THÈSE de DOCTORAT de l'UNIVERSITÉ PARIS VI

Spécialité :
MATHÉMATIQUES

présentée par

Andrea SURROCA ORTIZ

pour obtenir le grade de DOCTEUR de l'UNIVERSITÉ PARIS VI

Sujet :

Méthodes de transcendance et géométrie diophantienne

Table des matières

Présentation de la thèse **5**

I Première partie **9**

Valeurs algébriques de fonctions transcendantes **11**
1.1 Introduction. 11
1.2 Notations. 15
1.3 Estimation du cardinal de $E_{D,N}$. 17
1.3.1 Démonstration du lemme 2. 18
1.3.2 Démonstration du lemme 1. 21
1.3.3 Autres résultats. 23
1.4 Construction d'exemples. 25
1.4.1 Construction de la fonction f. 25
1.4.2 Construction de la fonction g. 31
1.5 Démonstration du théorème 2. 32
1.5.1 Schéma de démonstration. 32
1.5.2 Énoncés préliminaires. 32
1.5.3 La démonstration. 34

Bibliographie de la première partie **41**

II Deuxième partie **43**

La conjecture *abc* et le théorème de Siegel **45**
2.1 Introduction. 45
2.2 Notations et préliminaires. 51
2.2.1 Valeurs absolues, hauteurs et radicaux. 51
2.2.2 Plongements affines et points S-entiers. 56
2.2.3 Modèles entiers et bonne réduction. 59
2.2.4 Lemmes analytiques. 61
2.3 *abc* implique Siegel. 63
2.3.1 Des théorèmes et conjectures. 63

2.3.2 Vers "Siegel effectif". 65
2.3.3 Variation sur "Siegel effectif". 67
2.3.4 Majoration du radical. 67
2.4 De Siegel uniforme à *abc*. 71
2.4.1 L'hypothèse "Siegel uniforme". 71
2.4.2 Vers *abc*. 75
2.5 Cas de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$. 78
2.5.1 Introduction. 78
2.5.2 $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, *abc* et les S-unités. 80
2.6 Applications. 83

Appendice : Le théorème de Siegel uniforme sur les corps de fonctions. 89

Bibliographie de la deuxième partie 95

Présentation de la thèse

Cette thèse se compose de deux parties distinctes : “Valeurs algébriques de fonctions transcendantes” et “Sur la conjecture *abc* et le théorème de Siegel”. Toutefois nous pouvons remarquer que, de près ou de loin, les deux doivent quelque chose aux méthodes dites de transcendance.

En ce qui concerne la première partie, la présence des méthodes de transcendance est claire : c'est l'outil essentiel dans la démonstration du résultat principal. Il s'agit d'une majoration du nombre de points algébriques où une fonction analytique transcendante prend des valeurs algébriques. La démonstration utilise des méthodes classiques de transcendance, avec dans un premier temps, choix des paramètres et construction d'une fonction auxiliaire à l'aide d'un lemme de Siegel ; nous utilisons ensuite une récurrence, avec un lemme de Schwarz et l'inégalité de Liouville.

Les méthodes de transcendance interviennent de façon beaucoup plus indirecte dans la deuxième partie du travail, portée plutôt sur des problèmes diophantiens. Cette partie traite du théorème de Siegel sur les points entiers de courbes algébriques et des liens avec la conjecture *abc* de Masser et Oesterlé. Que ce soit pour les résultats connus allant dans le sens de la conjecture *abc* ou pour les versions effectives et uniformes du théorème de Siegel, les deux types de résultats reposent sur des minorations de formes linéaires de logarithmes, démontrées avec des méthodes de transcendance.

L'autre point commun des deux parties est l'usage des fonctions hauteurs. Encore ici, l'approche n'est pas la même dans tout le texte. La première partie est portée sur le décompte de points algébriques de hauteur et de degré bornés. Il s'agit donc de la hauteur de Weil sur $\mathbf{P}^1(\overline{\mathbf{Q}})$, de la hauteur naïve d'un polynôme et de la mesure de Mahler. La deuxième partie du texte s'intéresse aux points de courbes algébriques. Nous utilisons des fonctions hauteur de Weil définies sur des courbes.

Présentons maintenant ces deux parties indépendamment.

La première partie, réalisée sous la direction de Michel Waldschmidt, est consacré à la majoration du nombre de points algébriques où une fonction analytique trascendante prend des valeurs algébriques. Étant donnée une fonction f analytique sur un disque ouvert $D(0,R)$, on considère l'ensemble de points algébriques du disque en lesquels la fonction f prend des valeurs algébriques. Nous nous intéressons aux fonctions transcendantes sur $\mathbf{C}(z)$,

c'est-à-dire telles qu'il n'existe pas de polynôme non nul en deux variables et à coefficients complexes, s'annulant sur tous les points $(z, f(z))$ pour $z \in D(0, R)$.

Le théorème de Hermite-Lindemann montre que la fonction exponentielle ne prend des valeurs algébriques que en un seul point algébrique, à savoir 0. Suivant une suggestion de Weierstrass, Stäckel montre qu'il existe des fonctions entières et transcendantes prenant des valeurs algébriques en tous les points algébriques.

Filtrons l'ensemble dénombrable des nombres algébriques par le degré et la hauteur. Pour tout entier naturel D et tout réel $N > 0$, on considère l'ensemble $E_{D,N}$ des nombres algébriques de hauteur logarithmique absolue et de degré bornés. Le lemme 1 donne un encadrement du cardinal de $E_{D,N}$ de l'ordre de e^{D^2N}. Ensuite, nous fixons une fonction f analytique sur $D(0, R)$ et trascendante et nous considérons, pour $r < R$, l'ensemble $\Sigma_{D,N}(f, r)$ des éléments de $E_{D,N} \cap \overline{D(0, r)}$ tels que leur image aussi soit dans $E_{D,N}$. Le résultat principal de cette partie, le théorème 1, montre que, pour tout entier naturel D, il existe une infinité de nombres réels N arbitrairement grands, tels que le cardinal de $\Sigma_{D,N}(f, r)$ soit inférieur à $\delta D^3 N^2$, avec δ ne dépendant que de la fonction f.

Nous généralisons ensuite ce résultat au cas de plusieurs fonctions analytiques algébriquement indépendantes. C'est le théorème 2. La démonstration utilise des méthodes classiques de transcendance.

Dans la section 1.4, nous construisons des fonctions entières transcendantes vérifiant le théorème de Stäckel. En particulier, le théorème 3 montre que, dans le théorème 1, on ne peut pas obtenir une version uniforme en la borne de la hauteur. Le théorème 5 assure l'existence d'une fonction entière et transcendante, dont toutes ses dérivées, envoient tout nombre algébrique α dans $\mathbf{Z}\left[\frac{1}{2}, \alpha\right]$; et dont on contrôle aussi la hauteur des valeurs prises aux points entiers.

Nous renvoyons le lecteur à l'introduction de cette première partie, la section 1.1, où les théorèmes sont énoncés en détail.

La deuxième partie de notre travail, réalisée sous la direction de Marc Hindry, concerne des problèmes diophantiens. Elle est consacrée aux liens entre le théorème de Siegel sur les points entiers des courbes algébriques et la conjecture *abc* de Masser et Oesterlé.

Siegel démontra en 1929 que l'ensemble de points entiers d'une courbe algébrique non exceptionnelle est fini. Ce résultat a été élargi par la suite par Mahler aux points ayant les facteurs premiers de leurs dénominateurs dans un ensemble fini S ; ce sont ce que l'on appelle des points S-entiers.

Cependant la démonstration de Siegel n'est pas effective, dans le sens ou elle ne permet pas de déterminer toutes les solutions. Les versions effectives du théorème de Siegel connues à l'heure actuelle ont été obtenues grâce aux minorations de formes linéaires de logarithmes introduites par Baker. Il s'agit

de bornes pour la hauteur des points S-entiers de la courbe et c'est ce à quoi nous nous sommes intéressés.

Une approche plus récente, qui a influencé ce travail, a été proposée par Elkies et se base sur la conjecture *abc*. Avec cette approche, et en supposant vraie la conjecture *abc*, nous majorons la hauteur des points S-entiers d'une courbe vérifiant les hypothèses du théorème de Siegel, pour tout ensemble S. Nous obtenons le théorème 9 de la section 2.3, ainsi que sa variante, le théorème 13.

Un autre aspect sur lequel nous avons mis l'accent est celui de l'uniformité des bornes par rapport à l'ensemble S. Dans la section 2.4 nous formulons une hypothèse du type "Siegel uniforme". Celle-ci a été inspirée d'une part par une hypothèse sur les points rationnels formulée par Moret-Bailly, et d'autre part, par des résultats sur les corps de fonctions qui sont détaillés dans l'appendice. Le fait de pouvoir faire varier S, nous permet de remonter la démonstration dans l'autre sens, c'est-à-dire d'aller de Siegel effectif et uniforme vers *abc* et de démontrer le théorème 10.

Nous traitons par la suite le cas particulier de la droite projective privée de 0,1 et l'infini, que nous mettons en relation avec l'équation classique aux S-unités et une variante de la conjecture *abc*. Le théorème 15 démontré ici met en valeur l'intérêt de considérer des points S-entiers.

Dans la section 2.6, nous obtenons des versions inconditionnelles des résultats mentionnés auparavant. Un théorème de Stewart et Yu (version affaiblie de la conjecture *abc*, mais non conjecturale) nous permet d'obtenir des bornes uniformes en S pour les solutions de l'équation aux S-unités, $Au + Bv = 1$ (théorème 18), ainsi que pour les points entiers de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ (théorème 20), dans le cas où le corps de nombres est $\mathbf{Q}$. À partir d'un théorème de Bilu (version uniforme du théorème de Siegel pour les courbes qui sont revêtement galoisien de la droite projective), nous obtenons un résultat allant dans le sens de la conjecture *abc*, valable sur tout corps de nombres à la différence des résultats connus à présent. C'est le théorème 17. Il nous permet d'étendre les théorèmes 18 et 20 à tout corps de nombres.

Pour une présentation plus large avec des énoncés précis, le lecteur est invité à se reporter à l'introduction de cette deuxième partie, la section 2.1.

I

Première partie

Valeurs algébriques de fonctions transcendantes

1.1 Introduction.

Un problème de base en théorie des nombres transcendants ([Mah] chapitre 3) est le suivant. Étant donnée une fonction f analytique sur un disque ouvert $D(0,\rho)$ (où ρ est un nombre réel strictement positif ou l'infini), on considère l'ensemble S_f des points algébriques dans $D(0,\rho)$ en lesquels la fonction f prend des valeurs algébriques. Il s'agit d'étudier l'ensemble S_f. Ici, la fonction f sera transcendante. Par exemple, d'après le théorème de Hermite-Lindemann (théorème 1.2 [W]), la fonction exponentielle prend des valeurs transcendantes en tout point algébrique, sauf en 0. Donc pour $f(z) = e^z$, on a $S_f = \{0\}$. Par la même raison, si on pose $f(z) = e^{P(z)}$ où $P \in \overline{\mathbf{Q}}[X]$, alors S_f est l'ensemble des zéros de P. En supposant vraie la conjecture de Schanuel ([La2] p. 30 ou [W]), pour $f(z) = \sin(\pi z)e^z$ on a $S_f = \mathbf{Z}$. Le théorème de Gel'fond-Schneider (théorème 1.4 [W]) nous fournit d'autres exemples : si $f(z) = e^{\lambda z}$ où $\lambda \neq 0$ est tel que e^λ soit algébrique (par exemple, $f(z) = 2^z$ ou $f(z) = e^{i\pi z}$), alors $S_f = \mathbf{Q}$.

Dans une lettre de 1886 adressée à Strauss [St1], Weierstrass montrait, avec un exemple, qu'il existe des fonctions entières et transcendantes prenant des valeurs rationnelles en tous les points rationnels (cf. aussi [NR]) et suggérait l'existence de fonctions entières transcendantes prenant des valeurs algébriques en tous les points algébriques. En suivant cette remarque, Strauss montre l'existence d'une fonction f analytique sur le disque unité, non rationnelle et vérifiant $f(\alpha) \in \overline{\mathbf{Q}},\ \forall \alpha \in \overline{\mathbf{Q}}$. Stäckel conclut, avec un théorème d'irréductibilité de Hilbert, que la fonction est forcément transcendante. La remarque suggérée par Weierstrass sera montrée en sa totalité, avec f entière, par Stäckel (cf. [Gr] et [St1]), qui énonce le théorème suivant :

Étant donnés un sous-ensemble Σ *dénombrable de* $\mathbf{C}$ *et un sous-ensemble* T *dense de* $\mathbf{C}$, *il existe une fonction entière transcendante envoyant* Σ *dans* T.

En prenant $\Sigma = T = \overline{\mathbf{Q}}$, on obtient une fonction f entière et transcendante vérifiant $S_f = \overline{\mathbf{Q}}$. Par ailleurs, on en déduit, en posant $\Sigma = \overline{\mathbf{Q}}$ et

$T = \mathbf{C} \setminus \overline{\mathbf{Q}}$, l'existence d'une fonction entière transcendante prenant des valeurs transcendantes en tous les points algébriques, c'est-à-dire, telle que $S_f = \emptyset$. (Sous la conjecture de Schanuel, on peut montrer que pour la fonction $f(z) = e^{e^z}$ on a $S_f = \emptyset$.)

F.Gramain remarque dans [Gr], que si Σ est contenu dans $\mathbf{R}$, la même démonstration s'applique avec T dense dans $\mathbf{R}$. Ceci nous permet de prendre $\Sigma = K$, corps de nombres réel, ou $\Sigma = O_{K,S}$ l'anneau des S-entiers d'un corps de nombres K réel, et, dans les deux cas, $T = \mathbf{Z}\left[\frac{1}{n}\right]$, pour n'importe quel entier naturel $n \geq 2$.

En suivant une remarque de Stäckel, qui construit [St2] une fonction algébrique qui prend, ainsi que toutes ses dérivées, des valeurs algébriques en tous les points algébriques, G. Faber [Fa] construit une fonction G entière et transcendante telle que, pour tout nombres entier k et tout $\alpha \in \overline{\mathbf{Q}}$, la valeur de la fonction dérivée $G^{(k)}$ en α est dans $\mathbf{Q} + i\mathbf{Q}$.

Dans la section 1.4, nous construisons une fonction f entière et transcendante (théorème 3), dont toutes ses dérivées, envoient tout corps de nombres dans lui-même (cf. aussi [VdP]), et pour laquelle on contrôle la hauteur des valeurs prises aux points algébriques. On construit aussi (théorème 5) une fonction g entière et transcendante, dont toutes ses dérivées, envoient tout nombre algébrique α dans $\mathbf{Z}\left[\frac{1}{2}, \alpha\right]$; et dont on contrôle aussi la hauteur des valeurs prises aux points entiers.

Nous filtrons l'ensemble dénombrable des nombres algébriques par le degré et la hauteur logarithmique absolue (dont la définition précise est rappelée dans la section 1.2) : pour D entier ≥ 1 et N nombre réel ≥ 0, l'ensemble

$$E_{D,N} = \{\alpha \in \overline{\mathbf{Q}} /\ [\mathbf{Q}(\alpha) : \mathbf{Q}] \leq D,\ \ h(\alpha) \leq N\}$$

est fini et son cardinal $\epsilon_{D,N}$ vérifie l'encadrement suivant.

Lemme 1. *Encadrement du cardinal de $E_{D,N}$.*

Pour tout entier $D \geq 1$ et tout nombre réel $N \geq 0$, le cardinal $\epsilon_{D,N}$ de $E_{D,N}$ vérifie

$$e^{D(D+1)(N-1)} < \epsilon_{D,N} \leq e^{D(D+1)(N+1)}.$$

(Dans ce travail, nous nous servons du lemme 1, mais d'autres énoncés sont connus (cf. la section 1.3.3).)

Dans ce texte, nous fixons une fonction f transcendante et nous intéressons à l'ensemble des $\alpha \in E_{D,N}$ tels que $f(\alpha) \in E_{D,N}$.

Le problème sera local. Pour tout couple de nombres réels (R, r) vérifiant $R > r > 0$, pour toute fonction f analytique sur $D(0, R)$ et à valeurs complexes, pour tout entier $D \geq 1$ et tout nombre réel $N \geq 0$, on note $\Sigma_{D,N} = \Sigma_{D,N}(f, r)$ l'ensemble des nombres $\alpha \in \overline{\mathbf{Q}} \cap \overline{D(0, r)}$ tels que

$$f(\alpha) \in \overline{\mathbf{Q}},\ \ [\mathbf{Q}(\alpha, f(\alpha)) : \mathbf{Q}] \leq D,\ \ h(\alpha) \leq N \ \text{ et } \ h(f(\alpha)) \leq N,$$

et $\sigma_{D,N}$ son cardinal. Ainsi, S_f est la réunion des $\Sigma_{D,N}$ pour $D \geq 1$ et $N \geq 0$.

Nous rappelons que la fonction analytique f est dite transcendante sur $\mathbf{C}(z)$, s'il n'existe pas de polynôme non nul en 2 variables et à coefficients complexes, s'annulant sur tous les points $(z, f(z))$ pour les z où f est définie.

Théorème 1. *Majoration du cardinal de* $\Sigma_{D,N}(f, r)$.

Soient R *et* r *deux nombres réels vérifiant* $R > r > 0$, $c_0 = \log\left(\frac{R^2+r^2}{2rR}\right)$ *et* δ *un nombre réel tel que* $\delta > 2\left(\frac{6}{c_0}\right)^2$. *Soit* f *une fonction analytique sur* $D(0, R)$, *continue sur* $\overline{D(0, R)}$ *et transcendante sur* $\mathbf{C}(z)$.

Pour tout entier $D \geq 1$, *il existe une suite de nombres réels* $N \geq 0$ *tendant vers l'infini pour lesquels*

$$\sigma_{D,N} < \delta D^3 N^2.$$

Remarques.

i) Les nombres réels c_0 et δ sont strictement positifs et dépendent uniquement des réels r et R.

ii) Pour D et N fixés, l'ensemble $\Sigma_{D,N}$ est fini, puisqu'il est contenu dans l'ensemble $E_{D,N}$. Le théorème 1 montre que, pour une infinité d'entiers N, le nombre $\sigma_{D,N}$ est beaucoup plus petit que $\epsilon_{D,N}$.

Nous démontrons le théorème 2 ci-dessous qui généralise le théorème 1.

Pour des nombres réels R, r et c_0 comme dans le théorème 1 et un entier $t \geq 2$, on note

$$\gamma_t = \max_{2 \leq \tau \leq t} \left(\frac{1}{2}\left(\frac{c_0}{3\tau}\right)^{\tau}\right)^{\frac{-1}{\tau-1}}. \tag{1.1}$$

Ainsi γ_t ne dépend que de R, r et t.

Pour $f_1, \ldots, f_t$ des fonctions analytiques sur $D(0, R)$, pour tout entier $D \geq 1$ et tout nombre réel $N \geq 0$, on considère l'ensemble $\Sigma_{D,N}(f_1, \ldots, f_t, r)$ des nombres $w \in \mathbf{C} \cap \overline{D(0, r)}$ tels que,

$$\forall i \in \{1, \ldots, t\}, \quad f_i(w) \in \overline{\mathbf{Q}}, \quad h(f_i(w)) \leq N$$

et

$$[\mathbf{Q}(f_1(w), \ldots, f_t(w)) : \mathbf{Q}] \leq D.$$

Théorème 2. *Majoration du cardinal de* $\Sigma_{D,N}(f_1, \ldots, f_t, r)$.

Soient R *et* r *des nombres réels vérifiant* $R > r > 0$ *et* $c_0 = \log\left(\frac{R^2+r^2}{2rR}\right)$. *Soient* t *un entier* ≥ 2 *et* γ *une constante réelle telle que* $\gamma > \gamma_t$.

Soient $f_1, \ldots, f_t$ *des fonctions analytiques sur* $D(0, R)$ *et continues sur* $\overline{D(0, R)}$, *algébriquement indépendantes.*

Pour tout entier $D \geq 1$, *il existe une infinité de nombres réels* $N \geq 0$ *pour lesquels*

$$\mathrm{card}(\Sigma_{D,N}(f_1,\dots,f_t,r)) < \gamma\, D^{a(t)} N^{b(t)},$$

où $a(t)=\frac{t+1}{t-1}$ *et* $b(t)=\frac{t}{t-1}$.

Notons que pour $t \geq 2$, on a $a(t) \leq 3$ et $b(t) \leq 2$.

Remarque 1. *Si* $t=2$, $a(t)=3$, $b(t)=2$ *et en prenant pour une des deux fonctions l'identité, l'autre fonction est alors transcendante, et nous retrouvons le théorème 1.*

Le théorème 3, qui sera démontré dans la section 1.4.1, montre qu'on ne peut pas remplacer, dans le théorème 1, "il existe une infinité de nombres réels N" par "pour tout N assez grand". Précisément, nous avons l'énoncé suivant.

Théorème 3. *Soit* ϕ *une fonction positive telle que* $\phi(x)/x$ *tende vers* 0 *quand* $x \to \infty$. *Il existe une fonction* f *entière et transcendante sur* $\mathbf{C}(z)$, *vérifiant*

$$\forall \alpha \in \overline{\mathbf{Q}},\ \ \forall \sigma \geq 0,\ \ f^{(\sigma)}(\alpha) \in \mathbf{Q}(\alpha), \tag{1.2}$$

et telle que, pour tout entier $D \geq 1$, *il existe une infinité de nombres réels* $N \geq 0$ *arbitrairement grands vérifiant*

$$\mathrm{card}(\Sigma_{D,N}(f,1)) \geq e^{D(D+1)\phi(N)-\log 2}. \tag{1.3}$$

Pour le cas $D=1$, Elkies [El] énonce le résultat suivant.

Théorème 4. *(Elkies)*
Soit C *un arc analytique transcendant dans* $\mathbf{P}^2$, *i.e.*

$$C = \{\varphi(x) :\ \ a \leq x \leq b\}$$

où φ *est une application analytique définie sur un voisinage de* $[a,b]$ *à valeurs dans* $\mathbf{P}^2$, *dont l'image n'est incluse dans aucune courbe algébrique.*

Alors, pour tout $\varepsilon > 0$, *il existe une constante* A_ε *telle que, pour tout* $N \geq 0$, *le nombre de points dans* $C \cap \mathbf{P}^2(\mathbf{Q})$ *de hauteur logarithmique* $\leq N$ *est inférieur ou égal à*

$$A_\varepsilon\, e^{\varepsilon N}.$$

Considérons un nombre réel r et une fonction analytique sur le disque $\overline{D(0,r)}$, transcendante sur $\mathbf{C}(z)$. En prenant $\varphi(x)=(1:x:f(x))$ et $a=-b=r$, le théorème 4 implique le corollaire ci-dessous.

Pour tout $\varepsilon > 0$ *il existe une constante* A_ε, *telle que, pour tout nombre réel* $N \geq 0$, *on ait*

$$\mathrm{card}(\Sigma_{1,N}(f,r)) \leq A_\varepsilon\, e^{\varepsilon N}.$$

En modifiant la fonction f du théorème 3, on peut construire une fonction g entière et transcendante, vérifiant la même conclusion (1.3) concernant le cardinal de $\Sigma_{D,N}(g,1)$, mais pour laquelle la première conclusion est changée. Précisément :

Théorème 5. *Il existe une fonction g entière et transcendante sur $\mathbf{C}(z)$ telle que,*

$$\forall \alpha \in \overline{\mathbf{Q}},\ \ \forall \sigma \geq 0,\ \ g^{(\sigma)}(\alpha) \in \mathbf{Z}\left[\frac{1}{2}, \alpha\right]. \tag{1.4}$$

Remarque. Le théorème 3, qui fait intervenir les dérivées de la fonction transcendante, pose le problème suivant. Peut-on espérer d'avoir un énoncé dans le sens du théorème 1, fesant lui aussi, intervenir les dérivées ? Il s'agirait de borner l'ensemble de points algébriques où toutes les dérivées de la fonction transcendante f prend des valeurs algébriques, de degré et hauteur bornés.

1.2 Notations.

Pour les notations qui suivent, on peut consulter [W].

Pour un corps de nombres K, on note M_K l'ensemble de ses valeurs absolues normalisées, c'est-à-dire, celles dont la restriction à $\mathbf{Q}$ sont, soit la valeur absolue archimédienne $|.|_\infty$, soit une des valeurs absolues $p-$adiques $|.|_p$, où p est un nombre premier, normalisées de la façon suivante :

$$|x|_\infty = x,\ \ \text{si}\ \ x \in \mathbf{Q},\ \ x > 0,$$
$$|p|_p = \frac{1}{p},\ \ \text{si}\ \ p\ \ \text{est un nombre premier.}$$

On note d_v le degré local en la valeur absolue v. La formule du produit pour un nombre algébrique α appartenant à un corps de nombres K s'écrit alors

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = 1.$$

Si α est un nombre algébrique et K un corps de nombres le contenant, on définit sa hauteur projective multiplicative absolue par

$$H(\alpha) = \left(\prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v} \right)^{\frac{1}{[K:\mathbf{Q}]}}.$$

On définit aussi sa hauteur projective logarithmique absolue, en posant

$$h(\alpha) = \log H(\alpha) = \frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\}.$$

On remarque que pour tout couple (α, β) de nombres algébriques, on a (cf. [W] chapitre 3) les inégalités suivantes :

$$h(\alpha\beta) \leq h(\alpha) + h(\beta) \tag{1.5}$$

$$h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2. \tag{1.6}$$

Plus généralement, pour $\alpha_1, \ldots, \alpha_d \in \overline{\mathbf{Q}}$, on a

$$h(\alpha_1 + \cdots + \alpha_d) \leq h(\alpha_1) + \cdots + h(\alpha_d) + \log d. \tag{1.7}$$

Si $a_0 X^d + a_1 X_{d-1} + \ldots + a_d$ est le polynôme minimal sur $\mathbf{Z}$ de α (où $d = [\mathbf{Q}(\alpha) : \mathbf{Q}]$) et $\alpha_1 = \alpha, \ldots, \alpha_d$ ses conjugués, on définit la mesure de Mahler de α par

$$M(\alpha) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Elle est reliée à la hauteur logarithmique absolue par la relation ([W] chapitre 3 lemma 3.10)

$$h(\alpha) = \frac{1}{d} \log M(\alpha) \tag{1.8}$$

et donc à la hauteur multiplicative absolue par

$$M(\alpha)^{\frac{1}{[\mathbf{Q}(\alpha):\mathbf{Q}]}} = H(\alpha). \tag{1.9}$$

La hauteur usuelle d'un polynôme $P \in \mathbf{C}[X]$ est, par définition, le maximum de ses coefficients. La hauteur usuelle d'un nombre algébrique α est définie comme étant la hauteur usuelle de son polynôme minimal, à savoir (en gardant les mêmes notations),

$$\mathcal{H}(\alpha) = \max\{|a_0|, \ldots, |a_d|\}.$$

La hauteur usuelle est liée à la hauteur logarithmique absolue par la double inégalité suivante ([W] chapitre 3 lemma 3.11)

$$\frac{1}{d} \log \mathcal{H}(\alpha) - \log 2 \leq h(\alpha) \leq \frac{1}{d} \log \mathcal{H}(\alpha) + \frac{1}{2d} \log(d+1). \tag{1.10}$$

Au lieu de la première inégalité, nous utiliserons plutôt celle-ci :

$$\frac{1}{d} \log \mathcal{H}(\alpha) - \frac{d-1}{d} \log 2 \leq h(\alpha), \tag{1.11}$$

obtenue de la même façon que la première, en remarquant que les coefficients binômiaux sont majorés par 2^{d-1}.

Pour un polynôme $P \in \mathbf{C}[X,Y]$ on note $L(P)$ sa longueur. C'est la somme des modules de ses coefficients.

Pour un nombre réel $\rho > 0$ et une fonction F continue dans le disque fermé $\overline{D(0,\rho)}$, on note

$$|F|_\rho = \max_{|z|\leq\rho} |F(z)|.$$

Pour $x \in \mathbf{R}$, $[x]$ désigne la partie entière de x. Elle vérifie

$$[x] \in \mathbf{Z} \text{ et } 0 \leq x - [x] < 1.$$

1.3 Estimation du cardinal de $E_{D,N}$.

On rappelle que pour D entier ≥ 1 et N réel ≥ 0, on a noté $E_{D,N}$ l'ensemble des nombres algébriques de degré majoré par D et de hauteur logarithmique absolue majorée par N.

Pour estimer son cardinal $\epsilon_{D,N}$, nous considérons l'ensemble $A_{D,H}$ (H étant un nombre réel positif) des nombres algébriques de degré majoré par D et de hauteur usuelle majorée par H,

$$A_{D,H} = \{\alpha \in \overline{\mathbf{Q}} / \ [\mathbf{Q}(\alpha) : \mathbf{Q}] \leq D, \ \mathcal{H}(\alpha) \leq H\}.$$

Pour tout entier d, $1 \leq d \leq D$, nous considérons aussi l'ensemble $\mathcal{A}_{d,H}$ des nombres algébriques dans $A_{D,H}$ de degré exactement d,

$$\mathcal{A}_{d,H} = \{\alpha \in \overline{\mathbf{Q}} / \ [\mathbf{Q}(\alpha) : \mathbf{Q}] = d, \ \mathcal{H}(\alpha) \leq H\},$$

et l'ensemble $\mathcal{P}_{d,H}$ des polynômes à coefficients entiers, à une variable, non nuls, de degré exactement $d \leq D$, de hauteur usuelle majorée par H, irréductibles dans $\mathbf{Z}[X]$ (donc les coefficients sont premiers entre eux dans leur ensemble) et dont le coefficient dominant est positif. Un polynôme P de $\mathcal{P}_{d,H}$ s'écrit :

$$P(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$$

avec $a_i \in \mathbf{Z}$, $|a_i| \leq H$, $\forall i \in \{1,\ldots,d\}$, $\text{pgcd}(a_0,\ldots,a_d) = 1$, $1 \leq a_0 \leq H$.

