telle que $\beta = \zeta'\alpha^d$, où $d := [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^p)] > 1$. On a :

$$Dh(\alpha) = \frac{D}{d}h(\alpha^d) = \frac{D}{d}h(\zeta'\alpha^d) = \frac{D}{d}h(\beta) \geq [\mathbb{Q}(\beta) : \mathbb{Q}]h(\beta),$$

Puisque $[\mathbb{Q}(\beta) : \mathbb{Q}] < D$, et puisque la fonction $D \mapsto \left(\frac{\log\log D}{\log D}\right)^3$ est décroissante, une simple récurrence sur D donne alors

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

- *Choix des paramètres*

On pose

$$\begin{cases} T & := & \left[c_0\dfrac{\log D}{\log\log D}\right] \quad c_0 \geq 10 \\ L & := & DT^2 \\ N & := & 6T^2\log T. \end{cases}$$

Comme $x/\log x$ est toujours minoré par e, nous avons en particulier $T \geq [10e] = 27$, et

$$\log(L+1) \leq 4\log c_0 \log D \quad \text{et} \quad \log N < 3\log T. \tag{3.3}$$

Nous supposerons dans la suite par l'absurde :

$$h(\alpha) < \frac{\log(L+1)}{NL}. \tag{3.4}$$

- *Construction d'une fonction auxiliaire*

Le lemme de Siegel 3.2 nous donne un polynôme F non nul de degré au plus L à coefficients entiers nul en α avec multiplicité au moins T vérifiant de plus :

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

On en déduit la majoration

$$\log\mathcal{L}(F) \leq \log(L+1) + \log H(F) \leq 4\log(L+1). \tag{3.5}$$

En effet, nous avons $L \geq 2DT$, en particulier $1/(L+1-DT) \leq 2/L$ d'où

$$H(F) \leq 1 + 2(L+1)^2H(\alpha)^{2DT}.$$

Si $2(L+1)^2 H(\alpha)^{2DT} \leq 1$ on obtient $\log H(F) \leq \log 2 \leq \log(L+1)$ et c'est fini, sinon

$$\log H(F) \leq \log 4 + 2\log(L+1) + 2DTh(\alpha).$$

Par hypothèse on a $h(\alpha) \leq \frac{\log(L+1)}{NL} \leq \frac{\log(L+1)}{6DT}$ d'où

$$\log H(F) \leq 3\log(L+1).$$

d'où le résultat.

• *Extrapolation.*

Montrons que F est nul en α^p pour tout $p \in [\log D, N]$. Supposons qu'il existe un tel $p \in [\log D, N]$, tel que $F(\alpha^p) \neq 0$, en appliquant la formule du produit, nous obtenons

$$1 = \prod_{v \in \mathcal{M}_{\mathbb{Q}(\alpha)}} |F(\alpha^p)|_v^{n_v}.$$

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

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

On en déduit :

$$1 \leq p^{-TD}\mathcal{L}(F)^D H(\alpha)^{DpL},$$

soit, en passant au log

$$T\log\log D \leq T\log p \leq \log \mathcal{L}(F) + pLh(\alpha).$$

En utilisant (3.4), (3.5), (3.3) et $T \geq \frac{c_0}{2}\frac{\log D}{\log\log D}$, on en déduit

$$\frac{c_0}{2}\log D \leq (16\log c_0 + 1)\log D,$$

contradiction, pour $c_0 \gg 0$, donc F est nul en α^p pour tout $p \in [\log D, N]$.

• *Lemme de zéros*

Par hypothèse nous avons

$$\forall p \in \mathcal{P},\ [\mathbb{Q}(\alpha^p) : \mathbb{Q}] = D,$$

en particulier l'ensemble

$$\Sigma := \{\sigma(\alpha^p), \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), p \in \mathcal{P} \cap [\log D, N]\}$$

contient donc $D \times \big(\pi(N) - \pi(\log D)\big)$ éléments, en effet, comme $\alpha \notin \overline{\mathbb{Q}}^*_{\text{tors}}$, α^p et α^q ne sont pas conjugués si $p \neq q$ (*c.f.* remarque p. 46).

Comme $\log D = \circ(N)$, le théorème des nombres premiers nous dit que

$$\pi(N) - \pi(\log D) \geq \frac{1}{2}\frac{N}{\log N} \text{ pour } D \gg 0$$

donc :

$$\#\Sigma \geq \frac{1}{2}D\frac{N}{\log N} > \frac{2}{2}DT^2 = L = \deg(F), \text{ pour } D \gg 0$$

De plus nous venons de voir que F s'annulait sur Σ, d'où une contradiction ; l'hypothèse (3.4) est donc fausse, c'est-à-dire :

$$h(\alpha) \geq \frac{\log(L+1)}{NL} \geq \frac{\log D}{6DT^4 \log T}.$$

donc

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

■

Remarque : Nous n'avons montré ici que l'existence d'une telle constante, néanmoins il est possible de l'expliciter, la meilleure connue à ce jour est $1/4$ (*c.f.* [Vo]).

Chapitre 4

Hauteurs en dimension supérieure.

Comme nous l'avons vu au chapitre 1, il y a plusieurs façons de définir la hauteur d'un nombre algébrique α :

- soit en utilisant la mesure de Malher de son polyôme minimal F sur $\mathbb{Z}$:

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

- soit en regardant ses conjugués et les différentes places d'un corps k le contenant :

$$h(\alpha) := \frac{1}{[k : \mathbb{Q}]} \sum_{v \in \mathcal{M}_k} n_v \log(\max\{1, |\alpha|_v\}),$$

On peut ainsi imaginer plusieurs façons de généraliser la notion de hauteur en dimension supérieure :

- soit considérer la hauteur de points de $\overline{\mathbb{Q}}^n$,
- soit considérer la hauteur de l'ensemble des zéros d'un polynôme ou, de façon générale, la hauteur de variétés algébriques.

I Hauteur et minimum essentiel.

I.1 Minimum essentiel.