Pour tout élément α de $A_{D,H}$, il existe un entier $d \leq D$, tel que $\alpha \in \mathcal{A}_{d,H}$, et tout α de $\mathcal{A}_{d,H}$ est un zéro d'un polynôme P de $\mathcal{P}_{d,H}$. (Les $d-1$ autres zéros de P sont les conjugués de α.) Inversement, tout zéro d'un polynôme de $\mathcal{P}_{d,H}$ est un élément de $\mathcal{A}_{d,H}$. On a donc

$$A_{D,H} = \bigcup_{1\leq d\leq D} \mathcal{A}_{d,H}\,,$$

et comme cette union est disjointe, et que tout polynôme de $\mathcal{P}_{d,H}$ possède d racines distinctes,

$$\mathrm{card}(A_{D,H}) = \sum_{d=1}^{D} \mathrm{card}(\mathcal{A}_{d,H}) \tag{1.12}$$

et

$$\mathrm{card}(\mathcal{A}_{d,H}) = d\,\mathrm{card}(\mathcal{P}_{d,H})\,, \quad \forall d \in \{1,\dots,D\}. \tag{1.13}$$

Lemme 2. *Encadrement du cardinal de $A_{D,H}$.*

Pour tout entier $D \geq 1$ et tout nombre réel $H \geq 1$, on a

$$\mathrm{card}(A_{D,H}) \leq DH(2H+1)^D;$$

pour tout entier $D \geq 2$ et tout nombre réel $H \geq 2$,

$$\frac{D}{8}(H-2)^{D+1} < \mathrm{card}(\mathcal{A}_{D,H}) \leq \mathrm{card}(A_{D,H})$$

et pour $D = 1$ et tout nombre réel $H \geq 1$,

$$(H-1)^2 < \mathrm{card}(\mathcal{A}_{1,H}) = \mathrm{card}(A_{1,H}).$$

1.3.1 Démonstration du lemme 2.

Majoration de $\mathrm{card}(A_{D,H})$**.**

On fixe $D \geq 1$ et $H \geq 1$.

Comme l'union $\bigcup_{1\leq d\leq D} \mathcal{P}_{d,H}$ est disjointe, en utilisant (1.12) et (1.13), on a

$$\mathrm{card}(A_{D,H}) = \sum_{d=1}^{D} d\,\mathrm{card}(\mathcal{P}_{d,H}) \leq D\sum_{d=1}^{D} \mathrm{card}(\mathcal{P}_{d,H}) = D\,\mathrm{card}(\bigcup_{1\leq d\leq D} \mathcal{P}_{d,H}).$$

Or le cardinal de $\bigcup_{1\leq d\leq D} \mathcal{P}_{d,H}$ est inférieur au nombre de polynômes $Q \in \mathbf{Z}[X]$ qui s'écrivent

$$Q(X) = a_0X^D + a_1X^{D-1} + \cdots + a_D$$

avec $|a_i| \leq H$ pour tout $i \in \{1,\dots,D\}$, de coefficient dominant strictement positif et inférieur ou égal à H.

Comme il existe $[H]$ nombres entiers > 0 de valeur absolue inférieure ou égale à H, il y a autant de choix pour le coefficient dominant, et $2[H]+1$ pour les D autres coefficients (éventuellement nuls). On en déduit qu'il existe $[H](2[H]+1)^D$ tels polynômes Q, et

$$\mathrm{card}(A_{D,H}) \leq DH(2H+1)^D.$$

Minoration de $\mathrm{card}(A_{D,H})$**.**

Soient D un entier ≥ 1 et H un nombre réel ≥ 0.
D'après (1.12) et (1.13), nous avons

$$\mathrm{card}(A_{D,H}) = \sum_{d=1}^{D} \mathrm{card}(\mathcal{A}_{d,H}) \geq \mathrm{card}(\mathcal{A}_{D,H}) = D\,\mathrm{card}(\mathcal{P}_{D,H}),$$

donc pour minorer le cardinal de $A_{D,H}$, il suffit de minorer celui de $\mathcal{P}_{D,H}$.

Pour $D \geq 2$ et $H \geq 2$, au lieu de considérer l'ensemble $\mathcal{P}_{D,H}$, nous pouvons juste compter les polynômes P de $\mathcal{P}_{D,H}$ tels que $\mathrm{pgcd}(a_0, a_1) = 1$. La condition $\mathrm{pgcd}(a_0, \ldots, a_D) = 1$ est alors automatiquement vérifiée. Parmi ces polynômes-là, nous pouvons encore nous restreindre à ceux qui vérifient le critère d'irréductibilité d'Eisenstein (cf. [La1]) sur l'anneau des entiers $\mathbf{Z}$, pour le nombre premier 2. On rappelle que le polynôme P est 2-Eisenstein sur $\mathbf{Z}$ (et donc irréductible sur $\mathbf{Q}$), si

$$2 \not| a_0, \;\; 2|a_i, \;\; \forall i \in \{1, \ldots, D\} \;\text{ et }\; 4 \not| a_D.$$

On note $\mathcal{E}_{D,H}(2)$ l'ensemble de ces polynômes P. Comme il est inclus dans $\mathcal{P}_{D,H}$, on a

$$\mathrm{card}(\mathcal{A}_{D,H}) \geq D\,\mathrm{card}(\mathcal{E}_{D,H}(2))$$

et nous sommes ramenés à minorer le cardinal de $\mathcal{E}_{D,H}(2)$.

On a

$$\mathrm{card}\{a \in \mathbf{Z}/ \;\; |a| \leq H, \;\; 2|a\} = 2\left[\frac{H}{2}\right] + 1 > H - 1,$$

et

$$\mathrm{card}\{a \in \mathbf{Z}/ \;\; |a| \leq H, \;\; 2|a, \;\; 4 \not| a\} = 2\left[\frac{H+2}{4}\right] > \frac{H-2}{2}.$$

En notant c_H le nombre de couples $(a_0, a_1) \in \mathbf{Z}^2$ tels que

$$1 \leq a_0 \leq H, \;\; |a_1| \leq H, \;\; 2|a_1, \;\; \mathrm{pgcd}(a_0, a_1) = 1,$$

nous obtenons

$$\mathrm{card}(\mathcal{E}_{D,H}(2)) = c_H \left(2\left[\frac{H}{2}\right] + 1\right)^{D-2} \left(2\left[\frac{H+2}{4}\right]\right),$$

et donc (comme $H \geq 2$), une minoration de ce cardinal, en fonction de c_H,

$$\mathrm{card}(\mathcal{E}_{D,H}(2)) > c_H (H-2)^{D-2} \left(\frac{H-2}{2}\right) = \frac{c_H}{2}(H-2)^{D-1}.$$

Il existe $[\frac{H+1}{2}]$ nombres impairs compris entre 1 et H, et $[\frac{H}{2}]$ nombres pairs compris entre 1 et H. En tenant compte du signe de a_1, cela implique que le cardinal de l'ensemble

$$\{(a_0,a_1)\in\mathbf{Z}^2/\ \ 1\leq a_0\leq H,\ \ 0<|a_1|\leq H,\ \ 2\not| a_0,\ \ 2|a_1\}$$

est égal à $2\left[\frac{H+1}{2}\right]\left[\frac{H}{2}\right]$, et nous avons $2\left[\frac{H+1}{2}\right]\left[\frac{H}{2}\right]\geq\frac{H(H-2)}{2}$ (voir les deux cas, pour n entier positif, $2n\leq H<2n+1$ et $2n+1\leq H<2n+2$).

Pour minorer c_H, on tient compte du couple $(1,0)$ et on enlève tous les couples (a_0,a_1) dont le pgcd est divisible par un nombre premier p (on a donc $p\geq 3$ car $2\not| a_0$.) Ici, p désignera toujours un nombre premier. Or, pour un nombre $p\geq 3$ premier, on a

$$\mathrm{card}\{a\in\mathbf{Z}/\ \ 1\leq a\leq H,\ \ 2\not| a,\ \ p|a\}\leq\mathrm{card}\{a\in\mathbf{Z}/\ \ 1\leq a\leq H,\ \ p|a\}=\left[\frac{H}{p}\right]$$

et $\mathrm{card}\{a\in\mathbf{Z}\setminus\{0\}/\ \ |a|\leq H,\ \ 2|a,\ \ p|a\}$ est égal au nombre de $a\in\mathbf{Z}\setminus\{0\}$ tels que $|a|\leq H$ et $2p|a$, c'est-à-dire $2\left[\frac{H}{2p}\right]$ d'où,

$$c_H\geq 1+2\left[\frac{H+1}{2}\right]\left[\frac{H}{2}\right]-\sum_{p\geq 3}2\left[\frac{H}{p}\right]\left[\frac{H}{2p}\right]$$

et donc

$$c_H\geq 1+\frac{H(H-2)}{2}-H^2\sum_{p\geq 3}\frac{1}{p^2}.$$

Comme, pour tout nombre $x\in[0,1[$, on a $-\log(1-x)=\sum_{k\geq 1}\frac{x^k}{k}\geq x$, et que, d'une part, $\zeta(2)=\sum_{k\geq 1}\frac{1}{k^2}=\prod_{p\geq 2}\left(\frac{1}{1-\frac{1}{p^2}}\right)$, et d'autre part, $\zeta(2)=\frac{\pi^2}{6}$, alors

$$\sum_{p\geq 2}\frac{1}{p^2}\leq\sum_{p\geq 2}-\log\left(1-\frac{1}{p^2}\right)=\log(\zeta(2))=\log\left(\frac{\pi^2}{6}\right)\leq\frac{1}{2},$$

$$\text{d'où}\ \ \sum_{p\geq 3}\frac{1}{p^2}\leq\frac{1}{4},$$

et ainsi

$$c_H\geq 1+\frac{H(H-2)}{2}-\frac{H^2}{4}=\frac{(H-2)^2}{4}.$$

On en déduit

$$\mathrm{card}(\mathcal{E}_{D,H}(2))>\frac{1}{8}(H-2)^{D+1},$$

et finalement, pour tout $D\geq 2$ et tout $H\geq 2$,

$$\mathrm{card}(\mathcal{A}_{D,H})>\frac{D}{8}(H-2)^{D+1}.$$

Pour $D = 1$ et tout nombre réel $H \geq 1$, on a $A_{1,H} = \mathcal{A}_{1,H}$ et leur cardinal est égal à celui de l'ensemble des polynômes $P \in \mathbf{Z}[X]$ qui s'écrivent

$$P(X) = aX + b \text{ avec } 1 \leq a \leq H, \ |b| \leq H, \ \text{pgcd}(a, b) = 1.$$

Avec des calculs analogues à ceux faits précédemment, on trouve

$$\text{card}(A_{1,H}) \geq 2\,[H]^2 - \sum_{p \geq 2} \left(\left[\frac{H}{p} \right] 2 \left[\frac{H}{p} \right] \right)$$

et alors

$$\text{card}(A_{1,H}) \geq 2\,[H]^2 - 2\,[H]^2 \sum_{p \geq 2} \frac{1}{p^2} \geq 2\,[H]^2 - 2\,[H]^2\,\frac{1}{2} = [H]^2$$

d'où

$$\text{card}(A_{1,H}) > (H-1)^2.$$

□

1.3.2 Démonstration du lemme 1.

Majoration de $\text{card}(E_{D,N})$**.**

Soient $D \geq 1$ un entier et $N \geq 0$ un nombre réel.

Nous montrons que l'ensemble $E_{D,N}$ est inclus dans l'ensemble $A_{D,H}$ pour $H = 2^{D-1} e^{DN}$. Soit $\alpha \in E_{D,N}$ avec $\deg(\alpha) = d$. On a $d \leq D$ et $h(\alpha) \leq N$. D'après (1.11),

$$\log \mathcal{H}(\alpha) - (d-1) \log 2 \leq d\,h(\alpha) \leq d\,N,$$

et donc

$$\mathcal{H}(\alpha) \leq 2^{d-1}\,e^{dN} \leq 2^{D-1}\,e^{DN},$$

ce qui montre que $\alpha \in A_{D,H'}$ dès que $H' \geq 2^{D-1}\,e^{DN}$.

On a donc $E_{D,N} \subset A_{D,H}$ pour $H = 2^{D-1}\,e^{DN}$ et, en utilisant la majoration obtenue pour le cardinal de $A_{D,H}$ au lemme 2 (on a $H \geq 1$ car $D \geq 1$ et $N \geq 0$), on a

$$\epsilon_{D,N} = \text{card}(E_{D,N}) \leq \text{card}(A_{D,H}) \leq DH(2H+1)^D,$$

c'est-à-dire

$$\epsilon_{D,N} \leq D\,2^{D-1}\,e^{DN} \left(2^D\,e^{DN} + 1\right)^D.$$

Montrons que

$$D\,2^{D-1}\,e^{DN} \left(2^D\,e^{DN} + 1\right)^D \leq e^{D(D+1)(N+1)},$$

ce qui donnera la majoration annoncée. On a

$$D\,2^{D-1}\,e^{DN}\left(2^D\,e^{DN}+1\right)^D = D\,2^{D-1}\,e^{DN}\left((2^D+1)e^{DN}-e^{DN}+1\right)^D$$

$$\leq D\,2^{D-1}\,e^{DN}\left((2^D+1)e^{DN}\right)^D = D\,2^{D-1}(2^D+1)^D\,e^{D(D+1)N}.$$

Il nous suffit donc de montrer que

$$D\,2^{D-1}(2^D+1)^D \leq e^{D(D+1)}.$$

Par récurrence sur D, on montre que

$$\forall D \geq 2, \quad D\,2^{D-1} \leq e^D,$$

et une étude facile de la fonction $x \mapsto e^x - 2^x - 1$, montre que

$$\forall D \geq 2, \quad (2^D+1)^D \leq e^{D^2}.$$

Pour $D = 1$ l'inégalité se montre par un calcul direct.

On en conclut que, pour tout $D \geq 1$ et tout $N \geq 0$, on a

$$\epsilon_{D,N} \leq e^{D(D+1)(N+1)}.$$

Minoration de $\mathrm{card}(E_{D,N})$**.**

Si $D \geq 1$ et $0 \leq N < 1$, alors

$$e^{D(D+1)(N-1)} < 1 \leq \mathrm{card}(E_{D,N}),$$

car l'ensemble $E_{D,N}$ contient 0.

Pour tout entier $D \geq 2$ et tout nombre réel $N \geq 1$, nous montrons que l'ensemble $E_{D,N}$ contient $\mathcal{A}_{D,H}$ pour $H = \frac{e^{DN}}{\sqrt{D+1}}$.

Soit H' un nombre réel positif, et soit $\alpha \in \mathcal{A}_{D,H'}$. Alors $\deg(\alpha) = D$ et $\mathcal{H}(\alpha) \leq H'$. D'aprés l'inégalité (1.10), on a

$$h(\alpha) \leq \frac{1}{D}\log\mathcal{H}(\alpha) + \frac{1}{2D}\log(D+1) \leq \log\left((D+1)^{\frac{1}{2D}}\,H'^{\frac{1}{D}}\right).$$

On en déduit que $\mathcal{A}_{D,H'} \subset E_{D,N}$ dès que $\log((D+1)^{\frac{1}{2D}}\,H'^{\frac{1}{D}}) \leq N$, c'est-à-dire dès que $H' \leq \frac{e^{DN}}{\sqrt{D+1}}$.

Comme $D \geq 2$ et $N \geq 1$, alors $H = \frac{e^{DN}}{\sqrt{D+1}} \geq 2$ et nous pouvons appliquer la minoration obtenue pour le cardinal de $\mathcal{A}_{D,H}$ au lemme 2 :

$$\epsilon_{D,N} = \mathrm{card}(E_{D,N}) \geq \mathrm{card}(\mathcal{A}_{D,H}) > \frac{D}{8}(H-2)^{D+1}.$$

Or, $\frac{e^D}{\sqrt{D+1}} \geq 4$, donc $H \geq 4e^{D(N-1)} \geq 2 + 2e^{D(N-1)}$, d'où $H - 2 \geq 2e^{D(N-1)}$ et

$$\epsilon_{D,N} > \frac{D}{8}\left(2e^{D(N-1)}\right)^{D+1} = D\,2^{D-2}e^{D(D+1)(N-1)},$$

donc

$$\epsilon_{D,N} > e^{D(D+1)(N-1)}.$$

Si α est de degré 1, on a $\alpha = a/b$ avec a et b des entiers, $b \neq 0$ et $\mathrm{pgcd}(a,b) = 1$. On a donc

$$h(\alpha) = \log(H(\alpha)) = \log(\max(|a|,|b|)) = \log(\mathcal{H}(\alpha))$$

et donc, $\forall N \geq 1$, $E_{1,N} = \{\alpha \in \mathbf{Q}/\ h(\alpha) \leq N\} = \{\alpha \in \mathbf{Q}/\ \log(\mathcal{H}(\alpha)) \leq N\}$. On voit que $E_{1,N} \supset A_{1,H'}$ dès que $H' \leq e^N$, donc, en particulier,

$$\epsilon_{1,N} = \mathrm{card}(E_{1,N}) \geq \mathrm{card}(A_{1,H}) > (H-1)^2 \ \text{ pour } \ H = e^N.$$

Comme $N \geq 1$, alors $H = e^N \geq 2e^{N-1} \geq 1 + e^{N-1}$, et on a

$$\epsilon_{1,N} > e^{2(N-1)},$$

ce qui complète la démonstration du lemme 1. □

1.3.3 Autres résultats.

Pour tout entier $d \geq 1$ et tout nombre réel $N \geq 0$, notons $\mathcal{E}_{d,N}$ l'ensemble des nombres algébriques de degré exactement d et de hauteur logarithmique absolue $\leq N$. En utilisant la majoration et la minoration du lemme1, on obtient l'encadrement suivant.

Lemme 3. *Pour tout entier $d \geq 2$ et tout nombre réel $N \geq 0$, le cardinal de $\mathcal{E}_{d,N}$ vérifie*

$$c_1(d,N)e^{d(d+1)N} < \mathrm{card}(\mathcal{E}_{d,N}) < c_2(d,N)e^{d(d+1)N}$$

où $c_1(d,N) = e^{-d(d+1)} - e^{-2dN+d^2-d}$ *et* $c_2(d,N) = (1 - e^{-2d(N+d)})e^{d(d+1)}$.

(Si $d = 1$ et $N \geq 0$, par un calcul simple analogue à celui de la fin de la preuve du lemme 1, on obtient $(e^N - 1)^2 < \mathrm{card}(\mathcal{E}_{1,N}) \leq 2e^{2N} + e^N$.)

Remarquons que pour N fixe et $d \to \infty$, le lemme3 ne donne aucune information au sujet de la minoration (car pour d assez grand $c_1(d,N) < 0$). Par contre, T.Loher [Lo] a le résultat suivant.

Théorème 6. *(Loher)*
Pour tout entier $d \geq 1$, et tout nombre réel $N \geq \frac{1}{d}\log 2$,

$$\mathrm{card}(\mathcal{E}_{d,N}) \geq c_3(d)\, e^{d(d+1)N}$$

où $c_3(d) = \frac{8}{15}(2\sqrt{d+1})^{-(d+1)}$.

Pour d fixe et $N \to \infty$, la minoration du lemme3 donne le même ordre de grandeur que le théorème de Loher, à savoir, $e^{d(d+1)N}$, mais la constante du théorème 6 est meilleure pour tout $d \geq 2$. D'ailleurs, en remarquant que l'ensemble $E_{D,N}$ est la réunion disjointe, pour $d \in \{1, \ldots, D\}$, des ensembles $\mathcal{E}_{d,N}$, on voit que le théorème de Loher implique :

Pour tout entier $D \geq 1$, et tout nombre réel $N \geq \frac{1}{D} \log 2$,

$$\mathrm{card}(E_{D,N}) \geq c_3(D)\, e^{D(D+1)N},$$

ce qui est supérieur à la borne du lemme1, pour tout $D \geq 2$.

Concernant la majoration, W. Schmidt obtient, dans [Sch2] (équation 1.4 p.170), une borne meilleure à celle du lemme 3.

Théorème 7. *(Schmidt)*

Pour tout entier $d \geq 1$, et tout nombre réel $N \geq 0$,

$$\mathrm{card}(\mathcal{E}_{d,N}) \leq 2^{2d^2+14d+11}\, e^{d(d+1)N}.$$

Concernant des estimations asymptotiques en N, il y a deux résultats connus. Pour $d = 1$, Schanuel (cf. [Scha] et aussi [Sch2]) montre que

$$\mathrm{card}(\mathcal{E}_{1,N}) \sim c_5\, e^{2N},$$

et pour $d = 2$, Schmidt montre dans [Sch3], que

$$\mathrm{card}(\mathcal{E}_{2,N}) = \frac{8}{\zeta(3)}\, e^{6N} + O(2Ne^4).$$

Aucune estimation asymptotique concernant le cardinal de $\mathcal{E}_{d,N}$ pour $d \geq 3$, ne semble actuellement connue ([Sch1] p. 27 et [Sch3] p. 346). Néanmoins, D. Masser a remarqué [Ma] qu'un théorème de Chern et Vaaler [Ch-Va] donne le résultat asymptotique en N, suivant.

Théorème 8. *(Chern-Vaaler)*

Pour tout entier $d \geq 1$, il existe un entier N_0 tel que, pour tout $N \geq N_0$, on a

$$\mathrm{card}(\mathcal{E}_{d,N}) \leq c_4(d)\, e^{d(d+1)N}$$

où $c_4(d) = \frac{dV}{2\zeta(d+1)}$
et $V = V(d) = 2^{d+1}(d+1)^D \prod_{k=1}^{D} \frac{(2k)^{d-2k}}{(2k+1)^{d+1-2k}}$ avec $D = \left[\frac{d-1}{2}\right]$.

Le théorème 8 implique le résultat suivant.

Corollaire 1. *(Chern-Vaaler)*

Pour tout entier $D \geq 1$, il existe un entier N_0 tel que, pour tout $N \geq N_0$, on a

$$\mathrm{card}(E_{D,N}) \leq \frac{D^2 2^D (D+1)^{\frac{D}{2}}}{\zeta(D+1)}\, e^{D(D+1)N}.$$

1.4 Construction d'exemples.

Dans cette section, nous construisons la fonction f du théorème 3 et la fonction g du théorème 5.

1.4.1 Construction de la fonction f.

On rappelle que $\epsilon_{D,N} = \text{card}\{\alpha \in \overline{\mathbf{Q}}/\ [\mathbf{Q}(\alpha) : \mathbf{Q}] \leq D,\ \ h(\alpha) \leq N\}$.

Soit ϕ une fonction positive telle que $\phi(x)/x$ tende vers 0 quand $x \to \infty$.

Nous nous donnons une suite $(b_k)_{k\geq 1}$ de nombres réels > 0 telle que la série $\sum_{k\geq 1} b_k$ soit convergente, et un nombre réel $x_0 \geq 1$, tel que pour tout nombre réel $x \geq x_0$,

$$\phi(x) \leq x - 1. \tag{1.14}$$

Nous allons construire, récursivement, une suite strictement croissante $(N_\delta)_{\delta\geq 1}$ de nombres réels $\geq x_0$ tendant vers l'infini et une suite $(a_\delta)_{\delta\geq 1}$ de nombres rationnels vérifiant les conditions suivantes.

i) Pour une infinité de δ, on a $a_\delta \neq 0$ et pour tout $\delta \geq 1$,

$$|a_\delta| \leq b_\delta \left(\delta + e^{\delta N_\delta}\right)^{-\delta \epsilon_{\delta, N_\delta}}. \tag{1.15}$$

ii) Pour tout $\delta \geq 2$,

$$N_\delta \geq 2\left(\log(\delta - 1) + \sum_{k=1}^{\delta-1} h(a_k) + (\delta-1)^2\, \epsilon_{\delta-1, N_{\delta-1}} (\log 2 + 1 + N_{\delta-1})\right). \tag{1.16}$$

iii) Pour tout $\delta \geq 2$,

$$\frac{N_\delta}{\phi(N_\delta)} \geq 2(\delta-1)^2\, \epsilon_{\delta-1, N_{\delta-1}}. \tag{1.17}$$

Pour la suite $(b_k)_{k\geq 1}$ on pourrait prendre, par exemple, $b_k = 2^{-k},\ \ \forall k \geq 1$.

Pour construire $(a_\delta, N_\delta)_{\delta\geq 1}$, on procède de la façon suivante.

On pose $N_1 = [x_0] + 1,\ \ c_1 = 1 + \left[2(1 + e^{N_1})^{\epsilon_{1,N_1}}\right]$, et $a_1 = \frac{1}{c_1}$.

Soit $\delta \geq 2$. Pour $1 \leq k \leq \delta - 1$, on suppose définis a_k et N_k vérifiant, pour $k \in \{1, \ldots, \delta - 1\}$,

$$|a_k| \leq b_k \left(k + e^{kN_k}\right)^{-\epsilon_{k,N_k}},$$

et pour $k \in \{2, \ldots, \delta - 1\}$,

$$N_k \geq 2\left(\log(k-1) + \sum_{r=1}^{k-1} h(a_r) + (k-1)^2\, \epsilon_{k-1, N_{k-1}} (\log 2 + 1 + N_{k-1})\right)$$

et

$$\frac{N_k}{\phi(N_k)} \geq 2(k-1)^2\, \epsilon_{k-1,N_{k-1}}.$$

(Remarquer que la dernière inégalité est possible puisque la fonction $\phi(x)/x$ tend vers 0 quand x tend vers l'infini.)

On choisit pour N_δ un nombre réel vérifiant les conditions (1.16) et (1.17), et on pose $c_\delta = 1 + \left[2^\delta(\delta + e^{\delta N_\delta})^{\epsilon_{\delta,N_\delta}}\right]$ et $a_\delta = c_\delta^{-1}$.

Il est clair que les a_δ peuvent être choisis de façon à ce que tous (à partir d'un ceratin rang) soient non nuls.

Ainsi, la suite $(a_\delta, N_\delta)_{\delta\geq 1}$ satisfait les conditions (1.15), (1.16) et (1.17). En particulier, la condition (1.16) implique que la suite $(N_\delta)_{\delta\geq 1}$ est strictement croissante et tend vers l'infini.

On pose, pour tout $k \geq 1$,

$$P_k(X) = \prod_{\beta\in E_{k,N_k}} (X-\beta)^k.$$

On définit la fonction f en posant, pour tout $z \in \mathbf{C}$,

$$f(z) = \sum_{k\geq 1} a_k P_k(z).$$

Pour démontrer le théorème 3, nous aurons besoin des lemmes suivants.

Lemme 4. *La fonction f est une fonction entière et transcendante sur $\mathbf{C}(z)$.*

Démonstration du lemme 4.

Soient $R > 0$ et $z \in \overline{D(0,R)}$. Nous écrivons la série

$$\sum_{k\geq 1} a_k P_k(z) = \sum_{k=1}^{[R]} a_k P_k(z) + \sum_{k\geq [R]+1} a_k P_k(z).$$

La première somme est finie et définit un polynôme. Nous regardons donc la deuxième. Pour tout $k \geq [R]+1$, nous avons

$$|a_k P_k(z)| = |a_k| \prod_{\alpha\in E_{k,N_k}} |z-\alpha|^k \leq |a_k| \prod_{\alpha\in E_{k,N_k}} (|z|+|\alpha|)^k.$$

Pour $\alpha \in E_{k,N_k}$, nous avons $|\alpha| \leq M(\alpha) = e^{\deg(\alpha)h(\alpha)} \leq e^{kN_k}$, et donc

$$|a_k P_k(z)| \leq |a_k| \prod_{\alpha\in E_{k,N_k}} (|z| + e^{kN_k})^k.$$

Or $|z| \leq R \leq k$, donc

$$|a_k P_k(z)| \leq |a_k| \left(k + e^{kN_k}\right)^{k\epsilon_{k,N_k}},$$

et, d'après la condition (1.15) sur la suite $(a_\delta)_{\delta \geq 1}$,

$$|a_k P_k(z)| \leq b_k.$$

Comme la série $\sum b_k$ est convergente, ceci montre que la série $\sum_{k\geq 1} a_k P_k(z)$ converge normalement sur tout compact de $\mathbf{C}$; sa limite f est une fonction holomorphe sur $\mathbf{C}$ tout entier.

Montrons maintenant que la fonction f n'est pas polynômiale ; comme elle est entière, cela montrera qu'elle est transcendante.

Supposons que f est un polynôme de degré $n \geq 1$.

Comme la suite $(\epsilon_{k,N_k})_{k\geq 1}$ est strictement croissante, il existe $k_0 \geq 1$, tel que pour tout $k \geq k_0$, $(k-1)\epsilon_{k-1,N_{k-1}} \geq n$.

Soit $K \geq k_0$ tel que $a_{K-1} \neq 0$ et considérons la somme

$$g_K(z) = \sum_{k=1}^{K-1} a_k P_k(z).$$

C'est un polynôme de degré $(K-1)\epsilon_{K-1,N_{K-1}} \geq n$. La différence

$$f(z) - g_K(z) = \sum_{k\geq K} a_k P_k(z)$$

est un polynôme de degré $\leq \max\{(K-1)\epsilon_{K-1,N_{K-1}}, n\} = (K-1)\epsilon_{K-1,N_{K-1}}$. Or, pour tout $k \geq K$, le polynôme P_k est multiple de P_K, donc $f(z) - g_K(z)$ s'annule en tous les zéros de P_K, c'est-à-dire, en $K\epsilon_{K,N_K}$ points.

Comme le polynôme $f(z) - g_K(z)$ est de degré $\leq (K-1)\epsilon_{K-1,N_{K-1}} < K\epsilon_{K,N_K}$, c'est le polynôme nul, et donc

$$-a_K P_K(z) = \sum_{k\geq K+1} a_k P_k(z).$$

Soit $z_0 \in E_{K+1,N_{K+1}} \setminus E_{K,N_K}$. Alors

$$\forall k \geq K+1, \;\; P_k(z_0) = 0 \;\text{ et }\; P_K(z_0) \neq 0.$$

Nous en concluons que, pour tout $K \geq k_0$, on a $a_K = 0$, ce qui contredit la condition i). □

Lemme 5. *Pour tout entier naturel σ, la fonction dérivée $f^{(\sigma)}$ envoie tout nombre algébrique α, dans $\mathbf{Q}(\alpha)$.*

En particulier, si α est un nombre algébrique,

$$f(\alpha) \in \overline{\mathbf{Q}} \;\text{ et }\; [\mathbf{Q}(\alpha, f(\alpha)) : \mathbf{Q}] = \deg(\alpha).$$

Démonstration du lemme 5.

Soient $\alpha \in \overline{\mathbf{Q}}$ et $\sigma \in \mathbf{N}$.

Par hypothèse, la suite $(N_\delta)_{\delta \geq 1}$ tend vers l'infini, donc

$$\overline{\mathbf{Q}} = \bigcup_{k \geq 1} E_{k,N_k},$$

et comme les ensembles $(E_{k,N_k})_{k\geq 1}$ forment une suite croissante pour l'inclusion, il existe $k' \geq 1$ tel que, pour tout $k \geq k'$, $\alpha \in E_{k,N_k}$.

Notons $k_0 = \min\{k' \geq 1/ \ \forall k \geq k', \ \alpha \in E_{k,N_k}\}$ et $M = \max\{k_0, \sigma + 1\}$.

Si $M = 1$ (i.e. $\sigma = 0$ et $k_0 = 1$), alors $f(\alpha) = 0$.

Si $M > 1$, pour tout $k \geq M$, on a $\alpha \in E_{k,N_k}$ et $k > \sigma$. Or, pour tout $k \geq 1$, le polynôme P_k est défini par :

$$P_k(X) = \prod_{\beta \in E_{k,N_k}} (X - \beta)^k,$$

donc, pour tout $k \geq M$, $P_k^{(\sigma)}(\alpha) = 0$ et

$$f^{(\sigma)}(\alpha) = \sum_{k=1}^{M-1} a_k P_k^{(\sigma)}(\alpha).$$

De plus, les polynômes P_k sont des puissances de polynômes unitaires dont les ensembles de zéros sont des réunions de systèmes complets de conjugués sur $\mathbf{Q}$, ils sont donc fixés par tout élément du groupe de Galois de $\overline{\mathbf{Q}}$ sur $\mathbf{Q}$. Ils sont donc à coefficients rationnels, ainsi que tous leurs polynômes dérivés, et comme, par définition, les nombres a_k sont aussi rationnels,

$$f^{(\sigma)}(\alpha) \in \mathbf{Q}(\alpha).$$

□

Lemme 6. *Pour tout entier $D \geq 1$ et tout nombre réel $N \geq 0$, nous avons*

$$\text{card}\left(E_{D,N} \cap \overline{D(0,1)}\right) \geq \frac{1}{2}\text{card}(E_{D,N}).$$

Démonstration du lemme 6.

Soient D un entier positif et N un nombre réel positif ou nul.

Pour un nombre algébrique α non nul, on a

$$\deg(\alpha) = \deg\left(\frac{1}{\alpha}\right) \ \text{ et } \ h(\alpha) = h\left(\frac{1}{\alpha}\right),$$

donc

$$\alpha \in E_{D,N} \Leftrightarrow \frac{1}{\alpha} \in E_{D,N};$$

et, de plus,

$$\alpha \in \overline{D(0,1)} \Leftrightarrow \frac{1}{\alpha} \notin D(0,1).$$

D'où

$$\mathrm{card}(E_{D,N} \cap \overline{D(0,1)}) = \mathrm{card}(E_{D,N} \setminus D(0,1)) + 1,$$

et donc

$$\begin{aligned} \mathrm{card}(E_{D,N}) &= \mathrm{card}(E_{D,N} \cap \overline{D(0,1)}) + \mathrm{card}(E_{D,N} \setminus D(0,1)) \\ &\leq 2\,\mathrm{card}(E_{D,N} \cap \overline{D(0,1)}), \end{aligned}$$

ce qui démontre le lemme. □

Démonstration du théorème 3.

Soient D et d des entiers tels que $d \geq D \geq 1$.

Nous commençons par remarquer que, d'après le lemme 5,

$$\Sigma_{D,N_d}(f,1) = \{\alpha \in \overline{\mathbf{Q}} \cap \overline{D(0,1)} / \ \deg(\alpha) \leq D, \ \ h(\alpha) \leq N_d, \ \ h(f(\alpha)) \leq N_d\}.$$

Montrons que cet ensemble contient $E_{D,\phi(N_d)+1} \cap \overline{D(0,1)}$.

Soit $\alpha \in \overline{\mathbf{Q}}$ tel que

$$\deg(\alpha) \leq d \ \text{ et } \ h(\alpha) \leq \phi(N_d) + 1.$$

Comme $N_d \geq x_0$, alors, d'après (1.14), $\phi(N_d) \leq N_d - 1$, et $h(\alpha) \leq N_d$. Comme, en plus, $\deg(\alpha) \leq d$, alors $\alpha \in E_{d,N_d}$ et $\forall k \geq d, \ \ P_k(\alpha) = 0$.

Si $d = D = 1$, alors $f(\alpha) = 0$ et on a l'inclusion $E_{1,\phi(N_1)+1} \cap \overline{D(0,1)} \subset \Sigma_{1,N_1}(f,1)$.

Supposons maintenant que $d \geq D \geq 1$ et $d \geq 2$. Alors

$$f(\alpha) = \sum_{k=1}^{d-1} a_k P_k(\alpha).$$

Majorons sa hauteur. En appliquant les formules (1.7), puis (1.5), on obtient

$$h(f(\alpha)) = h\left(\sum_{k=1}^{d-1} a_k P_k(\alpha)\right) \leq \log(d-1) + \sum_{k=1}^{d-1} h(a_k P_k(\alpha))$$

$$\leq \log(d-1) + \sum_{k=1}^{d-1} h(a_k) + \sum_{k=1}^{d-1} h(P_k(\alpha)).$$

On pose $A_{d-1} = \sum_{k=1}^{d-1} h(a_k)$.

Soit $k \in \{1, \ldots, d-1\}$. Nous avons

$$P_k(\alpha) = \prod_{\beta \in E_{k,N_k}} (\alpha - \beta)^k.$$

En utilisant les formules (1.5) et (1.6), on obtient

$$h(P_k(\alpha)) \leq k \sum_{\beta \in E_{k,N_k}} h(\alpha - \beta) \leq k \sum_{\beta \in E_{k,N_k}} (\log 2 + h(\alpha) + h(\beta)),$$

et comme, pour tout $\beta \in E_{k,N_k}$, on a $h(\beta) \leq N_k$, et que, par hypothèse, $h(\alpha) \leq \phi(N_d) + 1$, alors

$$h(P_k(\alpha)) \leq k\, \epsilon_{k,N_k} (\log 2 + \phi(N_d) + 1 + N_k).$$

D'où

$$h(f(\alpha)) \leq \log(d-1) + A_{d-1} + \sum_{k=1}^{d-1} k\, \epsilon_{k,N_k} (\log 2 + \phi(N_d) + 1 + N_k).$$

Or, les suites $(N_k)_{k\geq 1}$ et $(\epsilon_{k,N_k})_{k\geq 1}$ sont croissantes, donc $h(f(\alpha))$ est inférieure à

$$\log(d-1) + A_{d-1} + (d-1)^2 \epsilon_{d-1,N_{d-1}} (\log 2 + \phi(N_d) + 1 + N_{d-1}) =$$

$$\phi(N_d) \left((d-1)^2 \epsilon_{d-1,N_{d-1}}\right) + \log(d-1) + A_{d-1} + (d-1)^2 \epsilon_{d-1,N_{d-1}} (\log 2 + 1 + N_{d-1})$$

ce qui est $\leq N_d$, d'après les conditions (1.16) et (1.17).

En particulier, si $\alpha \in E_{D,\phi(N_d)+1} \cap \overline{D(0,1)}$, alors $\deg(\alpha) \leq D < d$ et $h(f(\alpha)) \leq N_d$, ce qui montre que $\alpha \in \Sigma_{D,N_d}(f,1)$.

Ainsi, pour tous $d \geq D \geq 1$, nous avons

$$\sigma_{D,N_d} = \operatorname{card}(\Sigma_{D,N_d}(f,1)) \geq \operatorname{card}(E_{D,\phi(N_d)+1} \cap \overline{D(0,1)}).$$

En appliquant le lemme 6 et le lemme 1, nous obtenons

$$\sigma_{D,N_d} \geq \frac{1}{2} \operatorname{card}(E_{D,\phi(N_d)+1}) > \frac{1}{2}\, e^{D(D+1)\phi(N_d)}.$$

□

Remarque 2. *La démonstration se simplifie considérablement si on se contente de construire f entière et transcendante vérifiant (1.2). Il suffit de se donner une suite strictement croissante $(N_\delta)_{\delta\geq 1}$ de nombres réels ≥ 1 tendant vers l'infini et une suite $(a_\delta)_{\delta\geq 1}$ de nombres rationnels vérifiant la condition i).*

1.4.2 Construction de la fonction g.

On se donne une suite $(N_k)_{k\geq 1}$ de nombres réels ≥ 1 et une suite $(b_k)_{k\geq 1}$ de nombres rationnels tels que :

i) pour une infinité de $k \geq 1$, $b_k \neq 0$,

ii) pour tout $k \geq 1$, on ait $|b_k| \leq 2^{-k}(k + e^{kN_k})^{-k\epsilon_{k,N_k}}$,

iii) pour tout $k \geq 1$,

$$b_k \in \mathbf{Z}\left[\frac{1}{2}\right]. \tag{1.18}$$

(Comme $\mathbf{Z}\left[\frac{1}{2}\right]$ est dense dans $\mathbf{Q}$, ceci est possible.)

On pose, pour tout $k \geq 1$,

$$Q_k(X) = \prod_{\beta \in E_{k,N_k}} P_\beta(X)^k,$$

où P_β est le polynôme minimal de β sur $\mathbf{Z}$, et, pour tout $z \in \mathbf{C}$,

$$g(z) = \sum_{k\geq 1} b_k Q_k(z).$$

Les lemmes suivants démontrent le théorème 5.

Lemme 7. *La fonction g est entière et transcendante.*

La démonstration est identique à celle du lemme 4.

Lemme 8. *Pour tout entier naturel σ, la fonction dérivée $g^{(\sigma)}$ envoie tout $\alpha \in \overline{\mathbf{Q}}$, dans $\mathbf{Z}\left[\frac{1}{2}, \alpha\right]$.*

Démonstration du lemme 8.

Cette démonstration suit celle du lemme 5.

Soient $\alpha \in \overline{\mathbf{Q}} = \bigcup_{k\geq 1} E_{k,N_k}$ et $\sigma \in \mathbf{N}$.

Il existe un nombre entier $M \geq 1$, tel que, pour tout $k \geq M$, on ait $\alpha \in E_{k,N_k}$ et $k > \alpha$, donc $Q_k^{(\sigma)}(\alpha) = 0$ et

$$g^{(\sigma)}(\alpha) = \sum_{k=1}^{M-1} b_k Q_k^{(\sigma)}(\alpha).$$

Comme les polynômes Q_k sont à coefficients dans $\mathbf{Z}$ et que, de plus, d'après la condition (1.18), pour tout $k \geq 1$, $b_k \in \mathbf{Z}\left[\frac{1}{2}\right]$, donc

$$g^{(\sigma)}(\alpha) \in \mathbf{Z}\left[\frac{1}{2}, \alpha\right],$$

ce qui démontre le lemme 8 et donc le théorème 5. □

Remarque 3. *Si on se donne une fonction ϕ comme au théorème 3 et les suites (N_k) et (b_k) intervenant dans la fonction g vérifient de plus les conditions (1.16) (avec (b_k) à la place de (a_k)) et (1.17), alors la fonction g ainsi obtenue satisfait de plus la conclusion (1.3) du théorème 3.*

1.5 Démonstration du théorème 2.

1.5.1 Schéma de démonstration.

La démonstration peut se faire par l'absurde.

On suppose qu'il existe un entier $D \geq 1$ et un entier $N_0 \geq 1$ suffisamment grand tels que, pour tout $N \geq N_0$, on ait

$$\mathrm{card}(\Sigma_{D,N}(f_1, \ldots, f_t)) \geq \gamma\, D^{a(t)} N^{b(t)}.$$

Pour tout $N \geq N_0$, on commence par extraire de $\Sigma_{D,N}$ un sous-ensemble convenable $S_{D,N}$ dont on connaît exactement le nombre d'éléments.

Le lemme de Siegel nous donne l'existence d'un polynôme P, non nul, à t variables et à coefficients entiers (et dépendant de N_0), tel que

$$P(f_1(\omega), \ldots, f_t(\omega)) = 0, \quad \forall \omega \in S_{D,N_0}.$$

On définit une fonction F sur le disque $\overline{D(0,R)}$ en posant

$$F(z) = P(f_1(z), \ldots, f_t(z)), \quad \forall z \in \overline{D(0,R)}.$$

Ainsi la construction de P entraîne

$$F(\omega) = 0, \quad \forall \omega \in S_{D,N_0}.$$

On montrera, grâce à une récurrence, à l'inégalité de Liouville et à un lemme de Schwarz, qu'on a

$$F(\omega) = 0, \quad \forall \omega \in \bigcup_{N \geq N_0} S_{D,N},$$

ce qui impliquera que F est la fonction nulle et contredira le fait que la fonction f et transcendante. D'où le résultat.

1.5.2 Énoncés préliminaires.

Nous avons besoin de la version suivante du lemme de Siegel [GMW].

Lemme 9. *(Lemme de Siegel)*

Soient $N_1, \ldots, N_\tau$ des entiers positifs. On considère un système linéaire homogène de la forme

$$\sum_{n_1=0}^{N_1-1} \dots \sum_{n_\tau=0}^{N_\tau-1} \alpha_{h,1}^{n_1} \dots \alpha_{h,\tau}^{n_\tau} x_{n_1,\dots,n_\tau} = 0 \qquad (1 \le h \le \mu)$$

où les $\alpha_{h,r}$ sont des nombres algébriques. On pose, pour tout $h \in \{1, \dots, \mu\}$ et pour tout $r \in \{1, \dots, \tau\}$,

$$K_h = \mathbf{Q}(\alpha_{h,1}, \dots, \alpha_{h,\tau}),$$

$$d_h = [K_h : \mathbf{Q}], \quad D = \sum_{1 \le h \le \mu} d_h, \quad L = \prod_{1 \le r \le \tau} N_r.$$

Pour $L > D$, ce système possède une solution

$$x_n = x_{n_1,\dots,n_\tau} \quad (0 \le n_r < N_r, \ 1 \le r \le \tau),$$

où les x_n sont des entiers rationnels non tous nuls qui vérifient, pour tout $n = (n_1, \dots, n_\tau)$,

$$|x_n| \le \left[\left(2^{\mu'} \prod_{1 \le h \le \mu} M_h \right)^{\frac{1}{(L-D)}} \right],$$

avec

$$M_h = L^{d_h} \prod_{1 \le r \le \tau} H(\alpha_{h,r})^{(N_r-1)d_h}$$

et $\mu' (\le \mu)$ désignant le nombre des corps K_h qui n'admettent aucun plongement réel.

Nous aurons besoin aussi du résultat suivant qui est la proposition 3.14 de [W].

Lemme 10. *(Inégalité de Liouville)*

Soient K un corps de nombres de degré D, v une valeur absolue archimédienne de K et l un nombre entier strictement positif. Pour $1 \le i \le l$, soient γ_i des éléments de K. Soit f un polynôme en l variables, à coefficients dans $\mathbf{Z}$, ne s'annulant pas au point $\gamma = (\gamma_i)_{1 \le i \le l}$. On suppose que f à un degré inférieur ou égal à N_i par rapport à la variable γ_i.

Alors nous avons l'inégalité suivante

$$\log |f(\gamma)|_v \ge -(D-1) \log L(f) - D \sum_{i=1}^{l} N_i h(\gamma_i).$$

Nous utiliserons plutôt la contraposée de ce lemme, à savoir, si

$$|f(\gamma)|_v < L(f)^{-(D-1)} \prod_{i=1}^{l} H(\gamma_i)^{N_i D},$$

alors $f(\gamma) = 0$.

Pour borner supérieurement la fonction auxiliaire F, nous appliquons le lemme suivant (cf. [W], exercice 4.3).

Lemme 11. *(Lemme de Schwarz)*
Soient $m, \sigma_1, \ldots, \sigma_m$ des entiers strictement positifs et r, R des nombres réels strictement positifs tels que $r \leq R$. Soient $\zeta_1, \ldots, \zeta_m$ des éléments distincts du disque $|\zeta| \leq R$ et F une fonction continue sur le disque fermé $\overline{D(0,R)}$ et holomorphe sur le disque ouvert $D(0,R)$ s'annulant sur chaque ζ_i avec une multiplicité $\geq \sigma_i$ pour $i \in \{1, \ldots, m\}$. Alors

$$|F|_r \leq |F|_R \prod_{i=1}^{m} \left(\frac{R^2 + r|\zeta_i|}{R(r + |\zeta_i|)} \right)^{-\sigma_i}.$$

1.5.3 La démonstration.

Dans cette section, nous noterons $\Sigma_{D,N}$ l'ensemble $\Sigma_{D,N}(f_1, \ldots, f_t, r)$ et $\sigma_{D,N}$ son cardinal.

Choix des paramètres et construction de $S_{D,N}$.

On fixe un entier $D \geq 1$ et un nombre réel $\gamma > \gamma_t$ et on suppose qu'il existe un nombre réel N_0 tel que, pour tout $N \geq N_0$,

$$\sigma_{D,N} \geq \gamma\, D^{a(t)} N^{b(t)}.$$

On pose $T = \left[\frac{c_0 \gamma}{3t} D^{\frac{2}{t-1}} N_0^{\frac{1}{t-1}} \right]$. Comme $b(t) = \frac{t}{t-1}$, quitte à augmenter N_0, on a

$$c_0 \left[\gamma\, D^{a(t)} (N_0 - 1)^{b(t)} \right] >$$

$$D \log 2 + 2tD \log T + T \left(2tN_0 D + \sum_{i=1}^{t} \log \max\{1, |f_i|_R\} \right). \tag{1.19}$$

On pose $u_1 = \log \left(2T^{2t} e^{tN_0 T} \max\{1, |f_1|_R^T\} \ldots \max\{1, |f_t|_R^T\} \right)$. L'inégalité (1.19) s'écrit alors :

$$c_0 \left[\gamma D^{a(t)} (N_0 - 1)^{b(t)} \right] > u_1 + (D-1) \log(2T^{2t}) + tTN_0(D-1) + tTN_0 D. \tag{1.20}$$

Puisque pour tout N, supérieur ou égal à N_0, le cardinal $\sigma_{D,N}$ de l'ensemble $\Sigma_{D,N}$ est supérieur ou égal à $\gamma D^{a(t)} N^{b(t)}$, on peut extraire de $\Sigma_{D,N}$ un sous-ensemble $S_{D,N}$ dont le cardinal $s_{D,N}$ est exactement $\left[\gamma\, D^{a(t)} N^{b(t)}\right]$.

Comme le nombre D sera fixé pour toute la suite, on notera, pour tout $N \geq N_0$,

$$\Sigma_{D,N} = \Sigma_N, \quad \sigma_{D,N} = \sigma_N, \quad S_{D,N} = S_N, \quad s_{D,N} = s_N.$$

Pour $N \geq N_0$, on numérote les éléments de S_N :

$$S_N = \{\omega_1, \omega_2, \ldots, \omega_{s_N}\}.$$

La fonction auxiliaire.

Lemme 12. *Il existe un polynôme $P \in \mathbf{Z}[X_1, \ldots, X_t]$, non nul, de degré en X_i strictement inférieur à T, pour tout $i \in \{1, \ldots, t\}$, tel que*

$$P(f_1(\omega), \ldots, f_t(\omega)) = 0, \quad \forall \omega \in S_{N_0}$$

et dont les coefficients sont majorés en valeur absolue par $2T^t e^{tTN_0}$.

Démonstration du lemme 12.

Nous allons appliquer le lemme 9. On écrit le polynôme cherché sous la forme

$$P(X_1, \ldots, X_t) = \sum_{i_1=0}^{T-1} \cdots \sum_{i_t=0}^{T-1} c_{i_1 \ldots i_t} X_1^{i_1} \ldots X_t^{i_t}.$$

Il s'agit de résoudre dans $\mathbf{Z}$ le système linéaire homogène suivant :

$$\sum_{i_1=0}^{T-1} \cdots \sum_{i_t=0}^{T-1} c_{i_1,\ldots,i_t} f_1(\omega_k)^{i_1} \ldots f_t(\omega_k)^{i_t} = 0, \quad \forall k \in \{1, \ldots, s_{N_0}\}.$$

On applique le lemme 9 en posant :

$$\tau = t, \quad N_1 = \ldots = N_t = T, \quad \mu = s_{N_0}, \quad L = T^t,$$

$$\{\alpha_{h,1}, \ldots, \alpha_{h,\tau}\}_{h=1,\ldots,\mu} = \{f_1(\omega_k), \ldots, f_t(\omega_k)\}_{k=1,\ldots,s_{N_0}},$$

et, pour $k \in \{1, \ldots, s_{N_0}\}$,

$$d_k = [\mathbf{Q}(f_1(\omega_k), \ldots, f_t(\omega_k)) : \mathbf{Q}].$$

Comme $\gamma > \gamma_t$, et $t \geq 2$, d'après (1.1), nous avons $2\gamma < \left(\frac{c_0\gamma}{3t}\right)^t$ et, quitte à augmenter N_0, T vérifie

$$2\,\gamma\, D^{\frac{2t}{t-1}} N_0^{\frac{t}{t-1}} < T^t \leq \left(\frac{c_0\gamma}{3t}\right)^t D^{\frac{2t}{t-1}}\, N_0^{\frac{t}{t-1}}, \tag{1.21}$$

et l'hypothèse $L > \sum_{h=1}^{\mu} d_h$ est satisfaite car

$$\sum_{h=1}^{\mu} d_h = \sum_{k=1}^{s_{N_0}} d_k \leq s_{N_0} D \leq \gamma\, D^{\frac{2t}{t-1}}\, N_0^{\frac{t}{t-1}} < T^t.$$

Le système possède donc une solution

$$c = (c_{i_1,\ldots,i_t})_{0\leq i_1,\ldots,i_t\leq T-1}$$

où les $c_{i_1,\ldots,i_t}$ sont des entiers rationnels non tous nuls qui vérifient

$$\max_{0\leq i_1,\ldots,i_t\leq T-1} |c_{i_1,\ldots,i_t}| \leq \left[\left(2^{s_{N_0}} \prod_{k=1}^{s_{N_0}} M_k \right)^{\frac{1}{T^t - s_{N_0} D}} \right]$$

où $M_k = T^{td_k} \prod_{r=1}^{t} H(f_r(\omega_k))^{(T-1)d_k}$.

Comme pour tout $k \in \{1,\ldots,s_{N_0}\}$ on a $d_k \leq D$ et $\omega_k \in S_{N_0}$, alors pour tout $r \in \{1,\ldots,t\}$, on a $H(f_r(\omega_k)) \leq e^{N_0}$, d'où

$$M_k \leq T^{tD} e^{tN_0(T-1)D}$$

et

$$\max_{0\leq i_1,\ldots,i_t\leq T-1} |c_{i_1,\ldots,i_t}| \leq \left(2^{s_{N_0}} T^{tDs_{N_0}} e^{tN_0 TDs_{N_0}}\right)^{\frac{1}{T^t - s_{N_0} D}}.$$

Or $D \geq 1$, $s_{N_0} \geq 1$ et, d'après (1.21), on a $T^t > 2s_{N_0}D$, ce qui conduit à la majoration des $c_{i_1,\ldots,i_t}$

$$\max_{0\leq i_1,i_t\leq T-1} |c_{i_1,\ldots,i_t}| \leq 2\, T^t\, e^{tTN_0}$$

et démontre le lemme. □

On définit une fonction F analytique sur le disque ouvert $D(0,R)$, en posant

$$F(z) = P(f_1(z),\ldots,f_t(z)), \quad \forall z \in D(0,R).$$

La récurrence.

On va montrer, par récurrence, que

$$\forall N \geq N_0,\ \ \forall \omega \in S_{D,N},\ \ F(\omega) = 0.$$

Par construction du polynôme P, on a $F(\omega) = 0$ pour tout $\omega \in S_{N_0}$, et les deux lemmes suivants permettent de conclure.

Lemme 13. *Pour tout $N \geq N_0$, on a*

$$[\forall \omega \in S_{D,N},\ \ F(\omega) = 0] \Rightarrow \left[\forall \omega \in S_{D,N+1},\ \ |F(\omega)| \leq e^{u_1 - c_0 s_N}\right].$$

Lemme 14. *Pour tout $N \geq N_0 + 1$ et tout $\omega \in S_{D,N}$, on a*

$$|F(\omega)| \leq e^{u_1 - c_0 s_{N-1}} \Rightarrow F(\omega) = 0.$$

Démonstration du lemme 13.

On se donne $N \geq N_0$ et on suppose que $F(\omega) = 0$ pour tout $\omega \in S_N$. Nous appliquons à la fonction F le lemme 11 avec :

$$m = s_N, \text{ et, pour chaque } i \in \{1, \ldots, s_N\},\ \ \sigma_i = 1 \text{ et } \zeta_i = \omega_i.$$

On obtient

$$|F|_r \leq |F|_R \prod_{k=1}^{s_N} \left(\frac{R^2 + r|\omega_k|}{R(r + |\omega_k|)} \right)^{-1}.$$

Or, $\dfrac{R^2 + r|\omega_k|}{R(r + |\omega_k|)} - \dfrac{R^2 + r^2}{2rR} = \dfrac{(R^2 - r^2)(r - |\omega_k|)}{2rR(r + |\omega_k|)} \geq 0$ dès que $|\omega_k| \leq r$,

donc, pour $\omega_k \in S_N$, on a

$$\frac{R^2 + r|\omega_k|}{R(r + |\omega_k|)} \geq \frac{R^2 + r^2}{2rR},$$

et comme $c_0 = \log\left(\frac{R^2+r^2}{2rR}\right)$, alors

$$|F|_r \leq |F|_R \, e^{-c_0 s_N}.$$

De plus, pour tout $z \in \overline{D(0,R)}$, on a

$$F(z) = P(f_1(z), \ldots, f_t(z)) = \sum_{i_1=0}^{T-1} \cdots \sum_{i_t=0}^{T-1} c_{i_1,\ldots,i_t} \, f_1(z)^{i_1} \ldots f_t(z)^{i_t},$$

et on peut donc majorer le module de $F(z)$ en s'aidant de la borne obtenue pour les coefficients $c_{i_1,\ldots,i_t}$ au lemme 12 :

$$|F(z)| \leq T^t \max_{0 \leq i_1,\ldots,i_t \leq T-1} \{|c_{i_1,\ldots,i_t}|\} \, |f_1|_R^T \ldots |f_t|_R^T$$

$$\leq 2\, T^{2t} \, e^{tTN_0} \max\{1, |f_1|_R^T\} \ldots \max\{1, |f_t|_R^T\}.$$

Comme $u_1 = \log\left(2\, T^{2t} \, e^{tTN_0} |f_1|_R^T \ldots |f_t|_R^T\right)$, alors $|F|_R \leq e^{u_1}$ et

$$\max_{|z| \leq r} |F(z)| = |F|_r \leq e^{u_1 - c_0 s_N}.$$

En particulier, tout $\omega \in S_{N+1}$ est de module $\leq r$, donc $|F(\omega)| \leq e^{u_1 - c_0 s_N}$, ce qui démontre le lemme 13. □

Démonstration du lemme 14.