Notation : Soit $n \in \mathbb{N}^*$, on note $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ ou plus simplement $\mathbb{G}_m^n$ et on appelle groupe multiplicatif l'ensemble $(\overline{\mathbb{Q}}^*)^n$.

Nous plongerons $\mathbb{G}_m^n$ de façon naturelle dans $\mathbb{P}^n(\overline{\mathbb{Q}})$: $(a_1, \ldots, a_n) \mapsto (1 : a_1 : \ldots : a_n)$.

Proposition 4.1 *Soit $v \in \mathcal{M}_k$ on a :*

$$n_v = [k_\nu : \mathbb{Q}_v],$$

où k_ν désigne le complété de k pour la topologie induite par la valeur absolue ν.

DÉMONSTRATION - Admis. ■

Définition 4.1 *Soit $P = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$, et soit k un corps de nombres contenant $x_0, \ldots, x_n$. On définit la hauteur de Weil (logarithmique) de P comme :*

$$h(P) := \sum_{\nu \in \mathcal{M}_k} \frac{[k_\nu : \mathbb{Q}_v]}{[k : \mathbb{Q}]} \log \max\{|x_0|_\nu, |x_1|_\nu, \ldots, |x_n|_\nu\},$$

Remarque : Cette définition a bien un sens (elle ne dépend pas du représentant choisi) ; en effet, en utilisant la formule du produit 1.3, on voit que le membre de droite ne change pas si l'on remplace P par $a \cdot P$ où $a \in \overline{\mathbb{Q}}^*$.

On définit alors la hauteur dans $\mathbb{G}_m^n$ par restriction de $\mathbb{P}^n(\overline{\mathbb{Q}})$ à $\mathbb{G}_m^n$:

$$h(\alpha_1, \ldots, \alpha_n) := \sum_{\nu \in \mathcal{M}_k} \frac{[k_\nu : \mathbb{Q}_v]}{[k : \mathbb{Q}]} \log \max\{1, |\alpha_1|_\nu, \ldots, |\alpha_n|_\nu\}.$$

Bien sûr, cette définition coïncide bien en dimension 1 avec la hauteur vu au chapitre 1.

Nous donnons maintenant une première notion de hauteur sur une variété algébrique. Soit V une variété algébrique affine (*c.f.* annexe) et soit ε un nombre réel, on note

$$V(\varepsilon) := \left\{\alpha \in V(\overline{\mathbb{Q}}) \mid h(\boldsymbol{\alpha}) \leq \varepsilon\right\}.$$

Définition 4.2 *Soit V une variété algébrique affine, on appelle minimum essentiel de V le réel :*

$$\hat{\mu}_{ess}(V) := \inf\left\{\varepsilon > 0 \mid \overline{V(\varepsilon)}^{Zar} = V\right\},$$

où $\overline{V(\varepsilon)}^{Zar}$ désigne l'adhérence de Zariski de $V(\varepsilon)$.

Remarque : En dimension 2 (V est alors une courbe) on a :

$$\hat{\mu}_{\text{ess}}(V) = \inf\left\{\varepsilon > 0 \mid \#V(\varepsilon) = \infty\right\}.$$

I.2 Hauteur normalisée.

Nous avons montré au chapitre 1 (*c.f.* théorème 1.1) l'égalité :

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

pour tout polynôme $F \in \mathbb{C}[\mathrm{x}]$, $F \neq 0$.

Ceci nous permet de généraliser de façon naturelle la mesure de Mahler d'un polynôme à plusieurs variables :

Définition 4.3 *Soit $F \in \mathbb{C}[\mathrm{x}_1, \ldots, \mathrm{x}_n]$; on définit sa mesure de Mahler en posant $M(0) = 0$ et si $F \neq 0$:*

$$\log M(F) = \frac{1}{(2\pi)^n} \int_0^{2\pi} \cdots \int_0^{2\pi} \log |F(e^{i\theta_1}, \ldots, e^{i\theta_n})| d\theta_1 \ldots d\theta_n.$$

On peut maintenant définir la hauteur normalisée d'une hypersurface :

Définition 4.4 *Soit V une hypersurface définie par le polynôme $F \in \overline{\mathbb{Q}}[\mathrm{x}_1, \ldots, \mathrm{x}_n]$ (F étant réduit, i. e. sans facteur carré), on définit la hauteur normalisée de V comme*

$$\hat{h}(V) = h_0(F).$$

où h_0 est défini comme en dimension 1.

Rappel : Si F est à coefficient dans un corps de nombres k on a : (*c.f.* 1.18)

$$h_0(F) = \sum_{\nu \in \mathcal{M}_k} \frac{[k_\nu : \mathbb{Q}_\nu]}{[k : \mathbb{Q}]} \log \big(M_\nu(F)\big),$$

où $M_\nu(F) = \begin{cases} \max\{|\operatorname{coeff}(f)|_\nu\} & \text{si } \nu \nmid \infty \\ M(\sigma F) & \text{si } \nu | \infty \end{cases}$

Remarque : Si $F \in \mathbb{Z}[\mathrm{x}_1, \ldots, \mathrm{x}_n]$, on peut voir que $h_0(F) = \log M(F)$.

I.3 Etude en dimension 1.

Il peut être intéressant de regarder, en dimension 1, ce que valent hauteur normalisée et minimum essentiel, on posera ici $k = \mathbb{Q}$.

Soient $\alpha \in \overline{\mathbb{Q}}$ et F son polynôme minimal sur $\mathbb{Z}$, on pose :

$$V := \big\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\big\} = Z\big((F)\big).$$

On a :

- Si $h(\alpha) \leq \varepsilon$ alors $V(\varepsilon) = V$, si $h(\alpha) > \varepsilon$ alors $V(\varepsilon) = \emptyset$, d'où $\hat{\mu}_{\mathrm{ess}}(V) = h(\alpha)$.

• De plus $\hat{h}(V) = \log M(F) = D \cdot h(\alpha)$, où $D := [\mathbb{Q}(\alpha) : \mathbb{Q}]$, d'où :

$$\hat{h}(V) = D \cdot \hat{\mu}_{\text{ess}}(V).$$

En dimension 2 on peut montrer, si $\mathcal{C}$ est une courbe :

$$\frac{\hat{h}(V)}{2\deg(\mathcal{C})} \leq \hat{\mu}_{\text{ess}}(\mathcal{C}) \leq \frac{\hat{h}(\mathcal{C})}{\deg(\mathcal{C})}.$$

On peut généraliser ceci en dimension supérieure, c'est un cas particulier d'un résultat montré par S. Zhang, on le verra à la section III.

II Premiers résultats en dimension supérieure.

Nous allons voir dans quelle mesure il est possible généraliser les résultats obtenus en dimension 1. Tout d'abord nous avons l'analogue du théorème de finitude de Northcott 1.2 :

Théorème 4.1 (Northcott) *Pour tout nombres $B, D \geq 0$, l'ensemble*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid h(P) \leq B \text{ et } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

est fini. En particulier, pour tout corps de nombres fixé k, l'ensemble

$$\{P \in \mathbb{P}^n(k) \mid h(P) \leq B\}$$

est fini.

Démonstration - Choisissons des coordonnées homogènes pour $P = (x_0 : \ldots : x_n)$ telles qu'une coordonnée soit égale à 1. Alors pour toute valeur absolue ν et tout indice i on a :

$$\max\{|x_0|_\nu, \ldots, |x_n|_\nu\} \geq \max\{|x_i|_\nu, 1\}.$$

On obtient alors :

$$h(P) \geq h(x_i) \qquad \text{pour } i = 1, \ldots, n.$$

De plus, il est clair que $\mathbb{Q}(P) \supset \mathbb{Q}(x_i)$. Il suffit donc de montrer que, pour tout $1 \leq d \leq D$, l'ensemble

$$\{\alpha \in \overline{\mathbb{Q}} \mid h(\alpha) \leq B \text{ et } [\mathbb{Q}(\alpha) : \mathbb{Q}] = d\}$$

est fini, ce qui découle du théorème 1.2. ■

Nous conservons également un certain nombres de propriétés :

Propriétés 4.1 *Soient $\boldsymbol{\alpha}, \boldsymbol{\beta} \in k^n$ et $l \in \mathbb{N}$, on a :*

1. $h(\boldsymbol{\alpha}\boldsymbol{\beta}) \leq h(\boldsymbol{\alpha}) + h(\boldsymbol{\beta})$
2. $h(\boldsymbol{\alpha}^l) = l \cdot h(\boldsymbol{\alpha})$
3. $h(\boldsymbol{\alpha}) \geq 0$
4. *Si* $\boldsymbol{\alpha} \in \mathbb{G}_m^n$, $h(\boldsymbol{\alpha}) = 0 \Longleftrightarrow \boldsymbol{\alpha} \in (\mathbb{G}_m^n)_{tors}$

DÉMONSTRATION - Les points 1. à 3. se traitent comme dans 1.6, montrons le 4. Si $\boldsymbol{\alpha} \in (\mathbb{G}_m^n)_{\text{tors}}$, alors par définition il existe $r \in \mathbb{N}^*$ tel que :

$$\boldsymbol{\alpha}^r := (\alpha_1^r, \ldots, \alpha_n^r) = (1, \ldots, 1),$$

d'où $h(\boldsymbol{\alpha}^r) = r \cdot h(\boldsymbol{\alpha}) = 0$, donc $h(\boldsymbol{\alpha}) = 0$.
Réciproquement supposons $h(\boldsymbol{\alpha}) = 0$. Soit $\varepsilon > 0$ et $D := [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]$, d'après le théorème 4.1, l'ensemble :

$$\left\{\boldsymbol{\beta} \in \mathbb{G}_m^n \mid h(\boldsymbol{\beta}) \leq \varepsilon,\ [\mathbb{Q}(\boldsymbol{\beta}) : \mathbb{Q}]\right\}$$

est fini. Comme $\boldsymbol{\alpha}^r$ est dans cet ensemble pour tout entier r, il existe $r \in \mathbb{N}^*$, tel que $\boldsymbol{\alpha}^{r+1} = \boldsymbol{\alpha}$, donc $\boldsymbol{\alpha}^r = (1, \ldots, 1)$ car $\boldsymbol{\alpha} \in \mathbb{G}_m^n$.

■

Une question qui alors vient naturellement est de savoir quelles sont les variétés de hauteur nulle. Ceci est un problème délicat, néanmoins le cas des hypersurfaces est plus simple ; en particulier, Boyd, Lawton et Smyth ont montré indépendamment (voir [Boy], [La] et [Sm]) le résultat suivant :

Proposition 4.2 *La mesure de Malher d'un polynôme irréductible*

$$F \in \mathbb{Z}[\mathbf{x}], \quad F(\mathbf{x}) \neq \pm \mathrm{x}_j,$$

est égale à 1 si et seulement si F est un polynôme cyclotomique généralisé, c'est-à-dire un polynôme irréductible de la forme

$$\mathbf{x}^{\boldsymbol{\lambda}} \varphi(\mathbf{x}^{\boldsymbol{\mu}}),$$

où $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbb{Z}^n$ sont deux multi-indices et $\varphi \in \mathbb{Z}[\mathrm{x}]$ un polynôme cyclotomique.

III Théorème de Zhang.

III.1 Enoncé.