On se donne $N \geq N_0 + 1$, $\omega \in S_N$, et on suppose que

$$|F(\omega)| \leq e^{u_1 - c_0 s_{N-1}}.$$

Comme $s_{N-1} = [\gamma D^{a(t)}(N-1)^{b(t)}]$, et qu'au paragraphe 1.5.3 nous avons supposé que N_0 vérifiait (1.20), alors N vérifie :

$$c_0 s_{N-1} > u_1 + (D-1)\log(2T^{2t}) + tTN_0(D-1) + tTND. \tag{1.22}$$

D'autre part, le lemme 12 nous a donné un majorant pour la longueur du polynôme P, à savoir,

$$L(P) = \sum_{i_1=1}^{T-1} \cdots \sum_{i_t=1}^{T-1} |c_{i_1,\ldots,i_t}| \leq T^t \max_{0 \leq i_1,\ldots,i_t \leq T-1} \{|c_{i_1,\ldots,i_t}|\} \leq 2T^{2t} e^{tTN_0},$$

et comme $\omega \in S_N$, on a

$$H(f_r(\omega)) \leq e^N, \ \ \forall r \in \{1, \ldots, t\}$$

et donc l'inégalité (1.22) donne

$$e^{u_1 - c_0 s_{N-1}} < L(P)^{-(D-1)} \prod_{r=1}^{t} H(f_r(\omega))^{-DT}.$$

D'après l'hypothèse, on a donc

$$|F(\omega)| < L(P)^{-(D-1)} \prod_{r=1}^{t} H(f_r(\omega))^{-DT}.$$

Pour conclure que $F(\omega) = 0$, nous appliquons le lemme 10 en posant :

$$K = \mathbf{Q}(f_1(\omega), \ldots, f_t(\omega)), \ \text{ corps de nombres de degré} \leq D, \ \ |.|_v = |.|,$$

$$l = t, \ \ N_1 = \ldots = N_t = T, \ \ \gamma = (f_1(\omega), \ldots, f_t(\omega)) \ \text{ et } \ f = P.$$

On en conclut que $P(f_1(\omega), \ldots, f_t(\omega)) = 0$, i.e. $F(\omega) = 0$, ce qui démontre le lemme 14 et donc la récurrence. □

Conclusion.

Nous avons montré que pour tout $N \geq N_0$, la fonction F s'annule sur l'ensemble S_N et donc

$$F(\omega) = 0, \quad \forall \omega \in \bigcup_{N \geq N_0} S_N. \tag{1.23}$$

Les ensembles S_N sont tous inclus dans le compact $\overline{D(0,r)}$ et la fonction F est holomorphe sur l'ouvert $D(0,R)$ qui contient $\overline{D(0,r)}$. De plus, F n'est pas la fonction identiquement nulle car elle est définie comme étant la valeur de $P \in \mathbf{Z}[X_1, \ldots, X_t]$ au point $(f_1(z), \ldots, f_t(z))$ où les f_i sont des fonctions algébriquement indépendantes sur $\mathbf{Q}$. Ainsi F ne peut pas s'annuler sur une infinité de points de $\overline{D(0,r)}$, et donc en particulier sur $\bigcup_{N \geq N_0} S_N$.

Ceci démontre que (1.23) contredit le théorème sur les zéros isolés d'une fonction holomorphe et nous donne le résultat cherché. □

Bibliographie

[Ch-Va] Chern, S., Vaaler, J.D., *The distribution of values of Mahler's measure*, Journal für die reine und angewandte Mathematik 540 (2001) 1-47.

[Elk] Elkies, N.D., *Rational points near curves and small nonzero $|x^3-y^2|$ via lattice reduction*, Algorithmic number theory (Leiden, 2000), Lectures Notes in Comput. Sci., 1838, Springer, Berlin, 2000, 33-63.

[Fa] Faber, G., *Über arithmetische Eingenschaften analytischer Funktionen*, Math. Annalen 58 (1904) 545-557.

[Gr] Gramain, F., *Fonctions entières arithmétiques : un aperçu historique*, Pub. IRMA-Lille, Vol.VI -Fasc.2 -n.1, 1984.

[GMW] Gramain, F., Mignotte, M. et Waldschmidt,M., *Valeurs algébriques de fonctions analytiques*, Acta Arithmetica XLVII (1986) 97-120.

[La1] Lang, S., *Algebra*, Addison-Wesley Publishing Co., Reading, Mas., London-Don Mills, Ont. 1965.

[La2] Lang, S., *Introduction to transcendental numbers*, Addison-Wesley Publishing Co., Reading, Mas., London-Don Mills, Ont. 1966.

[Lo] Loher, T., *Counting points of bounded height*, Inauguraldissertation, Basel, 2001.

[Mah] Mahler, K., *Lectures on transcendental numbers*, Lectures Notes on Mathematics 546, Springer-Verlag, Berlin-Heidelberg-New York, 1976.

[Ma] Masser, D., *Counting algebraic numbers with large height*, Preprint, January 2002.

[NR] Neumann, B.H. et Rado, R., *Monotone functions mapping the set of rational numbers on itself*, J. Austr. Math. Soc. 3 (1963) 282-287.

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

[Sch1] Schmidt, W., *Diophantine Approximations and Diophantine Equations*, Lectures Notes on Mathematics 1467, Springer-Verlag, Berlin-Heidelberg-New York, 1991.

[Sch2] Schmidt, W., *Northcott's Theorem on heights I. A general estimate*, Monats. Math. 115 (1993), 169-181.

[Sch3] Schmidt, W., *Northcott's Theorem on heights II. The quadratic case*, Acta Arith. 70 (1995), 343-375.

[St1] Stäckel, P., *Ueber arithmetische Eingenschaften analytischer Functionen*, Math. Annalen 46 (1895) 513-520.

[St2] Stäckel, P., *Arithmetische Eingenschaften analytischer Functionen*, Acta Math. 25 (1902) 371-383.

[VdP] Van der Poorten, A.J., *Transcendental entire functions mapping every algebraic number field into itself*, J. Austr. Math. Soc. 8 (1968) 192-193.

[W] Waldschmidt, M., *Diophantine approximation on linear algebraic groups : transcendence properties of the exponential function in several variables*, Grundlehren der Mathematischen Wissenschaften 326, Springer-Verlag, Berlin-Heidelberg, 2000.

II

Deuxième partie

Sur la conjecture *abc* et le théorème de Siegel

2.1 Introduction.

L'étude des équations diophantiennes remonte au moins au deuxième millénaire avant notre ère, à l'époque où des mathématiciens à Babylone s'intéressaient aux "triplets Pythagoriciens"

$$X^2 + Y^2 = Z^2.$$

La solution de cette équation a été donnée, sous forme algorithmique, par Diophantus d'Alexandrie, au troisième siècle. On trouve des résultats similaires dans d'autres civilisations comme la Chine et l'Inde.

Plus récemment, au vingtième siècle, le dixième problème posé par Hilbert concernait la totalité des équations de la forme

$$f(\underline{x}) = 0,$$

pour $f \in \mathbf{Q}[X_1, \ldots, X_n]$ un polynôme à coefficients rationnels. La question précise était : étant donnée une telle équation, existe-t-il un algorithme déterminant si ladite équation admet une solution entière ? La réponse à un problème si général étant négative [Mat], nous nous contenterons du cas 2-dimensionnel

$$f(x, y) = 0$$

donnant lieu aux courbes planes, où on sait beaucoup de choses, mais où de nombreuses questions demeurent ouvertes.

Nous pouvons chercher à résoudre de telles équations dans $\mathbf{Z}$ ou dans $\mathbf{Q}$, nous pouvons aussi élargir nos recherches en considérant des solutions entières ou rationnelles dans un corps de nombres. Par exemple, l'équation classique aux unités

$$u + v = 1$$

n'admet pas de solution (u, v) unités de $\mathbf{Z}$; mais si on remplace $\mathbf{Z}$ par l'anneau des entiers d'un corps de nombres, ou bien si on permet un nombre fini de facteurs premiers au dénominateur, la situation est différente. Si on

note S l'ensemble des facteurs premiers autorisés dans les dénominateurs, on obtient ce qu'on appelle des points S-entiers. Un thème central dans ce texte est l'étude du comportement des points S-entiers lorsque l'on augmente S.

Une autre question est la suivante : quand l'équation admet des solutions, sont-elles en nombre fini ? Deux théorèmes de finitude fondamentaux en géométrie diophantienne sont celui de Siegel, concernant les points entiers sur les courbes algébriques, et celui de Faltings, sur les points rationnels.

C. L. Siegel [Si3] démontra, en 1929, que l'ensemble des points entiers d'une courbe algébrique affine non exceptionnelle (i.e. de genre ≥ 1 ou de genre nul et ayant au moins trois points à l'infini) est fini. (Grâce à l'analogue p-adique du théorème de Thue-Siegel démontré par Mahler [Mah1] en 1933, le théorème de Siegel est généralisé aux points ayant leurs dénominateurs dans un ensemble fini S de places.)

Si g désigne le genre de la courbe affine U et s le nombre de points "à l'infini", la caractéristique d'Euler-Poincaré s'écrit $\chi(U) = 2 - 2g - s$. Une courbe affine U vérifie l'hypothèse du théorème de Siegel d'être non exceptionnelle si $\chi(U) < 0$.

Pour les courbes de genre ≥ 2, le théorème de Siegel est contenu dans celui de G. Faltings [Fa] (conjecturé par Mordell en 1922 et démontré en 1983), puisque ce dernier affirme que l'ensemble des points rationnels d'une courbe algébrique de genre ≥ 2 est fini.

Cependant, la question est loin d'être réglée. Un problème d'importance est celui de l'effectivité. Dans quelle mesure sommes-nous capables de dresser la liste de toutes les solutions ?

Pour démontrer son théorème, Siegel appliqua le théorème de Thue-Siegel (respectivement, [Th] en 1909 et [Si1] en 1921) sur l'approximation d'un nombre algébrique par des nombres rationnels, ce qui conduit à des résultats non effectifs, dans le sens où l'on sait borner le nombre de solutions, mais pas les déterminer. Borner la hauteur (i.e. la taille) des solutions, permettrait non seulement de redémontrer la finitude ; mais surtout de déterminer, au moins en théorie, l'ensemble des solutions.

Dans un certain nombre de cas des résultats effectifs ont été obtenus, et ce grâce au théorème de A. Baker [Ba1] (1966) sur les formes linéaires de logarithmes (cf. aussi [BM] chapitre 1 et [Ba3]). En dehors de quelques exemples isolés en genre supérieur ou égal à 2 (pour un historique, cf., par exemple, [BM] chapitre 3), les théorèmes d'effectivité concernent essentiellement les courbes de genre 0 et 1 (cf. [Ba2], [Ba3], [BC] et [Se1] et, pour celles qui sont revêtement galoisien de la droite projective, [Bi], [DZ], [P3]). Borner la hauteur des points (S-)entiers d'une courbe de genre ≥ 2 reste de nos jours un problème ouvert.

En vue d'un moyen d'attaque effectif pour résoudre des équations diophantiennes, regardons la conjecture *abc* de Masser-Oesterlé ([Mas] et [Oe]). Celle-ci, s'énonçant de façon élémentaire, cache une myriade de conséquences

en approximation diophantienne ; elle est souvent citée (cf., par exemple, [GS] et [Wa3]) pour faire le lien entre différents sujets, puisqu'elle est équivalente à des versions fortes d'importants théorèmes en théorie des nombres.

La conjecture *abc* énoncée sur $\mathbf{Q}$ prétend que, pour tout $\varepsilon > 0$, il existe un nombre réel $c_\varepsilon > 0$, tel que, pour tout triplet (a, b, c) d'entiers rationnels premiers entre eux et tels que $a + b = c$, le maximum des valeurs absolues de a, b et c est inférieur ou égal à $c_\varepsilon R^{1+\varepsilon}$, où R désigne le "radical" de abc, c'est-à-dire le produit des nombres premiers divisant abc. Les premiers résultats allant dans le sens de la conjecture *abc* sont dus à R. Tijdeman, C. L. Stewart et K. Yu, et, bien que ces résultats, qui reposent sur des minorations de formes linéaires de logarithmes, soient effectifs, la conjecture reste hors de portée (l'ordre de croissance du majorant est exponentielle au lieu de polynômial). L'analogue dans la théorie des corps de fonctions de la conjecture de Masser et Oesterlé est un théorème de Mason.

N. Elkies [El] propose, en 1991, une approche qui serait effective du théorème de Faltings ; mais celle-ci est conjecturale puisqu'elle se base sur la conjecture de Masser-Oesterlé. (E. Bombieri [Bo2] utilise le même type de démonstration pour prouver que la conjecture *abc* implique le théorème de Roth sur l'approximation diophantienne de nombres algébriques. M. van Frankenhuysen donne une démonstration unifiée de ces deux théorèmes dans [MvF].) Un autre outil utilisé par Elkies dans sa démonstration est le théorème de Belyĭ [Be], qui dit qu'une courbe algébrique est définie sur $\overline{\mathbf{Q}}$ si, et seulement si elle est revêtement de la droite projective, non ramifié en dehors de $0, 1$ et l'infini.

Dans ce travail, nous étudions les liens entre la conjecture *abc* et l'étude de bornes pour la hauteur des points S-entiers de courbes algébriques. Les bornes considérées sont uniformes en l'ensemble de places S. Nous verrons comment, en admettant la conjecture *abc*, nous obtenons des bornes pour la hauteur de points S-entiers pour n'importe quel ensemble S. Un point crucial dans notre approche est le fait de pouvoir faire varier S, puisqu'il nous permet de remonter la démonstration dans l'autre sens, c'est-à-dire d'aller de Siegel uniforme (et effectif) vers *abc*. L'ensemble S joue un rôle important dans ce travail, c'est pourquoi nous mettons souvent l'accent sur la dépendance en S dans les bornes obtenues.

Les outils employés tout le long de cette deuxième partie sont essentiellement la conjecture *abc* (sous diverses versions : conjectures 1, 2 et 3), le théorème de Belyĭ (théorème 12) et la théorie des hauteurs de Weil pour les courbes algébriques, ainsi qu'un peu de théorie analytique des nombres. La géométrie algébrique est présente de façon plus discrète, les prérequis étant relativement élémentaires. Nous faisons usage du théorème de Riemann-Roch pour les courbes et quelques propriétés des schémas sur $\mathbf{Z}$.

En suivant les lignes suggérées par Elkies [El] et en supposant vraie la conjecture *abc* étendue à tout corps de nombres, nous obtenons des bornes

uniformes en S pour les points S-entiers d'une courbe affine U vérifiant les hypothèses du théorème de Siegel, c'est-à-dire telle que $\chi(U) < 0$. Précisément, énonçons la conjecture, et le théorème démontré dans la section 2.3. (La hauteur et le radical sont définis dans la section 2.2.1.)

Conjecture 1. *(abc)*

Étant donné un corps de nombres K et un nombre réel $\varepsilon > 0$, il existe une constante $c_{\varepsilon,K} > 0$ telle que, pour tout triplet (a, b, c) de nombres algébriques dans K, non nuls, tels que $a + b = c$, on ait

$$(1 - \varepsilon)h_K(a : b : c) < \mathrm{rad}_K(a : b : c) + c_{\varepsilon,K}.$$

Théorème 9. *Soient K un corps de nombres, U une courbe algébrique affine définie sur K telle que la caractéristique d'Euler-Poincaré $\chi(U)$ soit strictement négative, S un ensemble fini de places ultramétriques de K et $h_{U,K}$ une fonction hauteur définie sur $U(K)$ associée à un diviseur de degré 1.*

Supposons vraie la conjecture 1.

Pour tout $\varepsilon \in]0, -\chi(U)[$ et tout point S-entier x de U, il existe une constante γ dépendant du corps de nombres K, de la courbe U, du choix de la hauteur $h_{U,K}$ et de ε, mais pas du point x ni de l'ensemble S, telle que

$$h_{U,K}(x) \leq -\frac{1}{\varepsilon + \chi(U)} \sum_{\wp \in S} \log N(\wp) + \gamma.$$

De plus, si la constante $c_{\varepsilon,K}$ de la conjecture 1 était effective, il en serait de même pour γ.

On peut essayer de préciser qu'elle pourrait être la dépendance en K de $c_{\varepsilon,K}$. D.W. Masser [Mas] montre qu'il faut faire apparaître le logarithme de la valeur absolue d_K du discriminant avec un coefficient > 1. En modifiant ainsi la conjecture *abc* (cf. la conjecture 3 pour un énoncé précis), nous démontrons le **théorème 13**, où la borne du théorème 9 est remplacée par :

$$h_{U,K}(x) \leq -\frac{1}{\varepsilon + \chi(U)} \sum_{\wp \in S} \log N(\wp) - \frac{2}{\varepsilon + \chi(U)} \log d_K + \kappa,$$

où la constante κ dépend du degré $[K : \mathbf{Q}]$ du corps de nombres, de la courbe U, du choix de la hauteur $h_{U,K}$ et de ε, mais pas du point x ni du corps K lui même, ni de l'ensemble S.

Dans la section 2.4, nous démontrons une sorte de réciproque de ces deux théorèmes, ce qui montre l'équivalence entre la conjecture *abc* et une version uniforme du théorème de Siegel pour n'importe quelle courbe donnée.

Précisément, étant donnée une courbe affine U définie sur un corps de nombres K telle $\chi(U) < 0$, nous considérons une hypothèse de type "Siegel uniforme" i.e. une borne uniforme en S de ses points S-entiers faisant intervenir aussi le discriminant du corps de nombres.

Hypothèse 1. *Siegel* (U, K)

Pour tout entier naturel $\delta > 0$*, il existe des constantes* $k_1(U, h, \delta) > 1$*,* $k_2(U, h, \delta) > 1$ *et* $k_3(U, h, \delta) > 0$ *telles que, pour toute extension finie* L/K *de degré* $[L : \mathbf{Q}] \leq \delta$*, pour tout sous-ensemble fini* S *de places ultramétriques de* L *et pour tout point* S*-entier* x *de* U*, on a*

$$h_{U,L}(x) \leq k_1 \sum_{\ell \in S} \log N_{L/\mathbf{Q}}(\ell) + k_2 \log d_L + k_3,$$

où d_L *est la valeur absolue du discriminant du corps* L*,* $h_{U,L} = [L : \mathbf{Q}]h_U$ *et* h_U *est une fonction hauteur sur* U*, associée à un diviseur de degré 1.*

L'hypothèse 1 a été inspirée, d'une part, par l'hypothèse de type "Mordell-effectif" formulée par Moret-Bailly dans [M-B] (où il démontre que cette dernière impliquerait la conjecture *abc*) et d'autre part, par l'analogie avec les corps de fonctions, domaine dans lequel on dispose des résultats uniformes et effectifs non conjecturaux (cf. l'appendice).

Pour un corps de nombres K on énonce une variante de la conjecture *abc* dépendant d'une fonction croissante ϕ.

Conjecture 2. *abc* (K, ϕ)

Pour tout triplet (a, b, c) *de nombres algébriques appartenant au corps de nombres* K*, non nuls et tels que* $a + b = c$*, on a*

$$h_K(a : b : c) \leq \phi(\mathrm{rad}_K(a : b : c)).$$

La conjecture 1 correspond à $\phi(x) = (1+\varepsilon)x + c_{\varepsilon,K}$. Le résultat principal de cette section est le suivant :

Théorème 10. *Soient* K *un corps de nombres,* U *une courbe algébrique affine telle que* $\chi(U) < 0$ *définie sur* K *et* h_U *une hauteur définie sur* U *associée à un diviseur de degré 1.*

L'hypothèse Siegel (U, K) *implique la conjecture abc*(K, ϕ) *pour une fonction explicite* ϕ *linéaire en* x*.*

Dans les sections 2.5 et 2.6, nous montrons des versions affaiblies mais non conjecturales des deux énoncés.

Pour un corps de nombres K et une fonction croissante ϕ (dépendant de K), on fait les hypothèses suivantes.

Hypothèse 2. $(u + v = 1)\,(K, \phi)$

Pour tout ensemble fini S *de places ultramétriques de* K *et tout couple* (u, v) *de* S*-unités vérifiant* $u + v = 1$*, on a*

$$\max\{h_K(u), h_K(v)\} \leq \phi\left(\Sigma_S\right).$$

Hypothèse 3. *Siegel* $(\mathbf{P}^1 \setminus \{0,1,\infty\}, K, \phi)$

Pour tout ensemble fini S de places ultramétriques de K et tout point S-entier P de $\mathbf{P}^1 \setminus \{0,1,\infty\}$, on a

$$h_K(P) < \phi\left(\Sigma_S\right).$$

Dans la section 2.5, **théorème 15**, nous montrons que

étant fixés un corps de nombres K et une fonction ϕ croissante, la conjecture 2, l'hypothèse 2 et l'hypothèse 3 sont trois énoncés équivalents.

Le théorème 15 permet de mettre en valeur l'intérêt de considérer des points S-entiers et de mettre l'accent sur la dépendance en S des bornes obtenues. De plus, cet énoncé étant assez souple, il nous permet d'obtenir des théorèmes effectifs à partir de versions faibles de la conjecture *abc*. (Le théorème 9, qui utilise la version plus forte de *abc*, reste à présent sans applications concrètes.)

Le théorème de C. L. Stewart et Kunrui Yu [S-Y] (version très affaiblie mais non conjecturale de *abc*) nous permet alors de déduire du théorème 15, dans la section 2.6, *de nouvelles bornes uniformes en S et effectives pour la hauteur des solutions de l'équation en S-unités $Au + Bv = 1$* (**théorème 18**) et *des points S-entiers de $\mathbf{P}^1 \setminus \{0,1,\infty\}$* (**théorème 20**), dans le cas où le corps de nombres est $\mathbf{Q}$.

Par ailleurs, le théorème de Yu. Bilu [Bi] (version effective du théorème de Siegel pour les courbes qui sont revêtements galoisiens de la droite projective, uniforme en le corps de base et l'ensemble de dénominateurs des points) nous permet, en appliquant le théorème 10, d'étendre le résultat de Stewart et Yu à tout corps de nombres et d'obtenir ainsi le **théorème 17**, qui dit précisément que

pour tout corps de nombres K, la conjecture 2 est vraie pour la fonction $\phi(x) = \exp(\gamma x)$, où γ est un nombre réel dépendant du degré et du discriminant de K, effectivement calculable.

Comme conséquence, *nous étendons les **théorèmes 18** et **20** à tout corps de nombres.*

Pour conclure, rappelons que résoudre l'équation aux S-unités en deux variables ou déterminer les points entiers de $\mathbf{P}^1 \setminus \{0,1,\infty\}$ sont des points clefs auxquels se ramène la recherche de points entiers des équations dites de Thue, superelliptiques et hyperelliptiques (cf., par exemple, [Se1] et le chapitre VI de [La2]). Certainement, les théorèmes 18 et 20 devraient permettre d'obtenir de nouvelles bornes sur ces équations ; cependant, ceci n'élargirait pas le spectre des équations pour lesquelles on connaît des bornes effectives. Un des problèmes majeurs demeure celui de résoudre de manière effective le théorème de Siegel pour les courbes de genre supérieur ou égal à 2.

Voici le plan de cette deuxième partie.

Dans la première section, section 2.2.1, on peut trouver les normalisations des valeurs absolues et des hauteurs qui sont employées dans le texte. On y rappelle aussi quelques formules concernant le degré, le discriminant et les places ultramétriques d'un corps de nombres. La définition précise du radical d'un point de l'espace projectif y est énoncée aussi, avec quelques variantes. Les définitions des points S-entiers et de la "réduction modulo un nombre premier" ainsi qu'un lemme et quelques propositions utiles pour la suite se trouvent dans les paragraphes 2.2.2 et 2.2.3. Au paragraphe 2.2.4, se trouvent quelques lemmes analytiques.

Dans la section 2.3, "*abc* implique Siegel", on peut lire les énoncés des théorèmes de Siegel et de Belyĭ, ainsi que les démonstrations des théorèmes 9 et 13.

Le premier paragraphe de la section 2.4, "De Siegel uniforme à *abc*", rappelle les énoncés des hypothèses d'uniformité et d'effectivité des théorèmes de Siegel et de Mordell. Il comporte aussi une discussion sur l'hypothèse *Siegel* (U, K) et l'énoncé du théorème de Bilu. Le deuxième paragraphe est consacré à la démonstration du théorème 10.

Le cas de la droite projective privée de 0,1 et le point "à l'infini" est traité dans la section 2.5. Le théorème 15 y est démontré.

Dans la dernière section, ont montre comment on peut utiliser les théorèmes 10 et 15 pour obtenir des résultats non conjecturaux à partir des théorèmes de Stewart-Yu et de Bilu. On y démontre les théorèmes 17, 18 et 20. On compare les bornes obtenues du théorème 18 avec celles connues auparavant.

On finit avec un appendice traitant le cas des corps de fonctions, où nous montrons en combinant divers résultats connus que l'analogue de notre hypothèse *Siegel* (U, K) est vérifiée sur les corps de fonctions.

2.2 Notations et préliminaires.

2.2.1 Valeurs absolues, hauteurs et radicaux.

Valeurs absolues.

La valeur absolue archimédienne sur $\mathbf{Q}$ est définie en posant, pour tout nombre rationnel r,

$$|r|_\infty = \max\{r, -r\}.$$

Notons $\mathcal{P}$ l'ensemble de tous les nombres premiers. Pour définir des valeurs absolues ultramétriques, nous écrivons le nombre rationnel r non nul sous la forme

$$r = \pm \prod_{p \in \mathcal{P}} p^{\mathrm{ord}_p(r)}.$$

Par convention, $\mathrm{ord}_p(0) = \infty$. On pose alors

$$|r|_p = p^{-\mathrm{ord}_p(r)},$$

Deux valeurs absolues $|.|_1$ et $|.|_2$ sont dites équivalentes s'il existe un nombre réel n tel que $|.|_1 = |.|_2^n$.

L'ensemble des places (i.e. classes d'équivalence de valeurs absolues) de $\mathbf{Q}$, noté $M_{\mathbf{Q}}$, admet comme système de représentants la valeur absolue archimédienne $|.|_\infty$ et toutes les valeurs absolues p-adiques, $|.|_p$, où p est un nombre premier.

La formule du produit pour un nombre rationnel r non nul s'écrit alors

$$\prod_{v \in M_{\mathbf{Q}}} |r|_v = 1.$$

Pour un corps de nombres K, on note M_K l'ensemble de ses places. Nous fixons comme représentants les valeurs absolues dont la restriction à $\mathbf{Q}$ sont, soit la valeur absolue archimédienne $|.|_\infty$, soit une des valeurs absolues $p-$adiques $|.|_p$. On notera M_K^∞ l'ensemble des valeurs absolues archimédiennes de K et M_K^0 celui des valeurs absolues ultramétriques.

Pour toute place $v \in M_K$, on note K_v le complété de K en v, $\mathbf{Q}_v$ le complété de $\mathbf{Q}$ en la restriction de v à $\mathbf{Q}$ et $d_v = [K_v : \mathbf{Q}_v]$ le degré local en la valeur absolue v. La formule du produit pour un nombre algébrique x appartenant à un corps de nombres K s'écrit alors

$$\prod_{v \in M_K} |x|_v^{d_v} = 1.$$

Si $d = [K : \mathbf{Q}]$ est le degré du corps de nombres, il existe d plongements $\sigma : K \hookrightarrow \mathbf{C}$ et pour chacun d'entre eux on peut définir une valeur absolue archimédienne, en posant,

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

où $|.|_\infty$ est la valeur absolue usuelle sur $\mathbf{C}$. On peut d'ailleurs montrer que toute valeur absolue archimédienne de K est de cette forme.

Notons O_K l'anneau des entiers de K et $\mathcal{P}_K$ l'ensemble de ses idéaux premiers non nuls. On dit que $\wp \in \mathcal{P}_K$ *divise* le nombre premier p ou que $\wp$ est *au-dessus de* p, et on note $\wp | p$, si $\wp$ apparaît dans la décomposition en idéaux premiers de pO_K. Dans ce cas, on peut lui associer une valeur absolue ultramétrique de la façon suivante. Pour $x \in K^*$, écrivons

$$xO_K = \prod_{\wp} \wp^{\mathrm{ord}_\wp(x)}.$$

Soit $e_\wp = \mathrm{ord}_\wp(p)$ l'indice de ramification de $\wp$ au-dessus de p et $f_\wp$ le degré du corps résiduel. Alors

$$d_\wp = [K_\wp : \mathbf{Q}_p] = e_\wp f_\wp, \ \sum_{\wp|p} e_\wp f_\wp = [K : \mathbf{Q}] \ \text{ et } \ N_{K/\mathbf{Q}}(\wp) = p^{f_\wp}. \quad (2.24)$$

On pose

$$|x|_\wp = p^{-\mathrm{ord}_\wp(x)/e_\wp}.$$

Pour toute place $v \in M_K$, on pose $v(x) = -\log|x|_v$, avec la convention $v(0) = \infty$.

Avec ces notations,

$$O_K = \{x \in K/ \ \forall v \in M_K^0, \ |x|_v \leq 1\},$$

et de façon plus générale, si $S \subset M_K^0$ est un ensemble fini de places ultramétriques de K, on note

$$O_{K,S} = \{x \in K/ \ \forall v \notin (S \cup M_K^\infty), \ |x|_v \leq 1\}$$

l'anneau des S-entiers de K. Si $S = \emptyset$, alors $O_{K,S} = O_K$. Si $K = \mathbf{Z}$, l'anneau $O_{\mathbf{Q},S}$ des S-entiers sur $\mathbf{Z}$ sera noté $\mathbf{Z}\,[1/S]$.

On notera

$$O_{K,S}^* = \{x \in K/ \ \forall v \notin (S \cup M_K^\infty), \ |x|_v = 1\}$$

le groupe des S-unités de K.

Quelques formules.

S'il n'y a pas de confusion possible, on notera $N(\wp) = N_{K/\mathbf{Q}}(\wp)$ la norme de l'idéal premier $\wp$ de O_K.

Si $S \subset M_K^0$ est un ensemble fini de places ultramétriques, on notera souvent,

$$\Sigma_S = \sum_{\wp \in S} \log N(\wp),$$

la somme des logarithmes des normes des idéaux premiers correspondant aux places de S,

$$\Pi_S = \prod_{\wp \in S} \log N(\wp),$$

leur produit, et

$$P(S) = \{p \in \mathcal{P}/ \ \exists \wp \in S, \ \wp|p\}$$

l'ensemble des caractéristiques résiduelles de S. Avec la convention classique sur les sommes et les produits vides, nous convenons que si $S = \emptyset$, alors $\Sigma_S = 0$ et $\Pi_S = 1$.

Si P désigne le maximum des caractéristiques résiduelles de S, on a

$$([K : \mathbf{Q}]\,\mathrm{card}(P(S)))^{-1}\,\Sigma_S \leq \log P \leq \Sigma_S. \quad (2.25)$$

En effet,

$$\log P \leq \sum_{p\in P(S)} \log p \leq \sum_{p\in P(S)} \sum_{\wp|p} f_\wp \log p = \sum_{p\in P(S)} \sum_{\wp|p} \log N(\wp) = \Sigma_S,$$

et, d'autre part

$$\Sigma_S = \sum_{p\in P(S)} \sum_{\wp|p} \log N(\wp) \leq [K:\mathbf{Q}] \sum_{p\in P(S)} \log p \leq [K:\mathbf{Q}] \operatorname{card}(P(S)) \log P.$$

On peut aussi majorer le cardinal de l'ensemble S en fonction du degré $[K:\mathbf{Q}]$ et du cardinal de $P(S)$:

$$\operatorname{card}(S) = \sum_{\wp\in S} 1 = \sum_{p\in P(S)} \sum_{\wp|p} 1 \leq \sum_{p\in P(S)} [K:\mathbf{Q}]$$

$$\text{i.e. } \operatorname{card}(S) \leq [K:\mathbf{Q}] \operatorname{card}(P(S)). \tag{2.26}$$

Si L/K est une extension finie, et $\ell \in O_L$ est un idéal premier au-dessus de $\wp \in O_K$, alors $e_{\ell|\wp} = e_\ell/e_\wp$ désigne l'indice de ramification relatif et $f_{\ell|\wp} = f_\ell/f_\wp$ le rapport des degrés des corps résiduels. On a donc les formules

$$\sum_{\ell|\wp} e_{\ell|\wp} f_{\ell|\wp} = [L:K] \text{ et } N_{L/K}(\ell) = N_{K/\mathbf{Q}}(\wp)^{f_{\ell|\wp}}. \tag{2.27}$$

Si $S' = \{\ell \in M_L^0 / \ \exists \wp \in S,\ \ell|\wp\}$ est l'ensemble de places de M_L qui prolongent celles de S, alors on a, en utilisant les formules (2.24) et (2.27), pour $\ell|\wp$ et $\wp|p$, $N_{L/\mathbf{Q}}(\ell) = p^{f_\ell} = N_{K/\mathbf{Q}}(\wp)^{f_{\ell|\wp}}$ et donc

$$\sum_{\ell\in S'} \log N_{L/\mathbf{Q}}(\ell) = \sum_{\wp\in S} \sum_{\ell|\wp} f_{\ell|\wp} \log N(\wp) \leq [L:K] \sum_{\wp\in S} \log N(\wp),$$

$$\text{i.e. } \Sigma_{S'} \leq [L:K]\Sigma_S, \tag{2.28}$$

et leurs caractéristiques résiduelles sont les mêmes, i.e. $P(S') = P(S)$.

Le discriminant relatif $\delta_{L/K}$ de l'extension L/K est un idéal entier non nul de O_K et si d_K et d_L désignent les valeurs absolues des discriminants des corps K et L, alors on a (cf. l'égalité (3) de [Se2])

$$\log N_{K/\mathbf{Q}}(\delta_{L/K}) = \log d_L - [L:K] \log d_K. \tag{2.29}$$

Hauteurs.

On note $h : \mathbb{P}^n(\overline{\mathbf{Q}}) \longrightarrow [0,\infty)$ la hauteur logarithmique absolue de Weil. Si $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n$ est à coordonnées dans un corps de nombres K, elle est définie par

$$h(x) = \frac{1}{[K:\mathbf{Q}]} \sum_{v\in M_K} d_v \log \max\{|x_0|_v, \ldots, |x_n|_v\},$$

et si $x \in \overline{\mathbf{Q}}$, on pose $h(x) = h(x : 1)$. (Grâce à la formule du produit, cette définition est indépendante du choix des coordonnées et elle a été normalisée de façon à ce qu'elle ne dépende pas non plus du corps K.)

On notera, pour $x \in \mathbf{P}^n(K)$,

$$h_K(x) = [K : \mathbf{Q}]h(x)$$

la hauteur relative à K. Si L/K est une extension de corps de nombres et $x \in \mathbf{P}^n(K)$, alors $h(x) = \frac{1}{[K:\mathbf{Q}]}h_K(x) = \frac{1}{[L:\mathbf{Q}]}h_L(x)$, et donc

$$h_L(x) = [L : K]h_K(x). \tag{2.30}$$

Si a et b sont des éléments de K et m un entier naturel, alors on a les formules

$$h_K(ab) \leq h_K(a) + h_K(b) \text{ et } h_K(a^m) = |m|h_K(a). \tag{2.31}$$

Si a, b et c sont des entiers rationnels premiers entre eux, on a

$$h(a : b : c) = h_{\mathbf{Q}}(a : b : c) = \log \max\{|a|, |b|, |c|\}.$$

Si X est une courbe projective définie sur un corps de nombres K et f une fonction non constante régulière sur C, on peut définir une fonction hauteur h_f sur la courbe X en posant, pour tout point $x \in X(\overline{\mathbf{Q}})$,

$$h_f(x) = \frac{1}{\deg(f)}h(f(x)),$$

où h est la hauteur sur $\mathbf{P}^1(\overline{\mathbf{Q}})$ définie précédemment.

Si g est une autre fonction régulière sur X, on a (cf., par exemple, [HS2] ou [MvF]), pour tout $x \in X(K)$,

$$|h_g(x) - h_f(x)| \leq c\sqrt{h_f(x)}, \tag{2.32}$$

où la constante c ne dépend que de la courbe X et des fonctions g et f. Cette inégalité peut s'écrire aussi avec les hauteurs relatives, à savoir,

$$|\deg(f)h_{g,K}(x) - \deg(g)h_{f,K}(x)| \leq c\sqrt{[K : \mathbf{Q}]}\sqrt{h_{f,K}(x)}. \tag{2.33}$$

Radicaux.

Soit K un corps de nombres. (On rappelle que $\mathcal{P}_K$ désigne l'ensemble des idéaux premiers non nuls du corps K.)

Pour un point $P = (x_0 : x_1 : x_2) \in \mathbf{P}^2(K)$, on définit (cf. [El]) le *radical* de P relatif à K par :

$$\mathrm{rad}_K(P) = \sum_{\wp \in I} \log N(\wp),$$

où $I = \{\wp \in \mathcal{P}_K / \ \mathrm{card}\{v_\wp(x_0), v_\wp(x_1), v_\wp(x_2)\} \geq 2\}$.

Si a, b et c sont des entiers rationnels premiers entre eux, on a

$$\mathrm{rad}_{\mathbf{Q}}(a : b : c) = \sum_{p|abc} \log p.$$

Pour tout r appartenant à K, on pose $P_r = (r : 1 - r : 1) \in \mathbf{P}^2(K)$ et on peut montrer facilement que

$$\mathrm{rad}_K(P_r) = \sum_{\wp \in H_r} \log N(\wp),$$

où $H_r = \{\wp \in \mathcal{P}_K / \ v_\wp(r) < 0 \ \text{ ou } \ v_\wp(r) > 0 \ \text{ ou } \ v_\wp(1-r) > 0\}$.

(On remarque que si $r \in \{0, 1, \infty\}$, alors $\mathrm{rad}_K(P_r) = \infty$.)

En vue d'un analogue de (2.30), on peut définir (cf. [Mas]), pour un point $P \in \mathbf{P}^2(K)$, son *radical ramifié*, en posant :

$$\mathrm{rad}^r_K(P) = \sum_{\wp \in I} \log N(\wp)^{e_\wp},$$

où $e_\wp$ est l'indice de ramification de l'idéal $\wp$. Si L est une extension finie de K, on a

$$\mathrm{rad}^r_L = [L : K]\mathrm{rad}^r_K. \tag{2.34}$$

Les deux définitions sont reliées par la double inégalité(cf. [Mas] (1.12)),

$$\mathrm{rad}_K \leq \mathrm{rad}^r_K \leq \mathrm{rad}_K + \log d_K. \tag{2.35}$$

2.2.2 Plongements affines et points S-entiers.

Le plongement affine.

Soient U une courbe algébrique affine définie sur un corps de nombres K, de genre g et ayant s points à l'infini et S un ensemble fini de places de K contenant les places archimédiennes.

Pour définir l'ensemble des points S-entiers de la courbe U, nous la plongeons dans un espace affine, par rapport au "diviseur à l'infini" de la façon suivante.

Soit $\widetilde{U}$ la normalisée de U, et C une courbe projective lisse contenant $\widetilde{U}$. La courbe C est définie sur K, de genre g et, si on note $U_\infty = C \setminus \widetilde{U}$, on a $\mathrm{card}(U_\infty) = s$. Notons $U_\infty = \{P_1, \ldots, P_s\}$ les points à l'infini, et soit D un diviseur de la courbe C défini sur K, très ample et ayant pour support les points $P_1, \ldots, P_s$. (Par exemple, $D = d((P_1) + \cdots + (P_s))$ avec $\deg(D) = ds \geq 2g + 1$.)

Soit $\mathcal{L}(D) = \{f \in K(C)/\mathrm{div}(f) \geq -D\} \cup \{0\}$ le K-espace vectoriel associé au diviseur D. On pose $\dim_K \mathcal{L}(D) = n + 1$. Soit $(f_0, \ldots, f_n)$ une base de $\mathcal{L}(D)$.

Par définition de la propriété d'être très ample, le diviseur D définit un plongement (c'est-à-dire un isomorphisme sur son image)

$$\begin{array}{rccl} \Phi_D : & C & \hookrightarrow & \mathbf{P}^n \\ & P & \longmapsto & (f_0(P) : f_1(P) : \ldots : f_n(P)) \end{array}$$

qui ne dépend pas (à automorphisme près) de la base de $\mathcal{L}(D)$ choisie. En effet, on peut considérer d'abord l'application

$$P \mapsto H_P = \{f \in \mathcal{L}(D) / \ f(P) = 0\}.$$

Cette application est indépendante de la base de $\mathcal{L}(D)$ choisie. Si on fixe une base $(f_0, f_1, \ldots, f_n)$, alors H_P s'identifie à l'hyperplan de $\mathcal{L}(D)$ défini par l'équation $\sum_{i=1}^{n} \alpha_i X_i = 0$ où $\alpha_i = f_i(P)$. (Au point $(X_1, \ldots, X_n)$ on lui associe la fonction $f = \sum_{i=1}^{n} X_i f_i$.) On peut donc associer à H_P le point projectif $(f_0(P) : f_1(P) : \ldots : f_n(P))$.

Le plongement Φ_D envoie les points $P_1, \ldots, P_s$ sur l'hyperplan H de $\mathbf{P}^n$ défini tel que le "tiré en arrière" $\Phi_D^* H$ de H par Φ_D soit le diviseur D. Par définition de Φ_D^*, on a $\Phi_D(\{P_1, \ldots, P_s\}) = H \cap \Phi_D(C)$. Si on veut que H soit l'hyperplan défini par l'équation $X_0 = 0$, il suffit de prendre la fonction f_0 telle que $\mathrm{div}(f_0)$ soit le diviseur nul, c'est-à-dire telle que f_0 soit constante.

On obtient ainsi un plongement (qu'on notera encore Φ_D) de la courbe affine U dans l'espace affine $\mathbb{A}^n$,

$$\begin{array}{ccc} U & \hookrightarrow & \mathbb{A}^n \\ P & \longmapsto & (f_1(P), \ldots, f_n(P)). \end{array}$$

Le plongement de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ dans $\mathbf{A}^3$.

Dans ce paragraphe, U est la droite projective privée de $0, 1$ et l'infini. Le diviseur $D = (0) + (1) + (\infty)$ étant très ample ($\deg(D) = 3 \geq 2g + 1 = 1$), le K-espace vectoriel $\mathcal{L}(D)$ nous fournit un plongement Φ_D. L'espace $\mathcal{L}(D)$ est engendré par les fonctions

$$w = 1, \ \ x = T, \ \ y = \frac{1}{T} \ \text{ et } \ z = \frac{1}{1 - T},$$

où w, x, y et z sont vues comme des fonctions régulières sur la courbe U et $1, T, \frac{1}{T}$ et $\frac{1}{1-T}$ comme des éléments de $K[T, \frac{1}{T(T-1)}]$. Le plongement Φ_D de $\mathbf{P}^1$ dans $\mathbf{P}^3$ est donné par les valeurs de ces quatre fonctions au point considéré.

De plus, $\Phi_D(\{0, 1, \infty\}) = \Phi_D(\mathbf{P}^1) \cap H$ où H est l'hyperplan défini par l'équation $X_0 = 0$. D'où

$$\begin{array}{rccl} \Phi_D : \mathbf{P}^1 \setminus \{0, 1, \infty\} & \hookrightarrow & \mathbf{A}^3 \\ P & \mapsto & (x(P), y(P), z(P)). \end{array}$$

On peut aussi le voir de la façon suivante.

L'algèbre de coordonnées affines de $\mathbf{P}^1 \setminus \{\infty\}$ étant $K[T]$, celle de $\mathbf{P}^1 \setminus \{0, \infty\}$ est le localisé $K[T]_{(T)}$ de $K[T]$ en les polynômes s'annulant en 0, c'est-à-dire $K\left[T, \frac{1}{T}\right]$, et celle de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ est $K\left[T, \frac{1}{T}, \frac{1}{1-T}\right] = K\left[T, \frac{1}{T(T-1)}\right]$. En plongeant la courbe dans l'espace affine grâce à son algèbre de coordonnées affines, on retrouve Φ_D.

Points S-entiers.

Définition 1. *On définit l'ensemble des points S-entiers de la courbe U par rapport à la base $(f_0, f_1, \ldots, f_n)$ du système $\mathcal{L}(D)$ choisie, en posant*

$$U_{(f_i)}(O_{K,S}) = \{P \in U/ \ \forall i \in \{1, \ldots, n\}, \ \ f_i(P) \in O_{K,S}\}.$$

Si $(g_0, g_1, \ldots, g_n)$ est une autre base de $\mathcal{L}(D)$, alors , pour $i, j \in \{0, \ldots, n\}$, il existe des $a_{ij} \in K$, tels que, pour tout j,

$$g_j = \sum_{i=1}^{n} a_{ij} f_i.$$

Soit $S' = S \cup \{\wp \in \mathcal{P}_K/ \ \exists (i,j) \in \{0, \ldots, n\}^2, \ v_\wp(a_{ij}) < 0\}$. (Comme les a_{ij} sont en nombre fini, l'ensemble S' est lui aussi fini.)

Si $P \in U_{(f_i)}(O_{K,S})$, alors $g_j(P) = \sum_{i=1}^{n} a_{ij} f_i(P) \in O_{K,S'}$, pour tout j, i.e.

$$U_{(f_i)}(O_{K,S}) \subset U_{(g_i)}(O_{K,S'}).$$

Si S est assez grand, les deux ensembles coïncident. Pour cette raison, on notera dans toute la suite, sans préciser la base,

$$U(O_{K,S})$$

l'ensemble des points K-rationnels S-entiers de la courbe U.

J.P. Serre [Se1] donne la définition suivante .

Définition 2. *L'ensemble $\Sigma \subset U(K)$ de points K-rationnels de U est S-quasi-entier si, pour toute fonction $\varphi \in O(U)$ régulière sur U, il existe $\delta \in K^\times$, tel que,*

$$\forall P \in \Sigma, \ \ \varphi(P) \in \delta^{-1} O_{K,S}.$$

Il faut (et il est évidemment nécessaire) de vérifier cette condition sur une famille génératrice $(\varphi_1, \ldots, \varphi_n)$ de l'algèbre de coordonnées affines $O(U)$ de U (en tant que K-algèbre).

En effet, si $\varphi \in O(U)$, alors il existe des $\alpha_i \in K$, tels que $\varphi = \sum_{i=1}^{n} \alpha_i \varphi_i$. Posons $\delta = \text{pgcd}\{d_i \delta_i\}$ où d_i est le "dénominateur" de α_i, i.e. $d_i = \min\{d \in \mathbf{N} \setminus \{0\}/ \ d\,\alpha_i \in O_{K,S}\}$. Soit $P \in \Sigma$. Comme, pour tout $i \in \{1, \ldots, n\}$, il existe $\delta_i \in K^\times$ tel que $\varphi_i(P) \in \delta_i^{-1} O_{K,S}$, alors

$$\varphi(P) = \sum_{i=1}^{n} \alpha_i \varphi_i(P) \in \delta^{-1} O_{K,S}.$$

En particulier, si on reprend le plongement affine $\phi_D : U \hookrightarrow \mathbf{A}^n$ et $(f_0, f_1, \ldots, f_n)$ est une base de $\mathcal{L}(D)$ (en tant que K-espace vectoriel) telle que f_0 soit constante, alors $(f_1, \ldots, f_n)$ engendre $O(U)$ en tant que K-algèbre.

Ainsi, l'ensemble $\Sigma \subset U(K)$ est S-quasi-entier si, et seulement si

$$\forall i \in \{0, \ldots, n\},\ \exists \delta_i \in K^\times,\ \forall P \in \Sigma,\ f_i(P) \in \delta_i^{-1} O_{K,S}.$$

Nous en déduisons la proposition suivante qui relie les deux définitions.

Proposition 1. *i) L'ensemble $U(O_{K,S})$ des points S-entiers de U est un ensemble S-quasi-entier.*

ii) Si $\Sigma \subset U(K)$ est un ensemble S-quasi-entier, alors il est inclus dans l'ensemble $U(O_{K,S'})$ des points S'-entiers de U, pour un ensemble fini de places S' contenant S.

Caractéristique d'Euler.

Soit $\chi(U) = 2 - 2g - s$ la caractéristique d'Euler de la courbe U. Alors $\chi(U) < 0$ si, et seulement si, $g = 0$ et $s \geq 3$ ou bien $g = 1$ et $s \geq 1$ ou bien $g \geq 2$. Dans ce cas, on dit que la courbe U est non exceptionnelle.

2.2.3 Modèles entiers et bonne réduction.

En ce qui concerne les rappels faits dans cette section, on peut se reporter à [HS2].

Soient $u : X \longrightarrow Z$ et $v : Y \longrightarrow Z$ deux morphismes de schémas. Le produit fibré de X et Y au-dessus de Z, noté $X \times_Z Y$, est un schéma P muni de deux morphismes $pr_1 : P \longrightarrow X$ et $pr_2 : P \longrightarrow Y$ tels que $u \circ pr_1 = v \circ pr_2$ et vérifiant la propriété universelle suivante :

Pour tout schéma P' et des morphismes $q_1 : P' \longrightarrow X$ et $q_2 : P' \longrightarrow Y$, il existe un morphisme unique $\phi : P' \longrightarrow P$ tel que $q_1 = pr_1 \circ \phi$ et $q_2 = pr_2 \circ \phi$.

Soient K un corps de nombres et S un ensemble fini de places de K éventuellement vide. On notera $\mathcal{S} = \mathrm{Spec}(O_{K,S}) = \mathrm{Spec}(O_K) \setminus S$ le spectre premier de l'anneau des S-entiers, $\eta = (0)$ le point générique de $\mathcal{S}$ et $\wp$ un point fermé.

À chaque point y de $\mathcal{S}$, correspond un morphisme allant du spectre du corps résiduel $k(y) = \mathcal{O}_{X,y}/\mathfrak{m}_y$ dans $\mathcal{S}$. (On a noté $\mathcal{O}_{X,y}$ l'anneau local en y et $\mathfrak{m}_y$ son idéal maximal. On a $k(\eta) = K$.)

Si $\mathcal{X} \longrightarrow \mathcal{S}$ est un morphisme de schémas, on peut donc considérer la fibre $\mathcal{X}_y = \mathcal{X} \times_{\mathcal{S}} \mathrm{Spec}(k(y))$ de $\mathcal{X} \longrightarrow \mathcal{S}$ au-dessus de chaque point y de $\mathcal{S}$. La fibre $\mathcal{X}_\eta$ est appelée la fibre générique et les $\mathcal{X}_\wp$ fibres spéciales. Si $\mathcal{X}$ est irréductible, il en est de même de la fibre générique et de toutes les fibres spéciales, sauf un nombre fini (cf. [HS2] Proposition A.9.1.4).

Définition. Soit X une courbe algébrique projective (resp. affine) et lisse définie sur K (i.e. il existe un morphisme de schémas $X \longrightarrow \mathrm{Spec}(K)$). Un modèle de X au-dessus de $\mathcal{S}$ est un schéma $\mathcal{X} \longrightarrow \mathcal{S}$ projectif (resp. affine) et plat, tel que la fibre générique $\mathcal{X}_\eta$ soit isomorphe à la courbe X.

Par exemple $\mathbb{P}^1_{\mathbf{Z}[\frac{1}{S}]}$ est un modèle de $\mathbb{P}^1_{\mathbf{Q}}$ au-dessus de $\mathrm{Spec}(\mathbf{Z}[\frac{1}{S}])$ et $\mathcal{Y} = \mathbb{P}^1_{\mathbf{Z}[\frac{1}{S}]} \setminus \{0, 1, \infty\} = \mathrm{Spec}(\mathbf{Z}[\frac{1}{S}][T, \frac{1}{T(1-T)}])$ est un modèle affine de $\mathbb{P}^1_{\mathbf{Q}} \setminus \{0, 1, \infty\}$ au-dessus de $\mathrm{Spec}(\mathbf{Z}[\frac{1}{S}])$.

Définition. Soit $\wp$ un idéal premier de l'anneau $O_{K,S}$. On dira que la courbe X a "bonne réduction en $\wp$" s'il existe un modèle $\mathcal{X}$ de X au-dessus de $\mathcal{S}$ tel que la fibre spéciale $\mathcal{X}_\wp$ soit une courbe algébrique projective et lisse.

Remarquons que X a bonne réduction en tout $\wp$, sauf un nombre fini (cf. [HS2] Proposition A.9.1.6). On a donc la proposition suivante :

Proposition 2. *Soit X une courbe algébrique projective et lisse définie sur un corps de nombres K. Il existe un ensemble fini $T \subset M_K$ et un modèle $\mathcal{X}$ de X au-dessus de $\mathcal{B} = \mathrm{Spec}(O_{K,T})$, tels que X ait bonne réduction au-dessus de $\mathcal{B}$, i.e. pour tout $\wp \in \mathcal{B}$, la fibre spéciale $\mathcal{X}_\wp$ soit encore une courbe projective et lisse.*

Soient C une courbe projective définie sur K et $\mathcal{C}$ un modèle de C au-dessus de $\mathcal{S} = \mathrm{Spec}(O_{K,S})$. Un point K-rationnel $x \in C(K)$ correspond à un morphisme $x : \mathrm{Spec}(K) \longrightarrow C$ et il s'étend en une section $\sigma_x : \mathcal{S} \longrightarrow \mathcal{C}$, car la courbe C est projective ([HS2] lemma A.9.1.5).

Si U est un ouvert affine de C, disons $U = C \setminus \mathrm{supp}(D)$ où D est un diviseur de la courbe C, on fabrique un schéma $\mathcal{U} \longrightarrow \mathcal{S}$ tel que sa fibre générique $\mathcal{U}_\eta$ soit isomorphe à U, en posant $\mathcal{U} = \mathcal{C} \setminus \overline{\mathrm{supp}(D)}^{Zar}$. (On a noté $\overline{\mathrm{supp}(D)}^{Zar}$ l'adhérence pour la topologie de Zarizki.)

Un point $x \in U(K)$ est S-entier dans le sens de la définition 1 (i.e. $x \in U(O_{K,S})$) si, et seulement s'il se prolonge en une section σ_x au-dessus de $\mathcal{S} = \mathrm{Spec}(O_{K,S})$. (On dit que σ_x est un $\mathcal{S}$-point de $\mathcal{U}$ ou un point de $\mathcal{U}$ à valeurs dans $\mathcal{S}$.) Dans ce cas là, pour tout idéal premier $\wp$ de $\mathcal{S}$, le point x est $\wp$-entier (i.e. $v_\wp(x) \geq 0$) et $\sigma_x(\wp) \in \mathcal{U}_\wp$.

On pose $\mathcal{U}(\mathcal{S}) = \mathcal{M}or_K(\mathcal{S} \to \mathcal{U})$ l'ensemble des morphismes de $\mathcal{S}$ dans $\mathcal{U}$ au-dessus de $\mathrm{Spec}(K)$. On a alors un isomorphisme

$$\begin{array}{ccc} U(O_{K,S}) & \simeq & \mathcal{U}(\mathcal{S}) \\ x & \mapsto & \sigma_x. \end{array}$$

L'énoncé suivant ([Se1] chapitre 7) fait le lien entre ce point de vue et la définition 2.

Proposition. L'ensemble $\Sigma \subset U(K)$ est S-quasi-entier au sens de la définition 2 si et seulement s'il existe un modèle (affine) $\mathcal{U}$ de U au-dessus de $\mathcal{S}$ tel que tout point x de Σ se prolonge en une section σ_x de $\mathcal{S}$.

Si $f : X \longrightarrow Y$ est un morphisme de courbes projectives défini sur K, et $\mathcal{X}$ et $\mathcal{Y}$ sont des modèles de X et Y au-dessus de $\mathcal{S}$, alors f s'étend en une application rationnelle $\tilde{f} : \mathcal{X} \cdots \to \mathcal{Y}$.

Proposition 3. *Soit $f : X \longrightarrow Y$ un morphisme de courbes projectives, défini sur un corps de nombres K. Il existe un ensemble fini T de places de K et des modèles $\mathcal{X}$ et $\mathcal{Y}$ de X et de Y au-dessus de $\mathcal{B} = \mathrm{Spec}(O_{K,T})$ tels que f se prolonge en un morphisme $\tilde{f} : \mathcal{X} \longrightarrow \mathcal{Y}$ et, de plus,*

i) si f est fini, il en est de même de $\tilde{f}$, et dans ce cas, $\deg(f) = \deg(\tilde{f})$,

ii) si f est non ramifié en dehors de certains points $\{P_1, \ldots, P_r\}$ de Y, alors, pour tout $\wp \in \mathcal{B}$, le morphisme $\tilde{f}$ restreint à la fibre $\mathcal{X}_\wp$ sera non ramifié en dehors de $\{\sigma_{P_1}(\wp), \ldots, \sigma_{P_r}(\wp)\}$.

La démonstration de la proposition 3 repose sur le fait que si un nombre, un discriminant, par exemple, est non nul, il en sera de même pour sa réduction modulo p, pour tout nombre premier p sauf un nombre fini.

Dans la section 2.4, nous aurons besoin du lemme suivant.

Lemme 15. *Soient K un corps de nombres et S un ensemble fini de places de K. Les revêtements étales de* $\mathrm{Spec}(O_{K,S})$ *sont des réunions finies de* $\mathrm{Spec}(O_{L,S'})$ *où L/K est une extension finie, de degré $[L : K]$ inférieur ou égal au degré du revêtement, non ramifiée en dehors de l'ensemble S et $S' = \{w \in M_L / \ \exists v \in S, \ w|v\}$.*

Démonstration du lemme 15.

On pose $A = O_{K,S}$ et $Y = \mathrm{Spec}(A)$. Soit X un revêtement étale de Y et $X = \cup_{i \in I} X_i$ sa décomposition en composantes connexes. L'ensemble I est fini et, pour tout $i \in I$, X_i est un revêtement étale connexe de Y.

Soit $i \in I$. On note $L_i = R(X_i)$ l'anneau des fonctions rationnelles de X_i et Y_i' le normalisé de Y dans L_i. D'après le corollaire 10.2 de [SGA] I, X_i est isomorphe à Y_i'. Or, d'après le corollaire 10.3 de [SGA] I, le foncteur $X \mapsto R(X)$ établie une équivalence entre la catégorie des revêtements étales connexes de Y et celle des extensions finies L/K non ramifiées sur $Y = \mathrm{Spec}(O_K) \setminus S$, donc L_i/K est une extension finie non ramifiée en dehors de S.

Comme le foncteur inverse est le foncteur normalisation, alors X_i a pour anneau le normalisé A_i' de A dans L_i, i.e. $X_i = \mathrm{Spec}(A_i')$ où $A_i' = O_{L_i,S_i'}$, et S_i' est l'ensemble de places du corps L_i qui sont au-dessus de celles de S.