Minimum essentiel et hauteur normalisée sont très liés comme nous l'avons vu à la section I, plus précisément nous avons :

Théorème 4.2 *Soit V une hypersurface algébrique propre géométriquement irréductible de $\mathbb{G}_m^n$, alors :*

$$\frac{\hat{h}(V)}{n\deg(V)} \leq \hat{\mu}_{ess}(V) \leq \frac{\hat{h}(V)}{\deg(V)}.$$

Démonstration - Nous montrerons ce résultat dans le cas où $n = 2$, rappelons que pour $n = 1$ nous avons (*c.f.* I.3) :

$$\hat{h}(V) = \deg(V) \cdot \hat{\mu}_{\text{ess}}(V).$$

On peut supposer $k = \mathbb{Q}$, quitte à remplacer V par

$$\{\sigma(V) \mid \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}.$$

• Montrons dans un premier temps que $\hat{\mu}_{\text{ess}}(V) \leq \frac{\hat{h}(V)}{\deg V}$ (pour $n = 2$).
Soit $P \in \mathbb{Q}[X, Y]$ irréductible tel que $V = Z\big((P)\big)$, on note

$$\begin{cases} D_X := \deg_X P \\ D_Y := \deg_Y P. \end{cases}$$

On peut supposer $P \in \mathbb{Z}[X, Y]$ car $\hat{h}(V) = h_0(P)$, on a alors

$$\hat{h}(V) = \log M(P) = \frac{1}{4\pi^2} \int_0^{2\pi} \int_0^{2\pi} \log |P(e^{i\theta_1}, e^{i\theta_1})| d\theta_1 d\theta_2.$$

Soient $y \in \mathbb{C}$ "générique" (*i.e.* tel que le coefficient du monôme X^{D_X} soit non nul) et l un nombre premier, on note $\omega_l := \exp(2i\pi/l)$; le polynôme $P(X, y) \in \mathbb{Z}[y][X]$ est de la forme :

$$P(X, y) = Q(y) \prod_{j=1}^{D_X} \big(X - \alpha_j(y)\big).$$

On s'intéresse à $\prod_{i=1}^{l-1} P(\omega_l^i, y)$ (on spécialise X) :

$$\begin{aligned} \prod_{i=1}^{l-1} P(\omega_l^i, y) &= Q(y)^{l-1} \prod_{i=1}^{l-1} \prod_{j=1}^{D_X} \big(\omega_i^l - \alpha_j(y)\big) \\ &= \pm Q(y)^{l-1} \prod_{j=1}^{D_X} \prod_{i=1}^{l-1} \big(\alpha_j(y) - \omega_i^l\big) \\ &= \pm Q(y)^{l-1} \prod_{j=1}^{D_X} \big(1 + \alpha_j(y) + \ldots + \alpha_j(y)^{l-1}\big) \end{aligned}$$

d'où

$$\begin{aligned}\prod_{i=1}^{l-1} P(\omega_l^i, y) &\leq Q(y)^{l-1} \prod_{j=1}^{D_X} \Big(l \cdot \max\{1, |\alpha_j(y)|\}^{l-1}\Big) \\ &\leq l^{D_X} M_X\big(P(X,y)\big)^{l-1}\end{aligned}$$

d'où

$$\sum_{i=1}^{l-1} \log|P(\omega_l^i, y)| \leq D_X \log l + \frac{l-1}{2\pi} \int_0^{2\pi} \log|P(e^{i\theta_1}, y)| d\theta_1.$$

Remarquons que, le coefficient du monôme X^{D_X} dans $P(X,y)$, (*i.e.* $Q(y)$) ne s'annulant que pour un nombre fini de $y \in \mathbb{C}$, l'inégalité ci-dessus est vraie presque partout sur le cercle unité, on a donc :

$$\begin{aligned}⨍_0^{2\pi} \log\Big(|\prod_{r=1}^{l-1} P(\omega_l^r, e^{i\theta})|\Big) d\theta &= ⨍_0^{2\pi} \sum_{r=1}^{l-1} \log|P(\omega_l^r, e^{i\theta})| d\theta \\ &\leq D_X \log l + \frac{l-1}{(2\pi)^2} \int_0^{2\pi}\int_0^{2\pi} \log|P(e^{i\theta_1}, e^{i\theta_2})| d\theta_1 d\theta_2 \\ &= D_X \log l + (l-1) \log M(P)\end{aligned}$$

Soit l tel que $\deg P(\omega_l^i, Y) = D_Y$ pour tout $i \in \mathbb{N}$, on pose :

$$P_l(Y) := \prod_{i=1}^{l-1} P(\omega_l^i, Y),$$

alors :

$$\log M(P_l) \leq D_X \log l + (l-1) \log M(P),$$

d'autre part :

$$\log M(P_l) = \sum_{\alpha | P_l(\alpha)=0} h(\alpha) \geq \deg(P_l) h(\alpha_l),$$

où α_l est une certaine racine de P_l (le polynôme P_l n'étant a priori pas irréductible, ses racines n'ont pas nécessairement les mêmes hauteurs).
De plus on a $\deg(P_l) = (l-1)D_Y$, donc :

$$(l-1) D_Y h(\alpha_l) \leq D_X \log l + (l-1) \log M(P).$$

Soit $\varepsilon > 0$, pour tout $i \in \mathbb{N}$ on a :

$$\begin{aligned}h(\omega_l^i, \alpha_l) &\leq h(\omega_l^i) + h(\alpha_l) \\ &\leq h(\alpha_l) \\ &\leq \frac{D_X \log l}{D_Y (l-1)} + \frac{\log M(P)}{D_Y} \\ &\leq \frac{\log M(P)}{D_Y} + \varepsilon\end{aligned}$$

dès que $l \geq l_0(\varepsilon)$, car $\frac{\log l}{l-1} \xrightarrow[l\to\infty]{} 0$.

Or, pour tout premier $l \geq l_0(\varepsilon)$, par définition de P_l, il existe $i \in \{0, \ldots, l-1\}$ tel que $(\omega_l^i, \alpha_l) \in V$ (*i.e.* $P(\omega_l^i, \alpha_l) = 0$).

On a donc montré :

$$\forall \varepsilon > 0,\ \#\Big\{(\omega, \alpha) \in V \mid \omega \in \overline{\mathbb{Q}}^*_{tors},\ h(\alpha) \leq \frac{\log M(P)}{\deg_Y(P)} + \varepsilon\Big\} = \infty.$$

en particulier $\hat{\mu}_{\text{ess}}(V) \leq \frac{\log M(P)}{D_Y}$, car $h(\omega, \alpha) \leq h(\alpha)$.