On a donc, $X = \cup_{i \in I} \mathrm{Spec}(O_{L_i,S_i'})$, ce qui démontre le lemme. □

2.2.4 Lemmes analytiques.

Dans ce paragraphe on énonce quelques lemmes analytiques. Le lemme 19, qui se démontre à l'aide des lemmes 17 et 18, intervient dans la démonstration du théorème 10. Le lemme 16 sert à démontrer le lemme 17.

Lemme 16. *Si, pour $n \geq 1$, $p_1, p_2, \ldots, p_n$ sont les n plus petits nombres premiers, et on note $T_n = \sum_{i=1}^{n} \log p_i$, alors, pour tout entier $n \geq 2$, on a*

$$n \leq 2\frac{T_n}{\log T_n}.$$

Démonstration du lemme 16.

Pour $n \geq 13$, le $i$ème nombre premier p_i est supérieur ou égal à $3i$ et, pour tout $n \geq 2$, $\sum_{i=1}^{n} \log i \geq \int_1^n \log x \ dx = n \log n - n + 1$. À l'aide de ces remarques, on minore T_n en fonction de n, pour $n \geq 13$:

$$T_n = \sum_{i=1}^{n} \log p_i \geq \sum_{i=1}^{n} \log(3i) \geq n \log n + n(\log 3 - 1) + 1 \geq n \log n.$$

Pour $x \geq e$, la fonction $x \mapsto \frac{x}{\log x}$ est croissante, et comme $n \log n \geq e$ pour $n \geq 3$, on a

$$\frac{T_n}{\log T_n} \geq \frac{n \log n}{\log(n \log n)}.$$

De plus, $\frac{\log n + \log\log n}{\log n} = 1 + \frac{\log\log n}{\log n} \leq 1 + \frac{1}{e}$, pour $n \geq 2$, alors, pour tout $n \geq 13$, on a

$$n \leq \left(1 + \frac{1}{e}\right) \frac{T_n}{\log T_n}.$$

Par le calcul, on vérifie que pour $n \in \{2, \ldots, 12\}$ on a aussi $n \leq 2\frac{T_n}{\log T_n}$, d'où le lemme. □

Lemme 17. *Soit K un corps de nombres, $S \subset M_K^0$ un ensemble fini de places ultramétriques de K et $P(S) = \{p \in \mathcal{P} / \ \exists \wp \in S, \ \wp | p\}$. Si $\mathrm{card}(P(S)) \geq 3$, alors*

$$\mathrm{card}(P(S)) \leq 2\frac{\Sigma_{P(S)}}{\log \Sigma_{P(S)}} \leq 2\frac{\Sigma_S}{\log \Sigma_S}.$$

Démonstration du lemme 17.

On note $r = \mathrm{card}(P(S))$ et on remarque que $\Sigma_{P(S)}$ est supérieur ou égal à la somme des logarithmes des r plus petits nombres premiers, c'est-à-dire, T_r et que $\Sigma_S = \sum_{p \in P(S)} \sum_{\wp | p} f_\wp \log p \geq \sum_{p \in P(S)} \log p = \Sigma_{P(S)}$.

De plus, pour $x \geq e$, la fonction $x \mapsto \frac{x}{\log x}$ est croissante, et comme, pour $r \geq 3$, $e \leq T_r \leq \Sigma_{P(S)} \leq \Sigma_S$, alors, en appliquant le lemme 16, on obtient

$$\frac{r}{2} \leq \frac{T_r}{\log T_r} \leq \frac{\Sigma_{P(S)}}{\log \Sigma_{P(S)}} \leq \frac{\Sigma_S}{\log \Sigma_S}.$$

□

Lemme 18. *Soit L/K une extension finie de corps de nombres, $\delta_{L/K}$ son discriminant relatif et $\wp$ un idéal premier de O_K qui divise le nombre premier p. Alors*

$$\mathrm{ord}_\wp(\delta_{L/K}) \leq [L:K] - 1 + [L:K] e_\wp \frac{\log[L:K]}{\log p}.$$

Démonstration du lemme 18. C'est le corollaire à la proposition 2, §1 de [Se2]. □

Lemme 19. *Soit L/K une extension de corps de nombres. Notons $\delta = \delta_{L/K}$ son discriminant relatif et $R = R_{L/K}$ l'ensemble des places de M_K correspondant aux idéaux premiers au-dessus desquels l'extension se ramifie, c'est-à-dire tels que $v_\wp(\delta_{L/K}) > 0$. On désigne par $P(R)$ l'ensemble des caractéristiques résiduelles de R. Si* $\mathrm{card}(P(R)) \geq 3$, *alors*

$$\log N(\delta_{L/K}) \leq [L:K]\left(\Sigma_R + 2[K:\mathbf{Q}]\log[L:K]\frac{\Sigma_R}{\log \Sigma_R}\right).$$

Démonstration du lemme 19.

Si $\wp$ est un idéal premier de O_K tel que $\wp | p$, alors $N(\wp) = p^{f_\wp}$. On a $N(\delta) = \prod_{\wp \in R} N(\wp)^{\mathrm{ord}_\wp(\delta)}$ et, en utilisant le lemme 18, on obtient

$$\begin{aligned}
\log N(\delta) &\leq \sum_{\wp\in R}\left([L:K] + [L:K]e_\wp \tfrac{\log[L:K]}{\log p}\right)\log N(\wp) \\
&= [L:K]\left(\sum_{\wp\in R}\log N(\wp) + \log[L:K]\sum_{\wp\in R} e_\wp f_\wp\right) \\
&= [L:K]\left(\Sigma_R + \log[L:K]\sum_{p\in P(R)}\sum_{\wp|p} e_\wp f_\wp\right) \\
&= [L:K]\left(\Sigma_R + [K:\mathbf{Q}]\log[L:K]\mathrm{card}(P(R))\right).
\end{aligned}$$

On conclut en appliquant le lemme 17 à l'ensemble de places R. □

2.3 *abc* implique Siegel.

2.3.1 Des théorèmes et conjectures.

Nous énonçons ici le théorème de Siegel (cf. [Si3], et aussi [La3] et [HS2] chapitre D) sous la version étendue par Mahler aux points S-entiers ([Se1], [La1]), la conjecture *abc* de Masser-Oesterlé ([Mas] et [Oe]) et le théorème de Belyĭ ([Be]) dont nous nous servirons.

Théorème 11. *(Siegel)*

Soit U une courbe affine définie sur un corps de nombres K, de genre g et ayant s points à l'infini. Soit S un ensemble fini de places de K. Si $\chi(U) = 2 - 2g - s < 0$, alors l'ensemble $U(O_{K,S})$ des points S-entiers de U est fini.

Conjecture 1 (*abc*)

Étant donné un corps de nombres K et un nombre réel $\varepsilon > 0$, il existe une constante $c_{\varepsilon,K} > 0$ telle que, pour tout triplet (a,b,c) de nombres algébriques dans K, non nuls, tels que $a + b = c$, on ait

$$(1-\varepsilon)h_K(a:b:c) < \mathrm{rad}_K(a:b:c) + c_{\varepsilon,K}.$$

Celle-ci est la conjecture sur $\mathbf{Q}$ étendue aux corps de nombres. Cependant, on peut tenter de préciser la dépendance en le corps de nombres K de la constante $c_{\varepsilon,K}$, en faisant intervenir le radical ramifié. Pour ainsi faire, D.W. Masser [Mas] montre qu'il est nécessaire de faire apparaître le logarithme de la valeur absolue d_K du discriminant de K avec un coefficient > 1. Considérons donc la conjecture suivante (suggérée, mais non formulée explicitement dans loc. cit. (1.17)), où rad_K^r désigne le radical ramifié, introduit dans la section 2.2.1.

Conjecture 3. *Étant donné un corps de nombres K et nombre réel $\varepsilon > 0$, il existe une constante $c = c(\varepsilon, [K : \mathbf{Q}]) > 0$ telle que, pour tout triplet (a, b, c) de nombres algébriques dans K, non nuls, tels que $a + b = c$, on ait*

$$h_K(a : b : c) < (1 + \varepsilon)\left(\mathrm{rad}_K^r(a : b : c) + \log d_K\right) + c.$$

On remarque qu'en utilisant l'inégalité (2.35) du paragraphe 2.2.1, on pourrait en déduire

$$(1 - \varepsilon)h_K(a : b : c) < \mathrm{rad}_K(a : b : c) + 2\log d_K + c.$$

Théorème 12. *(Belyĭ)*
Soit C une courbe algébrique projective. Alors la courbe C est définie sur $\overline{\mathbf{Q}}$ si et seulement s'il existe un morphisme fini et surjectif

$$f : C \longrightarrow \mathbf{P}^1$$

non ramifié en dehors de $\{0, 1, \infty\}$. De plus, étant donné un ensemble Σ de points algébriques de C, on peut choisir f tel que $f(\Sigma) \subset \{0, 1, \infty\}$.

La construction d'une telle fonction de Belyĭ est totalement explicite et montre que, si C est définie sur un corps de nombres K, alors la fonction f peut être choisie définie sur K.

Sous une version effective de la conjecture *abc*, à savoir, la connaissance de la constante $c_{\varepsilon,K}$, le théorème de Siegel (théorème 11) serait lui aussi effectif. Précisément, la conjecture 1 permettrait de démontrer le théorème 9, déjà énoncé dans l'introduction et que nous rappelons ici.

Théorème 9 *Soient K un corps de nombres, U une courbe algébrique affine non exceptionnelle définie sur K, S un ensemble fini de places ultramétriques de K et $h_{U,K}$ une fonction hauteur définie sur $U(K)$ associée à un diviseur de degré 1.*

Supposons vraie la conjecture 1.

Pour tout $\varepsilon \in]0, -\chi(U)[$ et tout point S-entier x de U, il existe une constante γ dépendant du corps de nombres K, de la courbe U, du choix

de la hauteur $h_{U,K}$ et de ε, mais pas du point x ni de l'ensemble S, telle que

$$h_{U,K}(x) \leq -\frac{1}{\varepsilon + \chi(U)} \sum_{\wp \in S} \log N(\wp) + \gamma. \tag{2.36}$$

Remarques.

i) La borne (2.36) impliquerait que l'ensemble $U(O_{K,S})$ est fini.

ii) Si la constante $c_{\varepsilon,K}$ de la conjecture 1 était effective, alors il en serait de même de γ.

iii) Pour la fonction hauteur $h_{U,K}$ on peut prendre $h_{f,K} = \frac{1}{d}(h_K \circ f)$, pour n'importe quelle fonction f de degré d définie sur U (cf. l'inégalité (2.33).)

La conjecture 3, qui précise la dépendance en le corps de nombres, permettrait de raffiner la borne du théorème précédent.

Théorème 13. *Sous les hypothèses du théorème 9, supposons vraie la conjecture 3.*

Pour tout $\varepsilon \in]0, -\chi(U)[$ et tout point S-entier x de U, il existe une constante κ dépendant du degré $[K : \mathbf{Q}]$ du corps de nombres, de la courbe U, du choix de la hauteur $h_{U,K}$ et de ε, mais pas du point x ni du corps K lui même, ni de l'ensemble S, telle que

$$h_{U,K}(x) \leq -\frac{1}{\varepsilon + \chi(U)} \sum_{\wp \in S} \log N(\wp) - \frac{2}{\varepsilon + \chi(U)} \log(d_K) + \kappa. \tag{2.37}$$

2.3.2 Vers "Siegel effectif".

Dans cette section nous démontrons le théorème 9.

Reprenons les notations du paragraphe 2.2.2. On se donne une courbe affine U définie sur K, de genre g et ayant s points à l'infini. On note $\widetilde{U}$ la normalisée de U, C une courbe projective lisse contenant $\widetilde{U}$, $U_\infty = \{P_1, \ldots, P_s\}$ les points à l'infini, D le diviseur correspondant à ces points et Φ_D le plongement affine.

Lemme 20. *Il existe un morphisme fini et surjectif $f : C \longrightarrow \mathbf{P}^1$, défini sur K, non ramifié au-dessus de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, tel que*

$$f(\{P_1, \ldots, P_s\}) \subset \{0, 1, \infty\}$$

et, si on note $m = \mathrm{card}(\{P \in C(\overline{\mathbf{Q}})/f(P) \in \{0, 1, \infty\}\})$ et $d = \deg(f)$, on ait

$$d - m + s = -\chi(U) > 0.$$

Démonstration du lemme 20.

On applique le théorème 12 à la courbe projective C qui est définie sur K et à l'ensemble de points $\{P_1, \ldots, P_s\}$.

Pour cette fonction de Belyĭ f le théorème de Riemann-Hurwitz donne :

$$\sum_{P\in C, f(P)\in\{0,1,\infty\}} (e_P(f)-1) = \sum_{P\in C,\text{ram.}} (e_P(f)-1) = 2d+2g-2.$$

Par ailleurs,

$$m = 3d - \sum_{P\in C, f(P)\in\{0,1,\infty\}} (e_P(f)-1) = 3d-2d-2g+2 = d-2g+2,$$

et donc $d-m+s = 2g-2+s = -\chi(U)$, ce qui démontre le lemme. □

Soit $x \in U(O_{K,S})$ tel que $f(x) \notin \{0,1,\infty\}$. (Si $f(x) \in \{0,1,\infty\}$, alors $h_K(f(x)) = 0$ et l'inégalité est vérifiée.)

Comme $U(O_{K,S}) \subset C(K)$, alors $f(x) = (r:1) \in \mathbb{P}^1(K) \setminus \{0,1,\infty\}$ et on peut appliquer la conjecture 1 à $P_x = (r : 1-r : 1)$. Pour tout $\varepsilon > 0$, il existe une constante $c_{\varepsilon,K}$, telle que

$$(1-\varepsilon)h_K(P_x) \leq \mathrm{rad}_K(P_x) + c_{\varepsilon,K}.$$

Comme $h_K(f(x)) = h_K(r:1) \leq h_K(r:1-r:1) = h_K(P_x)$, alors, pour tout $\varepsilon \in]0,1[$, on a

$$(1-\varepsilon)h_K(f(x)) \leq \mathrm{rad}_K(P_x) + c_{\varepsilon,K}. \tag{2.38}$$

La proposition 4, qui sera démontrée à la fin de cette section, nous donne une majoration du radical de P_x.

Proposition 4. *Il existe des constantes c_1 et c_2 dépendant du degré $[K:\mathbf{Q}]$ du corps de nombres K, de la courbe C, mais pas du corps K lui-même ni du point x ni de l'ensemble de places S, telles que*

$$\mathrm{rad}_K(P_x) \leq \left(\frac{\chi(U)}{d}+1\right) h_K(f(x)) + c_1\sqrt{h_K(f(x))} + c_2 + \sum_{\wp\in S}\log N(\wp).$$

En comparant l'inégalité (2.38) et celle de la proposition 4, on a

$$-\left(\varepsilon+\frac{\chi(U)}{d}\right) h_K(f(x)) \leq c_1(C,f)\sqrt{h_K(f(x))} + c_2(C,f) + c_{\varepsilon,K} + \sum_{\wp\in S}\log N(\wp),$$

où les constantes c_1, c_2 et $c_{\varepsilon,K}$ ne dépendent pas du point x ni de l'ensemble de places S. On a donc, pour tout $\varepsilon \in]0,1[$,

$$\left(-\varepsilon - \frac{\chi(U)}{d} - c_1\left(\sqrt{h_K(f(x))}\right)^{-1}\right) h_K(f(x)) \leq c_{\varepsilon,K} + c_2 + \sum_{\wp\in S}\log N(\wp).$$

Choisissons comme hauteur sur la courbe $h_{U,K} = h_{f,K} = \frac{1}{d}(h_K \circ f)$, où h_K est la hauteur logarithmique sur $\mathbf{P}^1$. Soient $\varepsilon < -\frac{\chi(U)}{d}$ et $\xi \in]0, -\varepsilon - \frac{\chi(U)}{d}[$.

Alors ou bien $h_K(f(x)) < \left(\frac{c_1}{\xi}\right)^2$, et donc $h_{U,K}(x) < \frac{c_1^2}{d\xi^2}$ et le théorème est démontré, ou bien $\frac{c_1}{\sqrt{h_K(f(x))}} \leq \xi$ et

$$-\left(d\left(\varepsilon + \xi\right) + \chi(U)\right) h_f(x) \leq \sum_{\wp \in S} \log N(\wp) + c_2 + c_{\varepsilon,K}.$$

D'où, pour tout $\varepsilon \in]0, -\chi(U)[$, on a

$$h_{U,K}(x) \leq -\frac{1}{\varepsilon + \chi(U)} \sum_{\wp \in S} \log N(\wp) + \gamma,$$

où γ est une constante dépendant du corps de nombres K, de la courbe U, du choix de la hauteur h_U et du nombre réel ε. □

2.3.3 Variation sur "Siegel effectif".

Nous démontrons ici le théorème 13.

Reprenons la démonstration du théorème 9. En appliquant la conjecture 3 au point P_x nous obtenons l'inégalité suivante qui remplace l'inégalité (2.38).

$$h_K(f(x)) \leq (1 + \varepsilon)\left(\mathrm{rad}_K^r(P_x) + \log d_K\right) + c \tag{2.39}$$

Or, d'après l'inégalité de droite de (2.35), $\mathrm{rad}_K^r(P_x) \leq \mathrm{rad}_K(P_x) + \log d_K$, donc on peut conclure en appliquant la proposition 4. □

2.3.4 Majoration du radical.

Dans cette section nous démontrons la proposition 4 qui intervient dans la démonstration du théorème 9.

Lemmes préliminaires.

Le lemme suivant se démontre (cf., par exemple, [MvF] lemma 6.3) à l'aide du théorème de Riemann-Roch.

Lemme 21. *Soient C une courbe projective définie sur un corps de nombres K et $M \in Div(C)$ un diviseur irréductible de C, défini sur K. Il existe un entier positif n (qui ne dépend que de la courbe C) et une fonction $m : C \longrightarrow \mathbf{P}^1$ tels que nM soit le diviseur des zéros de m, i.e.*

$$nM = m^*(0).$$

On peut prendre, par exemple, $n = 2g + 1$.

On introduit les diviseurs de zéro, de 1 et de l'infini, par rapport à la fonction f.

Pour $a \in \mathbb{P}^1(\overline{\mathbf{Q}})$, on note $f^*(a) \in \mathrm{Div}(C)$ le diviseur effectif sur C défini par :

$$f^*(a) = \sum_{x \in C(\overline{\mathbf{Q}}), f(x)=a} e_x(f)(x),$$

où $e_x(f)$ est l'indice de ramification de la fonction f au point x, et on notera

$$f^*(a)|_U = \sum_{x \in U(\overline{\mathbf{Q}}), f(x)=a} e_x(f)(x),$$

le diviseur restreint à la courbe affine U.

On pose $A = f^*(0)$, $B = f^*(1)$ et $C = f^*(\infty)$ et on les restreint à U. Comme la courbe U et la fonction f sont définies sur K, les diviseurs $A|_U, B|_U$ et $C|_U$ aussi. On les décompose en diviseurs irréductibles :

$$A|_U = e_1 M_1 + \cdots + e_i M_i,$$
$$B|_U = e_{i+1} M_{i+1} + \cdots + e_j M_j,$$
$$C|_U = e_{j+1} M_{j+1} + \cdots + e_k M_k.$$

Pour tout $\nu \in \{1, \ldots, k\}$, on pose $d_\nu = \deg(M_\nu)$. On applique le lemme 21 à tous les diviseurs M_ν et on prend $N = 2g + 1$. On a donc, pour tout $\nu \in \{1, \ldots, k\}$, une fonction $m_\nu : C \longrightarrow \mathbb{P}^1$ telle que

$$N M_\nu = m_\nu^*(0).$$

Nous avons besoin du lemme suivant.

Lemme 22. *On a*

$$\sum_{\nu=1}^{k} d_\nu = m - s.$$

Démonstration du lemme 22.

Pour tout $\nu \in \{1, \ldots, k\}$ on a $d_\nu = \deg(M_\nu) = \mathrm{card}(\mathrm{supp}(M_\nu))$, donc

$$\sum_{\nu=1}^{i} d_\nu = \mathrm{card}(\{x \in U(\overline{\mathbf{Q}}) / f(x) = 0\}).$$

De même, la somme allant de $i+1$ à j compte les points de $U(\overline{\mathbf{Q}})$ s'envoyant sur 1, et celle allant de $j+1$ à k, ceux s'envoyant sur l'infini. Comme $U_\infty = \{P_1, \ldots, P_s\}$ et que, d'après le lemme 20, $f(\{P_1, \ldots, P_s\}) \subset \{0, 1, \infty\}$, alors

$$\sum_{\nu=1}^{k} d_\nu = \mathrm{card}(\{x \in C(\overline{\mathbf{Q}}) / f(x) \in \{0, 1, \infty\}\}) - \mathrm{card}(U_\infty(\overline{\mathbf{Q}})),$$

c'est-à-dire que, $\sum_{\nu=1}^{k} d_\nu = m - s$. □

Lemme clef.

On utilise ici la notion de "bonne réduction" introduite au paragraphe 2.2.3.

D'après les propositions 2 et 3, il existe un ensemble fini $T \subset M_K$ de places (dépendant uniquement de la courbe U) tel que, si on note $\mathcal{B} = \mathrm{Spec}(O_{K,T}) = \mathrm{Spec}(O_K) \setminus T$, il existe un modèle $\mathcal{C}$ de la courbe C au-dessus de $\mathcal{B}$ tel que :

i) toutes les fibres spéciales de ce modèle soient encore des courbes lisses projectives,

ii) la fonction f et les fonctions m_ν s'étendent en des morphismes $\tilde{f}$ et $\tilde{m_\nu}$ de $\mathcal{C}$ dans $\mathbf{P}^1_{O_{K,T}} = \mathbf{P}^1_{\mathcal{B}}$ au-dessus de $\mathcal{B}$.

Lemme 23. *Soit $x \in U(O_{K,S})$ un point S-entier tel que $f(x) \notin \{0, 1, \infty\}$.*

Soit $\wp$ un idéal premier premier appartenant à $\mathcal{B}$, qui contribue au radical de P_x , c'est-à-dire tel que $\wp \in H_x$. Si $\wp \notin S$, alors

$$\log N(\wp) \leq \frac{d_\wp}{N} \sum_{\nu=1}^{k} \max\{0, v_\wp(m_\nu(x))\}.$$

Démonstration du lemme 23.

On fixe $\wp \in \mathcal{B}$ et on pose $\mathcal{U} = \mathcal{C} \setminus \overline{\mathrm{supp}(D)}^{Zar}$. Alors $\mathcal{U}$ est un modèle affine de U au-dessus de $\mathcal{B}$ dont toutes les fibres sont des courbes affines lisses.

Tout point rationnel $x \in C(K) \setminus f^{-1}(\{0, 1, \infty\})$ correspond à un morphisme $\mathrm{Spec}(K) \longrightarrow C$ et se prolonge en une section $\sigma_x : \mathcal{B} \longrightarrow \mathcal{C}$. Le point $f(x) \in \mathbf{P}^1_K$ se prolonge en une section $\sigma_{f(x)} : \mathcal{B} \longrightarrow \mathbf{P}^1_{O_{K,T}}$. De plus, on a $\tilde{f}(\sigma_x(p)) = \sigma_{f(x)}(p)$, i.e. le diagramme suivant, complété avec les sections, est commutatif.

$$\begin{array}{ccc} \mathcal{C} & \to & \mathbf{P}^1_{O_{K,T}} \\ \downarrow & \swarrow & \\ \mathcal{B} & & \end{array}$$

Par définition du radical et de la valuation $\wp$-adique, on a

$$\begin{array}{rcl} \wp \in H_x & \iff & v_\wp(f(x)) > 0 \ \text{ou} \ v_\wp(f(x)) < 0 \ \text{ou} \ v_\wp(1 - f(x)) > 0 \\ & \iff & \mathrm{ord}_\wp(f(x)) > 0 \ \text{ou} \ \mathrm{ord}_\wp(f(x)) < 0 \ \text{ou} \ \mathrm{ord}_\wp(1 - f(x)) > 0 \\ & \iff & \sigma_{f(x)}(\wp) = \tilde{0} \ \text{ou} \ \sigma_{f(x)}(\wp) = \tilde{\infty} \ \text{ou} \ \sigma_{f(x)}(\wp) = \tilde{1}, \\ & \iff & \tilde{f}(\sigma_x(\wp)) = \tilde{0} \ \text{ou} \ \tilde{f}(\sigma_x(\wp)) = \tilde{\infty} \ \text{ou} \ \tilde{f}(\sigma_x(\wp)) = \tilde{1} \\ & \iff & \sigma_x(\wp) \in \mathrm{supp}(\tilde{A}) \ \text{ou} \ \sigma_x(\wp) \in \mathrm{supp}(\tilde{C}) \ \text{ou} \ \sigma_x(\wp) \in \mathrm{supp}(\tilde{B}), \end{array}$$

où les diviseurs $\tilde{A}, \tilde{B}$ et $\tilde{C}$ appartiennent à $\mathrm{Div}(\mathcal{C}_\wp)$.

Si $D = \sum e_x(f)(x)$ est un diviseur de C défini sur K (i.e. la somme se fait sur des points $x \in C(K)$), on note $D|_U$, le diviseur restreint à U, c'est-à-dire

que la somme ne porte que sur les $x \in U(K)$ et, $\tilde{D} = \sum e_x(f)\sigma_x(\wp)$. (A priori, les points $\sigma_x(\wp) \in \mathcal{C}_\wp$ et, $\sigma_x(\wp) \in \mathcal{U}_\wp$ si et seulement si, x appartient à U et est $\wp$-entier). De plus, $\mathrm{supp}(\tilde{D}) \cap \mathcal{U}_\wp = \mathrm{supp}(\widetilde{D|_U})$.

Si on suppose que le point x appartient à $U(O_{K,S})$ et que $\wp \notin S$, alors le point réduit se trouve sur la courbe affine réduite, i.e. $\sigma_x(\wp) \in \mathcal{U}_\wp$. Dans ce cas là, on a donc

$$\begin{aligned} \wp \in H_x \setminus S \quad &\Longrightarrow \quad \sigma_x(\wp) \in (\mathrm{supp}(\widetilde{A|_U})) \cup (\mathrm{supp}(\widetilde{C|_U})) \cup (\mathrm{supp}(\widetilde{B|_U})) \\ &\Longleftrightarrow \quad \exists \mu \in \{1, \dots, k\}, \ \ \sigma_x(\wp) \in \mathrm{supp}(\widetilde{M_\mu}) \\ &\Longleftrightarrow \quad \exists \mu \in \{1, \dots, k\}, \ \ \mathrm{ord}_{\sigma_x(\wp)}(\widetilde{M_\mu}) \geq 1. \end{aligned}$$

Par définition, $v_\wp(m_\mu(x)) = \frac{\mathrm{ord}_\wp(m_\mu(x))}{d_\wp} \log N(\wp)$.
Comme $\mathrm{ord}_\wp(m_\mu(x)) \geq \mathrm{mult}_{\sigma_x(\wp)}(\widetilde{m_\mu}) = N\mathrm{ord}_{\sigma_x(\wp)}(\widetilde{M_\mu}) \geq N$, alors

$$v_\wp(m_\mu(x)) \geq \frac{N}{d_\wp} \log N(\wp) \ \text{ i.e. } \ \log N(\wp) \leq \frac{d_\wp}{N} v_\wp(m_\mu(x)).$$

Donc, si $x \in U(O_{K,S})$ et $\wp \in (\mathcal{B} \cap H_x) \setminus S$, alors

$$\log N(\wp) \leq \frac{d_\wp}{N} \sum_{\nu=1}^{k} \max\{0, v_\wp(m_\nu(x))\}.$$

Ceci achève la preuve du lemme 23. □

Démonstration de la proposition 4.

Soit $x \in U(O_{K,S})$ tel que $f(x) \notin \{0, 1, \infty\}$. On note $H = H_x$.