Ceci ne nous permet pas encore de conclure, c'est pourquoi nous allons appliquer ceci à une autre hypersurface ; posons

$$Q(X, Y) := P(XY, Y) \text{ et } W := Z\big((Q)\big),$$

on a :

$$\begin{cases} \deg_Y Q = \deg P \\ P(\omega\alpha, \alpha) = 0 \Leftrightarrow Q(\omega, \alpha) = 0 \\ M(P) = M(Q) \text{ (changement de variable dans l'intégrale).} \end{cases}$$

On obtient alors, en appliquant ce qui précède à W :

$$\forall \varepsilon > 0,\ \#\big\{(\omega, \alpha) \in W \mid \omega \in \overline{\mathbb{Q}}^*_{tors},\ h(\alpha) \leq \frac{\log M(Q)}{\deg_Y(Q)} + \varepsilon\big\} = \infty,$$

autrement dit :

$$\forall \varepsilon > 0,\ \#\big\{(\omega\alpha, \alpha) \in V \mid \omega \in \overline{\mathbb{Q}}^*_{tors},\ h(\alpha) \leq \frac{\log M(P)}{\deg(P)} + \varepsilon\big\} = \infty,$$

or $h(\omega\alpha, \alpha) = h(\alpha)$, ω étant racine de l'unité, car :

$$\forall v \in \mathcal{M}_k,\ \max\{1, |\omega\alpha|_v, |\alpha|_v\} = \max\{1, |\alpha|_v\},$$

donc

$$\hat{\mu}_{\text{ess}}(V) \leq \frac{\log M(P)}{\deg P} = \frac{\hat{h}(V)}{\deg(V)},$$

ce qui termine la première partie du du théorème. (On peut généraliser ce résultat en dimension n en spécialisant $n-1$ variables.) ■

Avant de montrer la seconde inégalité : $\frac{\hat{h}(V)}{2\deg(V)} \leq \hat{\mu}_{\text{ess}}(V)$, nous allons donner d'autres résultats, en particulier nous aurons besoin d'un lemme de Siegel plus général.

III.2 Lemme de Siegel sur les variétés.

Rappelons d'abord le théorème 3.2 :

Lemme de Siegel

Soit $\alpha \in \overline{\mathbb{Q}}^*$, de degré D, et soient $L, T \in \mathbb{N}^*$ vérifiant $L > DT$.
Alors il existe $F \in \mathbb{Z}[\mathrm{x}]$ tel que :

1. $\deg(F) \leq L$, *et α est une racine de F de multiplicité au moins T.*
2. $\log \max\{|coeff(F)|\} \leq \delta\Big((T+1)\log(L+1) + Lh(\alpha)\Big)$

où $\delta = \frac{DT}{L+1-DT}$.

Remarque : Si on pose :

$$E(\alpha, L, T) := \big\{P \in \mathbb{Q}[\mathrm{x}]_{\leq L} \mid P \text{ nul en } \alpha \text{ avec multiplicité } \geq T\big\},$$

on peut voir que δ appparait comme le quotient :

$$\delta = \frac{\dim \mathbb{Q}[\mathrm{x}]_{\leq L} - \dim E(\alpha, L, T)}{\dim E(\alpha, L, T)},$$

car $\dim_{\mathbb{Q}} E(\alpha, L, T) = L + 1 - DT$ et $\dim_{\mathbb{Q}} \mathbb{Q}[\mathrm{x}]_{\leq L} = L + 1$.

On a alors une généralisation naturelle, moyennant quelques définitions :
Notation : Soit S une partie finie de $\mathbb{G}_m^n$, on pose :

$$\begin{aligned} \omega_{\mathbb{Q}}(S) &:= \min\big\{\deg(P) \mid P \in \mathbb{Q}[\mathbf{x}]^*, P(\alpha) = 0, \forall \alpha \in S\big\}, \\ E(S, L, T) &:= \big\{P \in \mathbb{Q}[\mathbf{x}]_{\leq L} \mid P \text{ nul en } \boldsymbol{\alpha} \text{ avec multiplicité } \geq T,\ \forall \boldsymbol{\alpha} \in S\big\}. \end{aligned}$$

Remarque : On dira que $\boldsymbol{\alpha}$ est racine de F avec **multiplicité** $T \in \mathbb{N}^*$ si

$$\forall\ |\boldsymbol{\lambda}| < T,\ \frac{\partial^{\boldsymbol{\lambda}} F}{\partial \mathbf{x}^{\boldsymbol{\lambda}}}(\boldsymbol{\alpha}) = 0.$$

Propriétés 4.2 *Avec les mêmes notations on a :*

- $\dim E(S, L, T) \geq \binom{L - T\omega_{\mathbb{Q}}(S) + n}{n}$.
- *si $S := \{\boldsymbol{\alpha}\}$ et $D := [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]$ alors $1 \leq \omega_{\mathbb{Q}}(S) \leq nD^{1/n}$.*

Démonstration -

– Soit $F \in \mathbb{Q}[\mathbf{x}]_{\leq \omega_{\mathbb{Q}}(S)}$ tel que $F(\boldsymbol{\alpha}) = 0$ pour tout $\boldsymbol{\alpha} \in S$, on a :

$$\forall H \in \mathbb{Q}[\mathbf{x}], \deg H \leq L - T\omega_{\mathbb{Q}}(S) \Rightarrow F^T H \in E(S, L, T),$$

de plus $\dim \mathbb{Q}[\mathbf{x}]_{\leq L - T\omega_{\mathbb{Q}}(S)} = \binom{L - T\omega_{\mathbb{Q}}(S)+n}{n}$ d'où le résultat.

– Posons $\omega := [nD^{1/n}]$ et considérons l'application linéaire :

$$\begin{array}{ccc} \mathbb{Q}[\mathbf{x}]_{\leq \omega} & \longrightarrow & \mathbb{Q}(\boldsymbol{\alpha}) \\ P & \longmapsto & P(\boldsymbol{\alpha}). \end{array}$$

Remarquons que $\dim \mathbb{Q}[\mathbf{x}]_{\leq \omega} = \binom{\omega+n}{n} \geq n^{-n}(\omega+1)^n$. Or $n^{-n}(\omega+1)^n > D$, cette application n'est donc pas injective, *i.e.* il existe $P \in \mathbb{Q}[\mathbf{x}]_{\leq \omega} \setminus \{0\}$ tel que $P(\boldsymbol{\alpha}) = 0$, donc $\omega_{\mathbb{Q}}(\boldsymbol{\alpha}) \leq \omega \leq nD^{1/n}$.

■

On peut maintenant énoncer un lemme de Siegel sur les variétés :

Proposition 4.3 *Soit $V \subseteq \mathbb{G}_m^n$ une variété $\mathbb{Q}$-irréductible propre, et soient $L, T \in \mathbb{N}^*$. Si $E(V, L, T) \neq \{0\}$, alors il existe $F \in E(V, L, T) \cap \mathbb{Z}[\mathbf{x}] \setminus \{0\}$ tel que :*

$$\log \max\{|\operatorname{coeff}(F)|\} \leq \delta\Big((T+n)\log(L+1) + L\hat{\mu}_{ess}(V)\Big),$$

où $\delta = \frac{\dim \mathbb{Q}[\mathbf{x}]_{\leq L} - \dim E(V,L,T)}{\dim E(V,L,T)}$.

Remarque : On étend ici bien sûr naturellement la définition de $E(V, L, T)$ au cas où V est infini.

DÉMONSTRATION - On ne donne ici qu'une idée de la preuve.

• On montre dans un premier temps que $E(V, L, T) = E(S_{d_0}, L, T)$ pour une certaine partie finie S_{d_0} de $\mathbb{G}_m^n$.

Soit $\varepsilon > 0$, pour tout $d \in \mathbb{N}$ on pose :

$$S_d := \big\{\boldsymbol{\alpha} \in V \mid [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}] \leq d,\ h(\boldsymbol{\alpha}) \leq \hat{\mu}_{\text{ess}}(V) + \varepsilon\big\}$$

D'après le théorème 4.1, celui-ci est fini, de plus, il est stable sous l'action de $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; en effet, V étant définie sur $\mathbb{Q}$, pour tout $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et tout $\boldsymbol{\alpha} \in V$, on a $\sigma(\boldsymbol{\alpha}) \in V$.

On voit que $S_i \subset S_j$ si $1 \leq i \leq j$; de plus, par définition du minimum essentiel, $S := \bigcup_{d \in \mathbb{N}^*} S_d$ est Zariski-dense dans V.

On a :

$$E(S_1, T, L) \supset \cdots \supset E(S_d, T, L) \supset \cdots \supset E(V, T, L)$$

et $E(V, T, L)$ étant de dimension finie, il existe $d_0 \in \mathbb{N}$ tel que $E(S_d, T, L) = E(S_{d_0}, T, L)$ pour $d \geq d_0$. Les polynômes de $E(S_{d_0}, T, L)$ sont alors nuls sur S à un ordre $\geq T$ donc sur V. En effet, pour tout $\boldsymbol{\lambda} \in \mathbb{N}^n$ vérifiant $|\boldsymbol{\lambda}| \leq T - 1$, le polynôme $\frac{\partial^{\boldsymbol{\lambda}} P}{\partial \mathbf{x}^{\boldsymbol{\lambda}}}$ est nul sur S, donc sur sur adhérence de Zariski : V. On en déduit l'égalité

$$E(S_{d_0}, T, L) = E(V, T, L),$$

en particulier $E(V, T, L)$ n'est pas réduit à $\{0\}$ et $\omega_{\mathbb{Q}}(V)$ existe.

• En faisant apparaître $E(S_{d_0}, L, T)(= E(V, L, T))$ comme solution d'un système linéaire à coefficients rationnels, on peut alors montrer qu'il existe un polynôme :

$$F_\varepsilon \in E(S_{d_0}, L, T) \cap \mathbb{Z}[\mathbf{x}] \setminus \{0\}$$

tel que

$$\log \max\{|\operatorname{coeff}(F_\varepsilon)|\} \leq \delta\Big((T + N)\log(L + 1) + L(\hat{\mu}_{\text{ess}}(V) + \varepsilon)\Big),$$

puis, en faisant tendre ε vers 0, on obtient une suite de polynômes $F_\varepsilon \in \mathbb{Z}[\mathbf{x}]$ à coefficients bornés, donc admettant une sous-suite stationnaire, d'où le résultat. ■

III.3 Fin de la preuve.

Nous sommes maintenant en mesure de montrer la seconde inégalité du théorème 4.2 :

$$\frac{\hat{h}(V)}{2\deg(V)} \leq \hat{\mu}_{\text{ess}}(V).$$

DÉMONSTRATION - On se restreint toujours au cas $n = 2$, rappelons que l'on considère une hypersurface V définie par un polynôme $P \in \mathbb{Z}[\mathbf{x}]$ irréductible de degré D.

Soit $T \in \mathbb{N}^*$, $T \geq 3$, on pose $L := DT^2$, en particulier l'espace $E(V, L, T)$ n'est pas réduit à $\{0\}$. D'après le proposition 4.3, il existe $F \in E(V, L, T) \cap \mathbb{Z}[\mathbf{x}] \setminus \{0\}$ tel que :

$$\log \max\{|\operatorname{coeff}(F)|\} \leq \delta\Big((T + 2)\log(L + 1) + L\hat{\mu}_{\text{ess}}(V)\Big),$$

où $\delta = \frac{\dim \mathbb{Q}[\mathbf{x}]_{\leq L} - \dim E(V,L,T)}{\dim E(V,L,T)}$.