Le radical de P_x est la somme des $\log N(\wp)$ pour tous les idéaux $\wp$ dans H. Or, l'ensemble $H = ((H \cap \mathcal{B}) \setminus S) \cup (H \cap \mathcal{B} \cap S) \cup (H \cap T)$, et comme les deux dernières sommes sont inférieures ou égales à celles portant, respectivement, sur $S \cap M_K^0$ et $T \cap M_K^0$, c'est-à-dire Σ_S et Σ_T, on a

$$\mathrm{rad}_K(P_x) \leq \sum_{\wp \in (H \cap \mathcal{B}) \setminus S} \log N(\wp) + \Sigma_S + \Sigma_T.$$

Grâce au lemme 23,

$$\mathrm{rad}_K(P_x) \leq \sum_{\wp \in (H \cap \mathcal{B}) \setminus S} \frac{d_\wp}{N} \sum_{\nu=1}^{k} \max\{0, v_\wp(m_\nu(x))\} + \Sigma_S + \Sigma_T,$$

et puisque la somme $\sum_{v \in M_K^\infty} \frac{d_v}{N} \sum_{\nu=1}^{k} \max\{0, v(m_\nu(x))\}$ est positive, on peut l'ajouter au membre de droite de la dernière inégalité. De plus, la somme

portant sur les idéaux de $(H\cap\mathcal{B})\setminus S$ est majorée par la même somme portant sur les $v_\wp \in M_K^0$. Ainsi

$$\mathrm{rad}_K(P_x) \leq \sum_{\nu=1}^{k} \frac{1}{N} \sum_{v\in M_K} d_v \max\{0, v(m_\nu(x))\} + \Sigma_S + \Sigma_T.$$

D'autre part, comme $v(m_\nu(x)) = -\log|m_\nu(x)|_v = \log\frac{1}{|m_\nu(x)|_v}$, alors

$$\sum_{v\in M_K} d_v \max\{0, v(m_\nu(x))\} = \sum_{v\in M_K} d_v \log\max\left\{0, \frac{1}{|m_\nu(x)|_v}\right\}$$

$$= h_K((m_\nu(x))^{-1}) = h_K(m_\nu(x)),$$

et comme $\deg(m_\nu) = N\deg(M_\nu) = Nd_\nu$ et $\deg(f) = d$, alors, d'après l'inégalité (2.33) du paragraphe 2.2.1, on a

$$h_K(m_\nu(x)) = \frac{Nd_\nu}{d} h_K(f(x)) + O\left(\sqrt{h_K(f(x))}\right),$$

avec une constante implicite ne dépendant que du degré de K, de la courbe C et des fonctions m_ν et f. Ainsi

$$\mathrm{rad}_K(P_x) \leq \frac{1}{d}\left(\sum_{\nu=1}^{k} d_\nu\right) h_K(f(x)) + c_1\sqrt{h_K(f(x))} + \Sigma_S + \Sigma_T,$$

où la constante c_1 dépend du degré $[K:\mathbf{Q}]$, mais pas du corps K lui-même, ni du point x ni de l'ensemble de places S.

D'après les lemmes 22 et 20, $\sum_{\nu=1}^{k} d_\nu = m - s = \chi(U) + d$, donc

$$\mathrm{rad}_K(P_x) \leq \left(\frac{\chi(U)}{d} + 1\right) h_K(f(x)) + c_1\sqrt{h_K(f(x))} + \Sigma_S + \Sigma_T,$$

ce qui démontre la proposition 4. □

2.4 De Siegel uniforme à *abc*.

2.4.1 L'hypothèse "Siegel uniforme".

En nous inspirant de la preuve de Moret-Bailly ([M-B]) démontrant la conjecture *abc* sous un hypothétique "Mordell effectif" pour la courbe d'équation $y^2+y=x^5$, nous complétons ici une sorte d'équivalence entre la conjecture *abc* et une version effective conjecturale du théorème de Siegel. Étant donnée une courbe quelconque vérifiant les hypothèses du théorème 11, une borne effective sur la hauteur de ses points S-entiers faisant intervenir le discriminant du corps de nombres ainsi que les places de l'ensemble S, permettrait de démontrer un énoncé dans le sens de la conjecture *abc*. (Remarquons

toutefois que l'ensemble des points entiers étant inclus dans celui des points rationnels, le théorème 10 que nous démontrons ci-après est plus fort que celui démontré dans [M-B].)

Pour comparer ces énoncés, considérons une variante de la conjecture *abc*.

Pour un corps de nombres K et une fonction ϕ croissante positive définie sur $\mathbf{R}$, rappelons la conjecture suivante.

Conjecture 2 *abc* (K, ϕ)

Pour tout triplet (a, b, c) *de nombres algébriques appartenant au corps de nombres* K*, non nuls et tels que* $a + b = c$*, on a*

$$h_K(a : b : c) \leq \phi(\mathrm{rad}_K(a : b : c)).$$

La conjecture 1 est obtenue à partir de la conjecture 2 en prenant $\phi(x) = (1+\varepsilon)x + c_{\varepsilon,K}$. C'est ce qu'on appelle la "version forte" de la conjecture *abc*. Une version un peu plus faible correspondrait au cas où $\phi(x) = c_1 x + c_2$ avec c_1 une constante absolue supérieure ou égale à 1 et c_2 dépendant de K.

Le meilleur énoncé sur le sujet à l'heure actuelle est dû à C. L. Stewart et K. Yu (cf. [S-Y] ou théorème 16, section 2.5) et correspond à $\phi(x) = c\, x^3 \exp(\frac{1}{3}x)$, pour $K = \mathbf{Q}$.

Étant donnés un corps de nombres K, une courbe affine U définie sur K telle que $\chi(U) < 0$ et une fonction hauteur h_U sur U, associée à un diviseur de degré 1, le théorème 13 suggère l'hypothèse suivante du type "Siegel uniforme", déjà mentionnée dans l'introduction.

Hypothèse 1 *Siegel* (U, K)

Pour tout entier naturel $\delta > 0$*, il existe des constantes* $k_1(U, h, \delta) > 1$*,* $k_2(U, h, \delta) > 1$ *et* $k_3(U, h, \delta) > 0$ *telles que, pour toute extension finie* L/K *de degré* $[L : \mathbf{Q}] \leq \delta$*, pour tout sous-ensemble fini* S *de places ultramétriques de* L *et pour tout point* S*-entier* x *de* U*, on ait*

$$h_{U,L}(x) \leq k_1 \sum_{\ell \in S} \log N_{L/\mathbf{Q}}(\ell) + k_2 \log d_L + k_3,$$

où $h_{U,L} = [L : \mathbf{Q}] h_U$.

Remarques.

i) L'hypothèse *Siegel* (U, K) est indépendante de la fonction hauteur choisie. On peut prendre, par exemple, $h_U = h_f = h \circ f$ où h est la hauteur logarithmique absolue sur $\mathbf{P}^1$, pour n'importe quelle fonction rationnelle $f \in K(U)$ (cf. l'inégalité (2.32) du paragraphe 2.2.1).

ii) L'hypothèse 1 est trivialement fausse si on ne suppose pas $\chi(U) < 0$. (La droite affine $\mathbf{A}^1$ est de genre nul et a un seul point à l'infini. Elle admet une infinité de points à coordonnées dans $\mathbf{Z}$. L'équation de Pell-Fermat, $x^2 - Dy^2 = 1$, où $D \in \mathbf{N} \setminus \{0\}$ n'est pas un carré, définit une courbe affine

de genre nul et ayant un point à l'infini. Elle admet une infinité de points entiers. Un exemple sur un corps de nombres K est fourni par l'équation $xy = 1$, qui définit une courbe de genre nul et ayant un point à l'infini. Les solutions dans O_K correspondent aux unités.)

iii) Une version optimiste de cette hypothèse serait de considérer des constantes k_1 et k_2 indépendantes de δ (cf. le théorème 13).

L'hypothèse 1 est suggérée par le théorème 13, mais peut aussi être étayée de la façon suivante.

Tout d'abord, comme cela a été rappelé au début de cette section, celle-ci a été inspirée par l'hypothèse de type "Mordell effectif" de [M-B], qui pourrait s'appliquer, en particulier, aux points entiers de courbes affines de genre ≥ 2. Étant donné un corps de nombres K, une courbe algébrique projective X définie sur K, de genre ≥ 2, et h_X une hauteur définie sur X associée à un diviseur de degré 1, Moret-Bailly fait l'hypothèse suivante.

Hypothèse 4. *M.E.(X)*

Pour tout entier naturel $\delta \geq 1$, il existe des constantes réelles $A(X, h, \delta)$ et $B(X, h, \delta)$ telles que, pour toute extension finie L/K de degré $[L : \mathbf{Q}] \leq \delta$ et tout point L-rationnel x de X, on ait

$$h_X(x) \leq \frac{1}{\delta} A \log d_L + B.$$

Cette hypothèse avait déjà été formulée dans un cadre beaucoup plus général par P. Vojta (cf. la conjecture 4.1 du chapitre IX de [La4]).

Du côté des résultats inconditionnels, on a le théorème de Yu. Bilu ([Bi] théorème 1.1) sur les revêtements galoisiens de la droite projective. On énonce ici un cas pariticulier. (Sur les courbes qui sont revêtements galoisiens de la droite projective on a aussi les travaux de R. Dvornicich et U. Zannier [DZ] et de D. Poulakis [P1] et [P2].)

Théorème 14. *(Bilu)*

Soient K un corps de nombres et C la courbe algébrique projective définie sur K par l'équation affine

$$y^m = g(x),$$

où $g \in K[X]$ est un polynôme non nul, de degré n. Pour tout ensemble fini $S \subset M_K^0$, on pose

$$C(x, K, S) = \{P \in C(K) / \ x(P) \in O_{K,S}\}.$$

Si $x : C \to \mathbf{P}^1$ est un revêtement galoisien (i.e. l'extension $\overline{\mathbf{Q}}(x, y)/\overline{\mathbf{Q}}(x)$ est galoisienne) et C est de genre ≥ 1, alors, pour tout $P \in C(x, K, S)$ on a

$$h(x(P)) \leq P^{N_1[K:\mathbf{Q}]} \left(d_K \prod_{\wp \in S} N(\wp) \right)^{N_2} e^{\psi},$$

où $\psi = 100\,\mathrm{card}(S)N_2\,(\log(N\,\mathrm{card}(S)) + O(1)) + [K : \mathbf{Q}]N_3\,(h(g) + O(N))$, *les nombres* N, N_1, N_2 *et* N_3 *ne dépendent que de* m *et* n, $h(g)$ *désigne la hauteur du polynôme* g, *à savoir, la hauteur du point de l'espace projectif défini par les coefficients de* g, *et* P *est le maximum des caractéristiques résiduelles de l'ensemble* S.

On voit apparaître ici, même si c'est avec une exponentielle "de trop", les deux termes sur lesquels on a mis l'accent, à savoir, le discriminant du corps de rationnalité et la somme des normes des idéaux premiers correspondant aux places de l'ensemble S.

Il est d'ailleurs nécessaire de faire intervenir le discriminant dans la borne, comme le montre le raisonnement suivant.

Soit U la courbe affine plane définie par l'équation $f(x, y) = 0$, où

$$f(X, Y) = Y^n + Y^{n-1}a_{n-1}(X) + \cdots + a_0(X) \in \mathbf{Z}[X, Y] \setminus \{0\},$$

avec les $a_i \in \mathbf{Z}[X]$. Soit $x \in \mathbf{Z}$ tel que le polynôme $f(x, Y)$ soit irréductible dans $\mathbf{Z}[Y]$. Notons ξ_x une racine de $f(x, Y)$ et $K_x = \mathbf{Q}(\xi_x)$ le corps qu'elle engendre sur $\mathbf{Q}$. Alors $[K_x : \mathbf{Q}] = n$, $\xi_x \in O_{K_x}$ et $(1 : x : \xi_x) \in U(O_{K_x})$. Cependant

$$h_{K_x}(1 : x : \xi_x) \geq h_{K_x}(x) = [K_x : \mathbf{Q}] \log |x| = n \log |x|.$$

Ceci montre qu'il n'existe pas de fonction ψ telle que, pour tout corps de nombres K et tout point $P \in U(O_K)$,

$$h_K(P) \leq \psi([K : \mathbf{Q}]).$$

De plus, si on note d_{K_x} la valeur absolue du discriminant de K_x, Δ_x celle du discriminant de $\mathbf{Z}[\xi_x]/\mathbf{Z}$ et $m_x = [O_{K_x} : \mathbf{Z}[\xi_x]]$, alors

$$d_{K_x} = \frac{\Delta_x}{m_x^2} \leq \Delta_x = N_{K_x/\mathbf{Q}}(f'(x, \xi_x))$$

où f' est la dérivée de f par rapport à la deuxième variable Y. Comme la norme de $f'(x, \xi_x)$ est égale au produit des $|f'(x, \xi_i)|$ pour ξ_i racine de $f(x, Y)$, on a

$$\log d_{K_x} \leq \sum_{\xi_i} \log |f'(x, \xi_i)| \leq c_1 \log |x| + c_2,$$

où les constantes c_i ne dépendent ni du point x ni du discriminant de K_x. On peut donc espérer avoir une borne pour la hauteur en fonction du discriminant d_K.

Par ailleurs, lorsque l'ensemble de points rationnels $U(K)$ est infini (par exemple, si U est de genre nul et $s \geq 3$, ou bien si U est une courbe elliptique

de rang de Mordell-Weil supérieur ou égal à 1), il n'existe pas de fonction ψ telle que, pour tout ensemble fini S de places de K et tout point S-entier P de U,

$$h_K(P) \leq \psi(\log d_{K_x}).$$

Une autre motivation importante pour l'hypothèse 1 provient de la théorie des corps de fonctions. L'analogue de l'hypothèse *Siegel* (U, K) sur un corps de fonctions a été démontré et on y voit apparaître, en particulier, la dépendance en l'ensemble de places S . Pour les détails, on peut se reporter à l'appendice.

En tout cas, l'hypothèse 1 nous permet de démontrer le théorème 10.

2.4.2 Vers *abc*.

Rappelons le théorème 10 énoncé dans l'introduction.

Théorème 10

Soient K un corps de nombres, U une courbe algébrique affine non exceptionnelle (i.e. telle que $\chi(U) < 0$) définie sur K et h_U une hauteur définie sur U associée à un diviseur de degré 1.

L'hypothèse Siegel (U, K) implique la conjecture abc(K, ϕ) pour une fonction explicite ϕ linéaire en x.

Remarque 4. *On peut choisir plus précisément dans le théorème 10 :*

$$\phi(x) = \eta_1 x + \eta_2 \log d_K + \eta_3,$$

où les constantes η_2 et η_3 ne dépendent que du degré d de la fonction de Belyĭ associée à la courbe U et du degré $[K : \mathbf{Q}]$ du corps de base, et la constante η_1 dépend, en plus de d et de $[K : \mathbf{Q}]$, de la courbe U.

Démonstration du théorème 10.

Soit U une courbe affine définie sur un corps de nombres K, de genre g et ayant s points à l'infini, notés $\{P_1, \ldots, P_s\}$, et telle que $\chi(U) < 0$. Soit C une courbe projective la contenant. Notons Φ_D le plongement affine de U décrit au paragraphe 2.2.2.

On applique le théorème 12 à la courbe C. Soit $f : C \longrightarrow \mathbf{P}^1$ une fonction de Belyĭ de degré d, non ramifiée en dehors de $0, 1$ et l'infini, et telle que $f(\{P_1, \ldots, P_s\}) \subset \{0, 1, \infty\}$. On note $X = X_f = C \setminus f^{-1}(\{0, 1, \infty\})$ la courbe affine obtenue à partir de C en lui enlevant les points de ramification de la fonction f et $Y = \mathbf{P}^1 \setminus \{0, 1, \infty\}$. Alors $X_f \subset U$ et le morphisme $f : X_f \longrightarrow Y$ au-dessus de K est fini, surjectif et non ramifié, c'est-à-dire que f est un revêtement étale de Y.

D'après la proposition 3, il existe un ensemble fini S_0 de places de M_K^0 ne dépendant que de la courbe C et du morphisme f, et un modèle $\mathcal{C}$ de

C sur O_{K,S_0} tels que le revêtement f s'étend en un revêtement $\tilde{f} : \mathcal{C} \longrightarrow \mathbf{P}^1_{O_{K,S_0}}$ au-dessus de O_{K,S_0}, non ramifié en dehors de $\{0,1,\infty\}$. Si $\mathcal{X} = \mathcal{C}\backslash\overline{\tilde{f}^{-1}(\{0,1,\infty\})}^{Zar}$, alors $\tilde{f} : \mathcal{X} \longrightarrow \mathbf{P}^1_{O_{K,S_0}}\backslash\overline{\{0,1,\infty\}}^{Zar}$ est un revêtement étale, de degré égal au degré de f, c'est-à-dire d.

Soient a, b et c des nombres algébriques non nuls appartenant à K tels que $a + b = c$. On pose

$$S_1 = \{\wp \in \mathcal{P}_K/\ \ v_\wp(a/c) < 0 \ \text{ ou } \ v_\wp(a/c) > 0 \ \text{ ou } \ v_\wp(b/c) > 0\}.$$

(Avec les notations du paragraphe 2.2.1, on a $S_1 = H_{a/c}$.) Si $P(S_1) = \{p \in \mathcal{P}/\ \exists \wp \in S_1,\ \ \wp|p\}$, alors quitte à rajouter un ou deux nombres premiers, on peut supposer, dans toute la suite, que $\mathrm{card}(P(S_1)) \geq 3$.

On pose aussi, $S = S_0 \cup S_1$.

Le point $y = \frac{a}{c}$ de la courbe Y a pour coordonnées afines $(y, \frac{1}{y}, \frac{1}{1-y}) = (\frac{a}{c}, \frac{c}{a}, \frac{c}{b})$ (cf. le paragraphe 2.2.2 où l'on rappelle le plongement affine de $Y = \mathbf{P}^1 \setminus \{0,1,\infty\}$ dans $\mathbf{A}^3$). Comme les nombres a, b et c sont des S_1-unités, alors $(\frac{a}{c}, \frac{c}{a}, \frac{c}{b}) \in \mathbf{A}^3(O_{K,S_1})$ et y est un point S_1-entier de Y, et a fortiori, S-entier.

Soit $x \in X(\overline{\mathbf{Q}})$ un antécédent par f de y.

Lemme 24. *Le corps de définition $L = K(x)$ du point x est une extension finie de K de degré $[L : K] \leq \deg(f) = d$, non ramifiée en dehors de l'ensemble S, et, de plus, le point x se prolonge en une section σ_x au-dessus de $O_{L,S'}$ où $S' = \{\ell \in M_L/\ \exists \wp \in S,\ \ \ell|\wp\}$.*

Démonstration du lemme 24.

On notera $\mathcal{Y} = Y_{O_{K,S}} = \mathrm{Spec}(O_{K,S}[T, \frac{1}{T(1-T)}])$. On a alors un morphisme de $\mathrm{Spec}(O_{K,S})$ dans $\mathcal{Y}$. Considérons le produit fibré de $\mathcal{X}$ par $\mathrm{Spec}(O_{K,S})$ au-dessus de $\mathcal{Y}$.

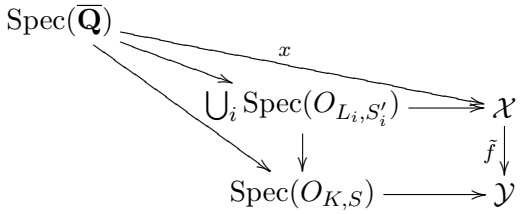
$$\begin{array}{ccc} \mathrm{Spec}(O_{K,S}) \times_{\mathcal{Y}} \mathcal{X} & \longrightarrow & \mathcal{X} \\ pr_1 \downarrow & & \downarrow \tilde{f} \\ \mathrm{Spec}(O_{K,S}) & \longrightarrow & \mathcal{Y} \end{array}$$

Le schéma $\mathrm{Spec}(O_{K,S}) \times_{\mathcal{Y}} \mathcal{X}$ est obtenu à partir de $\mathcal{X}$ par changement de base, de $\mathcal{Y}$ à $\mathrm{Spec}(O_{K,S})$; le morphisme $\tilde{f} : \mathcal{X} \longrightarrow \mathcal{Y}$ étant un revêtement étale, il en est donc de même de $pr_1 : \mathrm{Spec}(O_{K,S}) \times_{\mathcal{Y}} \mathcal{X} \longrightarrow \mathrm{Spec}(O_{K,S})$ (cf. [SGA] IX proposition 1.3). De plus, le degré du morphisme pr_1 est égal à celui de $\tilde{f}$, c'est-à-dire d.

D'après le lemme 15, $\mathrm{Spec}(O_{K,S}) \times_Y \mathcal{X} = \bigcup_{i \in I} \mathrm{Spec}(O_{L_i,S_i'})$, où, pour tout $i \in I$, l'extension L_i/K est finie, de degré $[L_i : K] \leq \deg(pr_1) = d$, non ramifiée en dehors de l'ensemble S, et $S_i' = \{\ell \in M_{L_i}/\ \exists \wp \in S,\ \ \ell|\wp\}$.

Par ailleurs, le point x de $\mathcal{X}$ à valeurs dans $\overline{\mathbf{Q}}$ correspond à un morphisme $x : \mathrm{Spec}(\overline{\mathbf{Q}}) \longrightarrow \mathcal{X}$, et l'inclusion $O_{K,S} \subset \overline{\mathbf{Q}}$, nous fournit un autre morphisme $\mathrm{Spec}(\overline{\mathbf{Q}}) \longrightarrow \mathrm{Spec}(O_{K,S})$.

Par la propriété universelle du produit fibré, on en déduit qu'il existe un morphisme $\mathrm{Spec}(\overline{\mathbf{Q}}) \longrightarrow \bigcup_{i\in I} \mathrm{Spec}(O_{L_i,S_i'})$ tel que le diagramme suivant soit commutatif.



Le spectre d'un corps étant réduit à un point, le schéma $\mathrm{Spec}(\overline{\mathbf{Q}}) = \{(0)\}$ s'envoie sur une des composantes connexes de $\bigcup_i \mathrm{Spec}(O_{L_i,S_i'})$, disons sur $\mathrm{Spec}(O_{L,S'})$.

Ainsi, le morphisme $x : \mathrm{Spec}(\overline{\mathbf{Q}}) \longrightarrow \mathcal{X}$ se factorise par $\mathrm{Spec}(O_{L,S'})$, ce qui revient à dire que x se prolonge en une section de $\mathcal{X}$ au-dessus de $\mathrm{Spec}(O_{L,S'})$. Ceci démontre le lemme 24. □

Appliquons l'hypothèse 1 à la courbe U définie sur K, à $\delta = d[K : \mathbf{Q}]$, à l'extension de corps de nombres L/K de degré $[L : \mathbf{Q}] = [L : K][K : \mathbf{Q}] \leq \delta$, à la fonction hauteur $h_{U,L} = h_{f,L} = \frac{1}{\deg(f)}(h_L \circ f)$ relative à la fonction de Belyĭ f et au corps L, à l'ensemble de places $S' \subset M_L$ et au point $x \in X \subset U$ qui relève y. On a

$$h_{f,L}(x) \leq k_1 \sum_{\ell\in S'} \log N_{L/\mathbf{Q}}(\ell) + k_2 \log d_L + k_3, \tag{2.40}$$

où les constantes $k_i(U, h_f, d)_{i\in\{1,2,3\}}$ dépendent de la courbe U, de la fonction hauteur $h_{f,L}$ et du degré d de la fonction f, mais pas du point x. En fait, le corps K et la courbe U étant fixés dès le début, les nombres k_1, k_2 et k_3 ne dépendent pas de a, b et c.

Regardons les éléments qui apparaissent dans cette inégalité.

D'après l'égalité (2.30), et parce que $f(x) = \frac{a}{c}$,

$$h_{f,L}(x) = \frac{1}{\deg(f)} h_L(f(x)) = \frac{[L : K]}{d} h_K(a : c).$$

De plus, pour toute place v de M_K, on a

$$|b|_v = |c - a|_v \leq 2 \max\{|a|_v, |c|_v\},$$

donc

$$h_K(a : c) \geq h_K(a : b : c) - [K : \mathbf{Q}] \log 2,$$

et comme, $[L : K][K : \mathbf{Q}] = [L : \mathbf{Q}] \leq d[K : \mathbf{Q}]$, alors

$$h_{f,L}(x) \geq \frac{[L : K]}{d} h_K(a : b : c) - [K : \mathbf{Q}] \log 2. \tag{2.41}$$

Grâce à la formule (2.28) on a

$$\sum_{\ell\in S'} \log N_{L/\mathbf{Q}}(\ell) = \Sigma_{S'} \leq [L:K]\Sigma_S. \tag{2.42}$$

D'après l'égalité (2.29), $\log d_L = \log N_{K/\mathbf{Q}}(\delta_{L/K}) + [L:K]\log d_K$. Pour majorer la norme du discriminant relatif $\delta_{L/K}$ de L/K, on applique le lemme 19 à l'extension L/K, qui d'après le lemme 24 a pour ensemble de ramification $R_{L/K} \subset S$. D'où

$$\log d_L \leq [L:K]\left(\log d_K + \Sigma_S + 2[K:\mathbf{Q}]\log[L:K]\frac{\Sigma_S}{\log \Sigma_S}\right). \tag{2.43}$$

En remplaçant dans l'inégalité (2.40) les inégalités (2.41), (2.42) et (2.43), et en remarquant que

$$\Sigma_S = \sum_{\wp\in S_0\cup S_1} \log N(\wp) \leq \sum_{\wp\in S_0} \log N(\wp) + \sum_{\wp\in S_1} \log N(\wp) = \mathrm{rad}_K(a:b:c) + k_0,$$

où $k_0 = \Sigma_{S_0}$ dépend de la courbe U, mais pas du point y ni de l'ensemble de places S_1, on obtient l'inégalité

$$h_K(a:b:c) \leq \gamma_1 \mathrm{rad}_K(a:b:c) + \gamma_2 \frac{\mathrm{rad}_K(a:b:c)+k_0}{\log(\mathrm{rad}_K(a:b:c)+k_0)} + \gamma_3,$$

$$\text{où } \gamma_1 = (k_1+k_2)d, \ \gamma_2 = 2k_2 d\log d[K:\mathbf{Q}]$$

$$\text{et } \gamma_3 = dk_2\log d_K + d\left([K:\mathbf{Q}]\log 2 + k_0(k_1+k_2)+k_3\right).$$

Les constantes $(\gamma_i)_{1\leq i\leq 3}$ et k_0 dépendent de la courbe U et du degré du corps de nombres K qui ont été fixés au début de la démonstration, mais pas du point $y = \frac{a}{c}$. Ceci achève la démonstration du théorème 10. □

2.5 Cas de $\mathbb{P}^1 \setminus \{0,1,\infty\}$.

2.5.1 Introduction.

Dans le cas où l'on considère la droite projective privée de $0, 1$ et l'infini, c'est-à-dire dans le cas où notre courbe affine U est $\mathbf{P}^1\setminus\{0,1,\infty\}$, la situation est beaucoup plus simple : sa complétée C est la droite projective $\mathbf{P}^1$, le genre g est nul, la fonction de Belyĭ du théorème 12 est l'identité, le degré $d = 1$, $m = s = 3$, et dans l'inégalité (2.32), le terme avec la racine carrée de la hauteur disparaît. En particulier, la borne pour la hauteur du théorème 2.3 ne dépend que de l'ensemble de places S.

Précisément, on obtient le théorème 15 ci-dessous qui montre l'équivalence entre la conjecture *abc* et une version uniforme du théorème de Siegel sur

$\mathbf{P}^1 \setminus \{0, 1, \infty\}$ en S-entiers. Pour démontrer cette équivalence, au lieu de reprendre les démonstrations des sections 2.3 et 2.4, on en présente une autre, à l'aide de l'équation en S-unités.

Soit K un corps de nombres. Pour tout ensemble fini S de places de K contenant les places archimédiennes, considérons l'équation classique en S-unités

$$u + v = 1 \tag{2.44}$$

avec u et v appartenant à $O_{K,S}^*$. On peut aussi considérer l'équation plus générale

$$Au + Bv = 1 \tag{2.45}$$

où A et B sont des éléments de K non nuls et u et v appartiennent à $O_{K,S}^*$.

Depuis les travaux de Siegel [Si2] et Mahler ([Mah1] et [Mah2]), on sait que l'ensemble des solutions de l'équation (2.45) est fini. Les premières versions effectives sont dues à Baker et se basent sur des formes linéaires de logarithmes. Les meilleurs bornes obtenues jusqu'à présent sont celles de Bugeaud-Györy [BG] ; la démonstration utilise une estimation archimédienne de M. Waldschmidt [Wa2] et une estimation p-adique de K. Yu [Yu1].

Bombieri et Cohen ([Bo1], [Bo-Co]) obtiennent des résultats effectifs sur plusieurs problèmes d'approximation diophantienne et, en particulier, des bornes pour les solutions de l'équation (2.45), avec des techniques d'approximation diophantienne (sans utiliser la méthode de Baker). Ils utilisent le lemme de Dyson pour obtenir une nouvelle version du principe de Thue-Siegel et de la géométrie des nombres. Bugeaud [Bu1] reprend cette nouvelle méthode en remplaçant le principe de Thue-Siegel par des formes linéaires en deux ou trois logarithmes. En ce qui concerne l'équation (2.45), il améliore le résultat de [Bo-Co] ; mais la borne de [BG] reste de qualité légèrement supérieure à celle obtenue dans [Bu1]. (Cf. [Bu2] pour un aperçu.)

On rappelle la notation, pour un ensemble fini S de places ultramétriques d'un corps de nombres K,

$$\Sigma_S = \sum_{\wp \in S} \log N(\wp),$$

et la conjecture 2 déjà énoncée dans l'introduction et dans la section 2.4 :

Conjecture 2 *abc* (K, ϕ)

Pour tout triplet (a, b, c) *de nombres algébriques appartenant au corps de nombres* K*, non nuls et tels que* $a + b = c$*, on a*

$$h_K(a : b : c) \leq \phi(\mathrm{rad}_K(a : b : c)).$$

Pour un corps de nombres K et une fonction ϕ (dépendant de K), rappelons les hypothèses 2 et 3, justifiées, en quelque sorte, par le théorème 15.

On rappelle que la conjecture 1 est obtenue à partir de la conjecture 2 en prenant $\phi(x) = (1+\varepsilon)x + c_{\varepsilon,K}$. L'hypothèse 3 ci-dessus avec $\phi(x) = c_1 x + c_2$ est le cas particulier de l'hypothèse 1, lorsque $U = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ et $\delta = 1$, .