Par définition on a :

$$\begin{aligned}\log M(F) &= \int_0^{2\pi}\int_0^{2\pi} \log|F(e^{i\theta_1}, e^{i\theta_1})| d\theta_1 d\theta_2 \\ &\leq \log \max_{\substack{|z|=1\\|w|=1}} |F(z,w)| \\ &\leq \log\max|\operatorname{coeff} F| + \log\binom{L+2}{2} \\ &\leq \log\max|\operatorname{coeff} F| + 2\log(L+2)\end{aligned}$$

où $\binom{L+2}{2}$ est un majorant du nombre de coefficients de F.
De plus, comme $F \in E(V,L,T) \cap \mathbb{Z}[\mathbf{x}]\setminus\{0\}$ il existe $G \in \mathbb{Z}[\mathbf{x}]\setminus\{0\}$ tel que $F = P^T G$, d'où :

$$M(F) = M(P)^T M(G) \geq M(P)^T,$$

donc :

$$\log M(P) \leq \frac{1}{T}\left\{\left(\delta(T+2)\log(L+1) + \delta L\hat{\mu}_{\text{ess}}(V)\right) + 2\log(L+2)\right\}. \qquad (4.1)$$

Majorons δ :

$$\begin{aligned}\delta &= \frac{\binom{L+2}{2}}{\binom{L-DT+2}{2}} - 1 \\ &= \frac{L+1}{L-DT+1}\times\frac{L+2}{L-DT+2} - 1 \\ &\leq \left(\frac{L}{L-DT}\right)^2 - 1\end{aligned}$$

or $L = DT^2$, soit $L - DT = DT(T-1)$ d'où

$$\begin{aligned}\delta &\leq \left(\frac{T}{T-1}\right)^2 - 1 \\ &\leq \frac{2T-1}{(T-1)^2} \\ &\leq \frac{DT}{L}\frac{(2T-1)T}{(T-1)^2} \\ &\leq 4\frac{DT}{L} \quad \text{car } T \geq 3\end{aligned}$$

Reportons ceci dans (4.1) :

$$\begin{aligned}\log M(P) &\leq \frac{1}{T}4\frac{DT}{L}(T+2)\log(L+1) + \frac{1}{T}\frac{2T-1}{(T-1)^2}L\hat{\mu}_{\text{ess}}(V) + \frac{1}{T}2\log(L+2) \\ &\leq \frac{4D(T+2)\log(L+1)}{L} + D\frac{T(2T-1)}{(T-1)^2}\hat{\mu}_{\text{ess}}(V) + \frac{2\log(L+2)}{T}.\end{aligned}$$

Comme $L = DT^2$, en faisant tendre T vers $+\infty$ on obtient :

$$\hat{h}(V) = \log M(P) \leq 2D\hat{\mu}_{\text{ess}}(V).$$

■

IV Approches de Lehmer en dimension supérieure.

Comme nous l'avons dit au début du chapitre, on peut étendre la notion de hauteur en considérant des points de $\mathbb{G}_m^n$ ou des variétés algébriques sur $\mathbb{G}_m^n$, les meilleurs résultats obtenus sont des analogues du théorème de E. Dobrowolski (3.1) dans les deux cas.

IV.1 Résultats dans $\mathbb{G}_m^n$.

On remplace ici le degré de $\boldsymbol{\alpha}$ par son *indice d'obstruction* : $\omega_{\mathbb{Q}}(\boldsymbol{\alpha})$, qui est donc le plus petit des degrés des polynômes de $\mathbb{Q}[\mathbf{x}]$ s'annulant en $\boldsymbol{\alpha}$, de plus on ne parle plus de nombre non racine de l'unité, mais de points à coordonnées multiplicativement indépendantes :

Définition 4.5 *Soient $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}^*$, on dit que ces nombres sont **multiplicativement indépendants** si :*

$$\forall (a_1, \ldots, a_r) \in \mathbb{Z}^r,\ \prod_{i=1}^{r} \alpha_i^{a_i} = 1 \Rightarrow (a_1, \ldots, a_r) = (0, \ldots, 0).$$

On peut généraliser la conjecture 1.1 ainsi

Conjecture 4.1 *Pour tout $n \in \mathbb{N}^*$, il existe une constante réelle $c(n) > 0$ telle que, pour tout $\boldsymbol{\alpha} \in \mathbb{G}_m^n$ dont les coordonnées sont multiplicativement indépendantes, on ait :*

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

Dans cette direction, [Am-Da1] obtiennent, en adoptant la méthode de Dobrowolski :

Théorème 4.3 *Pour tout $n \in \mathbb{N}^*$, il existe un réel $c(n) > 1$ tel que pour tout $\boldsymbol{\alpha} \in \mathbb{G}_m^n$ à coordonnées multiplicativement indépendantes, on ait :*

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

où $\kappa(n) = (n+1)(n+1)!^n - n$.

Dans ce même article, ils en déduisent un corollaire intéressant, nous dit que si $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{tors}$ ne possède pas un groupe de Galois trop «gros», alors la conjecture de Lehmer est vraie, plus précisément :

Corollaire 4.1 *Pour tout entier $m \in \mathbb{N}^*$, il existe une constante $c(m) > 0$ telle que la propriété suivante soit vraie.*

Pour tout $\alpha \in \overline{\mathbb{Q}}^* \setminus \overline{\mathbb{Q}}^*_{tors}$ tel que $\#Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \leq (\deg(\alpha))^m$ on a :

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

IV.2 Résultats pour les hypersurfaces.

Si V est une hypersurface définie par le polynôme $F \in \mathbb{Z}[\mathbf{x}]$ irréductible, le théorème de Zhang et la proposition 4.2 nous disent que :

$$\hat{\mu}_{\text{ess}}(V) = 0 \;\Leftrightarrow\; F \text{ est un polynôme cyclotomique généralisé.}$$

Dans ce cas précis des hypersurfaces, la conjecture suivante généralise la 1.1 en dimension supérieur :

Conjecture 4.2 *Pour tout $n \in \mathbb{N}^*$, il existe une constante réelle $c(n) > 0$ telle que pour tout polynôme non nul $F \in \mathbb{Z}[\mathbf{x}]$ irréductible $F(\mathbf{x}) \neq \pm \mathrm{x}_j$ qui ne soit pas un polynôme cyclotomique généralisé, on ait*

$$\log M(F) \geq c(n).$$

Dans cette direction [Am-Da1] on obtenue un résultat plus précis que le théorème 4.3 : l'exposant du logarithme du degré est absolu au lieu de se comporter en n^{n^2}.

Soit V une sous-variété de $\mathbb{G}_m^n$; on note G_V le stabilisateur de V, *i. e.* l'ensemble

$$G_V = \left\{ \mathbf{x} \in \mathbb{G}_m^n \;:\; \mathbf{x}.V = V \right\},$$

où

$$\boldsymbol{\xi}.V = \left\{ \boldsymbol{\xi}.\mathbf{x} = (\mathrm{x}_1\xi_1, \ldots, \mathrm{x}_n\xi_n) \;:\; \mathbf{x} \in V \right\}.$$

Théorème 4.4 *Soit V une hypersurface définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible de $\mathbb{G}_m^n$ de degré D et notons $s = \dim G_V$. Alors, si V n'est pas une réunion de translatés de sous-groupes algébriques par des points de torsion de $\mathbb{G}_m^n$, on a*

$$\hat{h}(V) \geq \frac{1}{Cn^6} \frac{\Big(\log\Big(n\log\big(nD\big)\Big)\Big)^{2+1/(n-s)}}{\Big(\log\big(nD\big)\Big)^{1+2/(n-s)}}$$

où C est une constante absolue.

ANNEXE.

Rappels de géométrie algébrique.

On note souvent en gras pour désigner un multi-indice : $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$ par exemple.
Soient I un idéal de $k[\mathrm{x}_1, \ldots, \mathrm{x}_n]$ et $V \subset k^n$, on note

$$Z(I) = \Big\{ \boldsymbol{\alpha} \in k^n \mid P(\boldsymbol{\alpha}) = 0, \forall P \in I \Big\}$$

$$I_V = \Big\{ P \in k[\mathrm{x}_1, \ldots, \mathrm{x}_n] \mid P(\boldsymbol{\alpha}) = 0, \forall \boldsymbol{\alpha} \in V \Big\}$$

Définition 4.6 *Une variété algébrique affine V est un ensemble de la forme $V = Z(I)$, où I est un idéal de $k[\mathrm{x}_1, \ldots, \mathrm{x}_n]$. On dit que V est définie sur k si son idéal I_V peut être engendré par des polynômes de $k[\mathbf{x}]$.*

Définition 4.7 *Soit V une variété algébrique (affine) définie sur k. On dit que V est k-irréductible si elle ne peut s'écrire comme union de deux sous-variétés propres définies sur k, ce qui revient à dire que I_V est premier.*
On dit que V est géométriquement irréductible si elle est $\overline{\mathbb{Q}}$-irréductible.

Cas particulier des hypersurfaces algébriques.

Définition 4.8 *On appelle hypersurface algébrique (définie sur k) une variété algébrique définie par les zéros d'un polynôme de $k[\mathbf{x}]$; i. e. il existe $F \in k[\mathbf{x}]$ tel que $V = Z\big((F)\big)$ (I_V est principal).*

Remarques :

- Une hypersurface V est irréductible sur k si et seulement s'il existe $F \in k[\mathbf{x}]$ irréductible sur k représentant V.
- Le degré de V est le plus petit des degrés des polynômes représentant V.

Exemple : le polynôme $x^4 - 5y^2$ défini une hypersurface de $\mathbb{G}_m^2$, irréductible sur $\mathbb{Q}$, mais sur $\mathbb{Q}(\sqrt{5})$ on a $Z\big((x^4 - 5y^2)\big) = Z\big((x^2 - \sqrt{5}y)\big) \cup Z\big((x^2 - \sqrt{5}y)\big)$.

Définition 4.9 *On appelle topologie de Zariski sur k^n la topologie où les fermés sont les ensembles $Z(I)$ où I est un idéal de $k[x_1, \ldots, x_n]$.*

Propriétés 4.3 *Une variété algébrique irréductible est en particulier connexe pour la topologie de Zariski.*

Bibliographie

[Am-Da1] F. Amoroso et S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. 513 (1999), p. 145-179.

[Am-Da2] F. Amoroso et S. David, *Minoration de la hauteur normalisée des hypersurfaces*, Acta Arithmetica 92.4 (2000), p. 339-366.

[AmDv1] F. Amoroso et R. Dvornicich, *A lower bound for the height in Abelian extension.*, Journal of Number Theory 80 (2000), no. 2, p. 260-272.

[Boy] D. Boyd, *Kronecker's Theorem and Lehmer's Problem for Polynomials in Several Variables*, Journal of Number Theory 13 (1980), p. 116-121.

[CF] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory.* Academic Press (1967).

[Do] E. Dobrowolski, *On a question of Lehmer and the number of irreductible factors of a polynomial*, Acta Arithmetica 34 (1979), p. 391-401.

[Go] X. Gourdon, *Les maths en tête. Algèbre.*, Ellipses (1994).

[HW] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers.*, Oxford : Clarendon press.

[La] W Lawton, *A generalization of a theorem of Kronecker*, J. Sci. Fac., Chang-mai Univ. (Thaïlande) 4 (1977), p. 15-23.

[Leh] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. (2) 34, (1933), p. 461-479.

[Ma] D. A. Marcus, *Number Fields*, Springer-Verlag (1977).

[MM] J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization.*, J. Reine Angew. Math. p.286 287

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

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

[Vo] P. Voutier, *An effective lower bound for the heigth of algebraic numbers*, Acta Arithmetica 74, (1996), p. 81-95.

[Wa] L. C. Washington, *Introduction to cyclotomic fields.*, Springer-Verlag (1982).