Hypothèse 2 $(u + v = 1)\,(K, \phi)$

Pour tout ensemble fini $S \subset M_K^0$ et tout couple (u, v) de S-unités vérifiant l'équation (2.44), on a

$$\max\{h_K(u), h_K(v)\} \leq \phi\,(\Sigma_S)\,.$$

Hypothèse 3 *Siegel* $(\mathbf{P}^1 \setminus \{0, 1, \infty\}, K, \phi)$

Pour tout ensemble fini $S \subset M_K^0$ et tout point S-entier P de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, on a

$$h_K(P) < \phi\,(\Sigma_S)\,.$$

Pour tout couple (A, B) d'éléments non nuls de K, faisons l'hypothèse suivante, qui généralise l'hypothèse 2.

Hypothèse 5. $(Au + Bv = 1)\,(K, \phi)$

Pour tout ensemble fini $S \subset M_K^0$ et tout couple (u, v) de S-unités vérifiant l'équation (2.45), on a

$$\max\{h_K(u), h_K(v)\} \leq \phi\,(\Sigma_S + c_{AB}) + c'_{AB},$$

où $c_{AB} = \Sigma_{T_{AB}}$ *avec* $T_{AB} = \{\wp \in \mathcal{P}_K /\ v_\wp(A) \neq 0 \ \ ou \ \ v_\wp(B) \neq 0\}$,
et $c'_{AB} = h_K(A^{-1} : B^{-1} : 1)$.

2.5.2 $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, *abc* et les S-unités.

Le théorème suivant montre que, étant donnés un corps de nombres et une fonction ϕ, la conjecture 2, variante de la conjecture *abc*, l'hypothèse 2 sur l'équation $u + v = 1$, l'hypothèse 5 sur l'équation $Au + Bv = 1$ et l'hypothèse 3 sur les points S-entiers de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ sont quatre énoncés équivalents.

Théorème 15. *Soient K un corps de nombres et ϕ une fonction positive croissante définie sur $\mathbf{R}_+$.*

i) La conjecture 2 implique l'hypothèse 2.

ii) L'hypothèse 2 est équivalente à l'hypothèse 5.

iii) L'hypothèse 2 est équivalente à l'hypothèse 3.

iv) L'hypothèse 2 relative à K et à ϕ implique la conjecture 2 relative à K et à la fonction $(\phi + [K : \mathbf{Q}] \log 2)$.

Remarque 5. *Si l'on considère des points entiers sur* $\mathbf{Z}$*, i.e.* $K = \mathbf{Q}$ *et* $S = \emptyset$*, le théorème 15 est vide car l'ensemble* $U(\mathbf{Z})$ *est lui-même vide, ainsi que l'ensemble des solutions de l'équation (2.44). Le problème n'est intéressant que si l'on fait varier* S*.*

Démonstration du théorème 15.

On fixe K et ϕ vérifiant les hypothèses du théorème.

La conjecture 2 implique l'hypothèse 2.

Soient S un ensemble fini de places de M_K^0 et u, v des S-unités de K vérifiant l'équation (2.45).

On pose $u = \frac{a}{c}$ et $v = \frac{b}{c}$ avec a, b et c des nombres non nuls de K. Alors

$$u + v = 1 \Leftrightarrow a + b = c.$$

Pour le triplet (a, b, c) la conjecture 2 nous donne l'inégalité suivante

$$h_K(a : b : c) \leq \phi\left(\mathrm{rad}_K(a : b : c)\right). \tag{2.46}$$

Par ailleurs, on a

$$h_K(a : b : c) = h_K(u : v : 1) \geq \max\{h_K(u), h_K(v)\}$$

et

$$\mathrm{rad}_K(a : b : c) = \mathrm{rad}_K(u : 1 - u : 1) = \sum_{\wp \in H_u} \log N(\wp),$$

où $H_u = \{\wp \in \mathcal{P}_K / \ v_\wp(u) < 0 \ \text{ ou } \ v_\wp(u) > 0 \ \text{ ou } \ v_\wp(1-u) > 0\}$.

Comme u et $1 - u$ sont des S-unités, si la valuation $v_\wp$ n'appartient pas à S, $v_\wp(u)$ et $v_\wp(1 - u)$ sont nulles, et donc la valuation $v_\wp$ n'appartient pas à H_u, c'est-à-dire que

$$(v_\wp \in H_u \Rightarrow v_\wp \in S) \ \text{ i.e. } \ H_u \subset S.$$

On en déduit que

$$\mathrm{rad}_K(a : b : c) \leq \sum_{\wp \in S} \log N(\wp) = \Sigma_S.$$

Comme la fonction ϕ est croissante, de l'inégalité (2.46) découle

$$\max\{h_K(u), h_K(v)\} \leq \phi\left(\Sigma_S\right).$$

□

On peut aussi démontrer directement, c'est-à-dire sans utiliser le ii) du théorème 15, que la conjecture 2 implique l'hypothèse 5. Pour cela, on pose $Au = \frac{a}{c}$ et $Bv = \frac{b}{c}$ et on montre que $H_{Au} \subset (S \cup T_{AB})$.

L'hypothèse 2 est équivalente à l'hypothèse 5.

Dans le sens réciproque c'est trivial, il suffit de prendre $A = B = 1$. On a alors $c_{AB} = c'_{AB} = 0$.

Pour le sens direct, supposons vraie la conjecture 2. Soient $A, B \in K$ non nuls, S un ensemble fini de places de K et $u, v \in O_{K,S}^*$ vérifiant l'équation (2.45). Posons $S' = S \cup T_{AB}$. Alors Au et Bv sont des S'-unités auxquelles on applique l'hypothèse 2. Comme la fonction ϕ est croissante, on obtient

$$h_K(Au : Bv : 1) \leq \phi\left(\Sigma_{S'}\right) \leq \phi\left(\Sigma_S + \Sigma_{T_{AB}}\right).$$

On conclut en remarquant que

$$h_K(u : v : 1) \leq h_K(Au : Bv : 1) + h_K(A^{-1} : B^{-1} : 1).$$

□

L'hypothèse 2 est équivalente à l'hypothèse 3.

On plonge $U = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ dans $\mathbf{A}^3$ comme au paragraphe 2.2.2, à l'aide des fonctions $x = T, y = \frac{1}{T}$ et $z = \frac{1}{1-T}$. On pose aussi $t = 1 - x$.

Soit S un ensemble fini de places de M_K^0. Les fonctions x et t prennent aux points S-entiers de U des valeurs dans $O_{K,S}$ et on a les relations

$$xy = 1, \;\; zt = 1 \;\text{ et }\; x + t = 1,$$

ce qui veut dire que x et t sont des S-unités de somme 1.

Ainsi, à un point $P \in U(O_{K,S})$ on associe, en posant $u = x(P)$ et $v = t(P)$, un couple (u, v) de S-unités vérifiant $u+v = 1$, auxquelles nous pouvons appliquer l'hypothèse 2.

Réciproquement, à un couple (u, v) de S-unités vérifiant l'équation (2.44), on fait correspondre le point S-entier P de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ tel que $x(P) = u$, auquel nous appliquons l'hypothèse 3. Par symétrie, nous pouvons supposer que $h_K(v) \leq h_K(u)$.

Comme $h_K(u) = h_K(x(P)) = h_K(P)$, on a le résultat cherché dans les deux situations. □

Remarquons que toute borne pour $h(u)$ et $h(v)$ en est une pour $h(P)$, et réciproquement.

Comme la borne de la hauteur du point P est indépendante de celui-ci, l'hypothèse 2 implique la finitude des points S-entiers de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$.

L'hypothèse 2 implique la conjecture 2.

Soient a, b et c des nombres algébriques appartenant à K, non nuls et vérifiant $a + b = c$.

Soit $S = \{\wp \in \mathcal{P}_K / \ v_\wp(a/c) < 0 \ \text{ou} \ v_\wp(a/c) > 0 \ \text{ou} \ v_\wp(b/c) > 0\}$. Alors

$$u = \frac{a}{c} \ \text{et} \ v = \frac{b}{c}$$

sont des S-unités qui vérifient l'équation (2.44). On leur applique l'hypothèse 2. Comme $h_K(a : b : c) \leq \max\{h_K(u), h_K(v)\} + [K : \mathbf{Q}] \log 2$ et

$$\Sigma_S = \sum_{\wp \in S} \log N(\wp) = \sum_{\wp \in H_{a/c}} \log N(\wp) = \mathrm{rad}_K(a : b : c),$$

on en déduit que $h_K(a : b : c) \leq \phi\left(\mathrm{rad}_K(a : b : c)\right) + [K : \mathbf{Q}] \log 2$. □

2.6 Applications.

On présente, dans cette section, des résultats obtenus à partir des théorèmes 10 et 15. On obtient un théorème allant dans le sens de la conjecture *abc* (le théorème 17), valable pour tout corps de nombres (à la différence des résultats connus jusqu'à présent). Le théorème 17 nous permet d'obtenir, en particulier, des bornes uniformes et effectives pour la hauteur des solutions de l'équation en S-unités (théorème 18), ainsi que pour les points S-entiers de $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ (théorème 20), en mettant l'accent sur la dépendance en l'ensemble de places S.

On constate, dans le premier paragraphe de la démonstration du théorème 15, section 2.5.2, que la majoration du radical du point $(a : b : c)$ ne dépend que de l'ensemble de places S. En particulier, elle ne dépend pas du couple (u, v).

Pour démontrer le théorème de Siegel sur $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, ou pour borner les solutions de l'équation en S-unités, nous n'avons pas besoin de toute la force de la conjecture *abc*. En effet, une majoration de la hauteur du point $(a : b : c)$ en fonction de son radical suffit pour majorer la hauteur de ces points. Dans ce sens, on dispose de résultats non conjecturaux, comme le théorème de C.L. Stewart et Kunrui Yu ([S-Y] théorème 1) que nous énonçons ci-après. (Cf. aussi [S-T] théorème 1.)

Théorème 16. *(Stewart-Yu)*

Il existe une constante $\eta > 0$ effective telle que, pour tout triplet (a, b, c) d'entiers naturels positifs, premiers entre eux et vérifiant $a + b = c$, on ait

$$h(a : b : c) < \eta \ \mathrm{rad}(a : b : c)^3 \exp\left(\frac{1}{3}\mathrm{rad}(a : b : c)\right).$$

Le théorème 16 correspond à la conjecture 2 où le corps de nombres est $\mathbf{Q}$ et la fonction ϕ est définie par $\phi(x) = \eta x^3 \exp(\frac{1}{3}x)$. Il se démontre à l'aide de formes linéaires de logarithmes. En particulier, les théorèmes de Stewart et Yu se basent sur une estimation archimédienne due à M. Waldschmidt [Wa1] et sur des estimations p-adiques dues à K.Yu ([Yu1], [Yu2] et [Yu3]), et sur des travaux de E. Matveev, A. Baker et G. Wüstholz.

Il nous permet de démontrer une version inconditionnelle des hypothèses $(u + v = 1)$ $(\mathbf{Q}, \phi)$ et *Siegel* $(\mathbb{P}^1 \setminus \{0, 1, \infty\}, K, \phi)$.

D'autre part, bien que la borne de l'hypothèse 1 soit plus forte que celle du théorème 14 de Yu. Bilu, nous pouvons déduire, de ce dernier, la conjecture 2, pour tout corps de nombres K et pour une fonction ϕ ayant même ordre de grandeur que celle du théorème 16 de Stewart-Yu, en appliquant le théorème 10 (section 2.4). On démontre ici le théorème suivant.

Théorème 17. *Pour tout corps de nombres K, il existe une constante réelle $\gamma > 1$ effective, dépendant du degré $[K : \mathbf{Q}]$ et du discriminant d_K de K, telle que, pour tout triplet (a, b, c) de nombres algébriques non nuls appartenant à K et tels que $a + b = c$, on ait*

$$h_K(a : b : c) \leq \exp\{\gamma \operatorname{rad}_K(a : b : c)\}.$$

Démonstration du théorème 17.

Soit K un corps de nombres. On se donne une courbe algébrique affine U définie sur K, par l'équation

$$y^m = g(x),$$

où $g \in K(X)$ est un polynôme non nul, de degré n, tel que la courbe U soit de genre $g \geq 1$ et l'extension $\overline{\mathbf{Q}}(x, y)/\overline{\mathbf{Q}}(x)$ soit galoisienne. (On pourrait prendre, par exemple, $y^2 = x^3 - x$.)

Soient a, b et c dans $K \setminus \{0\}$ tels que $a + b = c$.

Reprenons la démonstration du théorème 10. Soient C la courbe projective contenant U, f la fonction de Belyĭ associée à U, de degré d et S_0 l'ensemble de places de M_K ne dépendant que de la courbe U. Posons $q_0 = \frac{a}{c}$, $S_1 = H_{a/c}$ et $S = S_0 \cup S_1 \cup M_K^\infty$. Quitte à élargir S_0, nous pouvons supposer que $\operatorname{card}(P(S)) \geq 3$. Soit p_0 un antécédant de q_0 par la fonction f.

D'après le lemme 24, le corps de rationalité $L = K(p_0)$ du point p_0 est une extension de degré $[L : K] \leq d$ et le point p_0 est S'-entier, où S' désigne l'ensemble de places de L qui sont au-dessus de celles de S.

Au lieu de l'hypotèse *Siegel* (U, K), appliquons ici le théorème 14 à la courbe C, au corps L, à la fonction rationnelle x et au point $p_0 \in U(O_{L,S'}) \subset C(x, L, S')$. Ainsi

$$h(x(p_0)) \leq \exp\left\{N_2(\Sigma_{S'} + \log d_L) + N_1[L : \mathbf{Q}] \log P + \psi\right\},$$

où $\psi = 100\,\mathrm{card}(S')N_2\,(\log(N\,\mathrm{card}(S')) + O(1)) + [L:\mathbf{Q}]N_3\,(h(g) + O(N))$, les constantes N, N_1, N_2 et N_3 ne dépendent que de m et n, $h(g)$ désigne la hauteur du polynôme g, à savoir, la hauteur du point de l'espace projectif formé par ses coefficients, et P est le maximum des caractéristiques résiduelles de l'ensemble S'.

Remplaçons l'inégalité (2.41) par

$$h(x(p_0)) \geq \frac{n}{d\,[K:\mathbf{Q}]} h_K(a:b:c) - \frac{n}{d}\log 2.$$

Comme $[L:K] \leq d$, l'inégalité (2.42) devient $\Sigma_{S'} \leq d\,\Sigma_S$, et l'inégalité (2.43),

$$\log d_L \leq d\left(\log d_K + \Sigma_S + 2\,[K:\mathbf{Q}]\log d\frac{\Sigma_S}{\log \Sigma_S}\right).$$

Par ailleurs, l'inégalité (2.25) nous majore le maximum P des caractéristiques résiduelles de S' (ou de S) :

$$\log P \leq \Sigma_S,$$

et l'inégalité (2.26) ainsi que le lemme 17, appliqués à l'ensemble S', nous permettent de majorer le cardinal de S' :

$$\mathrm{card}(S') \leq [L:\mathbf{Q}]\,\mathrm{card}(P(S')) \leq 2\,[L:\mathbf{Q}]\frac{\Sigma_{S'}}{\log \Sigma_{S'}}.$$

En appliquant l'inégalité (2.28) on obtient

$$\mathrm{card}(S') \leq 2\,d^2\,[K:\mathbf{Q}]\frac{\Sigma_S}{\log([L:K]\Sigma_S)},$$

ce qui nous permet de majorer ψ.

En remarquant que $\Sigma_S \leq \mathrm{rad}_K(a:b:c) + \Sigma_{S_0}$ et que S_0 ne dépend que de la courbe U choisie au début, nous obtenons l'inégalité

$$h_K(a:b:c) \leq \exp\{\gamma\,\mathrm{rad}_K(a:b:c)\},$$

où le nombre réel γ dépend de $m, n, h(g)$, du degré $[K:\mathbf{Q}]$ et du discriminant d_K du corps de base K, mais pas de a, b et c. Ceci achève la démonstration. □

Remarque 6. *Il est vraissemblable qu'on puisse étendre également le résultat de Stewart et Yu (théorème 16) à tout corps de nombres, en utilisant les formes linéaires de logarithmes, archimédiennes et p-adiques, connues à l'heure actuelle. Il serait alors intéressant de comparer la qualité du résultat obtenu avec celle du théorème 17.*

Des théorèmes 16 (Stewart-Yu) et 17 (que nous venons de démontrer) on déduit les théorèmes 18 et 20.

Théorème 18. *Soient K un corps de nombres, A et B des éléments non nuls de K et S un ensemble fini de places de M_K^0. Si u et v appartiennent au groupe des S-unités $O_{K,S}^*$ et vérifient l'équation (2.45), $Au + Bv = 1$, alors*

$$\max\{h_K(u), h_K(v)\} \leq \exp\{\gamma\,(\Sigma_S + c_{AB})\} + c'_{AB},$$

où γ est un nombre réel ne dépendant que de $[K : \mathbf{Q}]$ et d_K, et c_{AB} et c'_{AB} ne dépendent que de A et B.

Si le corps de nombres est $\mathbf{Q}$, on a

$$\max\{h_K(u), h_K(v)\} \leq \eta\,(\Sigma_S + c_{AB})^3 \exp\left(\frac{1}{3}(\Sigma_S + c_{AB})\right) + c'_{AB},$$

où η est une constante effective et c_{AB} et c'_{AB} ne dépendent que de A et B.

Démonstration du théorème 18.

On applique le théorème 15 dans le cas général à la fonction $\phi(x) = \exp(\gamma x)$, qui nous est donnée par le théorème 17, et, dans le cas où $K = \mathbf{Q}$, à la fonction $\phi(x) = \eta x^3 \exp(\frac{1}{3}x)$ du théorème 16. □

Comme cela a été mentionné au début de la section 2.5, Y. Bugeaud et K. Györy ont obtenu des résultats effectifs et uniformes en S pour les bornes de la hauteur des solutions de l'équation en S-unités, $Au + Bv = 1$. En ce qui concerne la dépendance en S, les bornes du théorème 18 sont meilleures que celle du théorème 1 de [BG], ci-dessous.

Théorème 19. *(Bugeaud-Györy)*

Soient K un corps de nombres, H un nombre réel $\geq e$, A et B des éléments non nuls de K tels que $\max\{h(A), h(B)\} \leq H$ et S un ensemble fini de places de M_K^0.

Les solutions u, v de l'équation (2.45) appartenant à $O_{K,S}^*$ vérifient

$$\max\{h(u), h(v)\} \leq \exp\left(\gamma P^{[K:\mathbf{Q}]} R_S\,(\log^+ R_S)(\log^+(PR_S)/\log^+ P)\log H\right),$$

où γ est un nombre réel dépendant de K et de $\mathrm{card}(S)$, P est le maximum des caractéristiques résiduelles de S, R_S est le S-régulateur et $\log^+(.)$ est une notation pour $\max\{\log ., 1\}$.

Précisément, $\gamma = c_K^{\mathrm{card}(S)+a+1}\,(\mathrm{card}(S) + a)^{5\,(\mathrm{card}(S)+a+2)}$, où $c_K \geq 1$ ne dépend que de K, et a est le nombre de places archimédiennes de K. On a $\gamma \geq \mathrm{card}(S)^{\mathrm{card}(S)}$.

Pour comparer la borne du théorème 19 à celle obtenue dans le théorème 18, rappelons que, pour un ensemble fini de places S, on a noté

$$\Pi_S = \prod_{p \in S} \log N(\wp).$$

Si $\mathrm{card}(S) = 0$, la borne du théorème 18 est un nombre réel dépendant du corps de nombres K, que nous n'avons pas explicité, à différence de Bugeaud et Györy.

Si $\mathrm{card}(S) \geq 1$, on a

$$R_S \geq R_K \Pi_S \geq R_K \Sigma_S.$$

(La première inégalité est le lemme 3 de [BG]. La deuxième est triviale.) D'après l'inégalité (2.25) et le lemme 17, $\log(P^{[K:\mathbf{Q}]}) \geq \frac{1}{\mathrm{card}(P(S))}\Sigma_S \geq \frac{1}{2}\log \Sigma_S$,

$$\text{i.e. } P^{[K:\mathbf{Q}]} \geq \sqrt{\Sigma_S}.$$

Si $P \geq e$ (ce qui est toujours le cas sauf si $P(S) = \{2\}$), alors

$$(\log^+(PR_S)/\log^+ P) \geq 1$$

et donc la borne du théorème 19 est supérieure à

$$\exp\left(\mathrm{card}(S)^{\mathrm{card}(S)}\sqrt{\Sigma_S}\, R_K\, \Pi_S\, (\log R_K \Pi_S)\right)$$

ce qui est supérieur à la borne du théorème 18.

Remarque 7. *Avec le théorème de Bugeaud et Györy nous pouvons aussi obtenir un résultat dans le sens de la conjecture 2, nettement moins fort que le théorème 17 démontré dans cette section. Pour cela, on majore les termes de la borne du théorème 19 faisant intervenir l'ensemble S, à savoir P, R_S et* $\mathrm{card}(S)$*, en fonction de K et de Σ_S, et on applique le théorème 15 à la fonction ϕ de Σ_S ainsi obtenue.*

En effet, d'après l'inégalité (2.26) et le lemme 17, $\mathrm{card}(S) \leq 2[K : \mathbf{Q}]\frac{\Sigma_S}{\log \Sigma_S}$. De plus, d'après l'inégalité (2.25), $P^{[K:\mathbf{Q}]} \leq \exp([K : \mathbf{Q}]\Sigma_S)$. La remarque 1 de [BG] nous donne :

$$\frac{\log^+(PR_S)}{\log^+ P} \leq 2\log^+(R_S)$$

et si $S \neq \emptyset$, alors

$$R_S \leq R_K \mathfrak{h}_K \Pi_S \leq R_K \mathfrak{h}_K \left(\frac{1}{\mathrm{card}(S)}\Sigma_S\right)^{\mathrm{card}(S)},$$

où $\mathfrak{h}_K$ désigne le nombre de classes de $\mathrm{Pic}(O_K)$. La première inégalité est le lemme 3 de [BG] et la deuxième est obtenue en appliquant l'inégalité arithmético-géométrique.

Avec ces majorations, on arrive à majorer la borne du théorème 19 par $\phi(\Sigma_S)$ où la fonction ϕ (dépendant de K et de A et B) a même ordre de grandeur que $\exp\{\exp(x)\}$.

Théorème 20. *Pour tout corps de nombres K, tout ensemble fini S de places de M_K^0 et tout point S-entier P de $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, on a la majoration suivante :*

$$h_K(P) < \exp(\gamma\, \Sigma_S),$$

où γ est un nombre réel ne dépendant que du corps K.

Si le corps de nombres est $\mathbf{Q}$, on a

$$h_K(P) < \eta\, (\Sigma_S)^3 \exp\left(\frac{1}{3}\Sigma_S\right),$$

où η est la constante absolue effective du théorème 16.

(Si l'ensemble S est vide, on obtient ici une borne dépendant du corps K que l'on n'a pas cherché à expliciter.)

Démonstration du théorème 20.

Il suffit d'appliquer le théorème 15, dans le cas général à la fonction $\phi(x) = \exp(\gamma\, x)$, qui nous est donnée par le théorème 17 et, dans le cas où $K = \mathbf{Q}$, à la fonction $\phi(x) = c\, x^3 \exp(\frac{1}{3}x)$ du théorème 16. □

On peut considèrer que la première version effective du théorème de Siegel pour $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ est dûe à Baker ([Ba1] et [Ba3]) puisqu'il donne des bornes effectives pour la hauteur des solutions de l'équation aux unités ; cependant, le premier a l'avoir présenté sous cette forme est J.P. Serre dans son livre [Se1]. (Pour des majorations complètement explicites et récentes, dans le cas où $S = \emptyset$, on peut consulter [P3].)

Le théorème 20 a l'avantage de mettre en valeur la dépendance en l'ensemble de places S. Par ailleurs, il peut être appliqué, comme le résultat de A. Baker et suivant [Se1], pour montrer la finitude des points S-entiers d'autres courbes, et ce de façon effective. Depuis les travaux de Siegel, il est connu que la recherche de points (S-)entiers sur certaines équations diophantiennes, comme les équations dites de Thue, les superelliptiques et les hyperelliptiques, peut se ramener à la recherche de points (S-)entiers sur les équations aux unités (cf, par exemple, [La2]). Nous pouvons donc imaginer que les théorèmes 18 et 20 pourraient donner de nouvelles bornes pour ces équations-là et que la dépendance en l'ensemble S pourrait être améliorée.

Appendice : Le théorème de Siegel uniforme sur les corps de fonctions.

Comme nous l'avons mentionné dans la section 2.4, notre hypothèse de type "Siegel uniforme", hypothèse 1, peut être vue comme l'analogue, dans la théorie des corps de nombres, de plusieurs résultats concernant les corps de fonctions.

Commençons par rappeler très brièvement l'analogie entre les corps de nombres et les corps de fonctions. Si k est un corps algébriquement clos, on a une équivalence de catégories entre, la catégorie des courbes algébriques intègres, propres et lisses définies sur k et la catégorie opposée des extensions séparables de type fini et de degré de transcendance 1 de k, appelées "corps de fonctions d'une variable sur k". Cette équivalence est donnée par le foncteur (contravariant) qui à une courbe B/k associe son corps de fonctions $k(B)$. De ce point de vue, à un morphisme de courbes $B' \to B$ correspond le morphisme d'extensions de k, $k(B) \hookrightarrow k(B')$. Si x est un point (fermé) de la courbe B, l'anneau local $O_{B,x}$ est un anneau de valuation discrète. Le corps $K = k(B)$ est son corps de fractions. Ainsi, les places de K correspondent aux points fermés de B.

Soit C une courbe algébrique projective définie sur un corps K de caractéristique 0, qui peut être, soit un corps de nombres, soit le corps des fonctions rationnelles $k(B)$ d'une courbe B. Classiquement, on considère que l'analogue du logarithme de la valeur absolue d_K du discriminant, dans le cas où K est un corps de nombres, est le nombre $2\,g_K - 2$, où $g_K = g(B)$ est le genre du corps K (ou de la courbe B), et que, étant donné un ensemble fini S de places de M_K, $\Sigma_S = \sum_{\wp \in S} \log N(\wp)$ est, dans le cas où K est un corps de nombres, ce qui est $\mathrm{card}(S) = \sum_{x \in S} 1$ dans le cas du corps de fonctions.

En juxtaposant divers énoncés connus, nous obtenons le théorème suivant, analogue dans la théorie des corps de fonctions de notre hypothèse *Siegel* (U, K) de la section 2.4.

Théorème 21. *Soient $K = k(B)$ un corps de fonctions, C une courbe définie sur K et h une fonction hauteur définie sur C associée à un diviseur*

de C de degré 1. Soit U un ouvert affine de C tel que $\chi(U) < 0$. Alors pour toute extension finie $L = k(B')$ de K et tout ensemble fini S de places de L, on a, pour tout point S-entier $P \in U(O_{L,S})$,

$$h_L(P) \leq c_1\,(2\,g_L - 2) + c_2\,\mathrm{card}(S) + c_3,$$

où $h_L = [L : K]h$ et $g_L = g(B')$ désigne le genre de l'extension L et les nombres c_1 et c_2 ne dépendent que de la courbe U et c_3 dépendent de U, du choix de la hauteur h et du degré $[L : K]$.

Nous verrons ci-après, que quand le genre g de la courbe U est supérieur ou égal à 2, quand $g = 1$ et U a un point à l'infini ou quand $U = \mathbf{P}^1\backslash\{0, 1, \infty\}$, les nombres c_1 et c_2 ne dépendent que de la caractéristique d'Euler-Poincaré $\chi(U)$ et $c_3 = c_3'\,[L : K]$, où c_3' ne dépend que de la courbe et $[L : K]$ est le degré de l'extension de corps considérée.

Dans le cas où la courbe C est de genre $g = g(C) \geq 2$, des résultats plus forts ont été prouvés. En effet, le théorème est démontré pour les points rationnels (cf. les références qui suivent), c'est l'équivalent de "Mordell effectif". Nous pouvons donc oublier dans ce cas le terme faisant intervenir le cardinal de S. Comme $g \geq 2$, le diviseur canonique ω est effectif, de degré $2g - 2$. Pour toute extension finie L de K, soit $h_{L,C}$ la hauteur associée au diviseur $\frac{1}{2g-2}\omega$ de degré 1 et relative à L,

$$\text{i.e. } h_{L,C} = [L : K]\frac{h_\omega}{2g(C) - 2}.$$

Avec ce choix de hauteur, le théorème de P. Vojta [Vo] s'énonce

Théorème 22. *(Vojta)*
Soit C une courbe de genre $g = g(C) \geq 2$ définie sur un corps de fonctions K de caractéristique nulle. Pour tout point $P \in C(L)$ où L est une extension finie de K et pour tout $\varepsilon > 0$,

$$h_{L,C}(P) \leq \frac{2 + \varepsilon}{2g(C) - 2}(2g_L - 2) + c_3'\,[L : K],$$

où la constante c_3' ne dépend que de C et ε.

La démonstration se base sur celle donnée par Grauert pour démontrer l'analogue pour les corps de fonctions de la conjecture de Mordell. Bien qu'il ne soit pas clair si le nombre c_3' peut être calculé de manière explicite, ce résultat est celui qui donne la meilleure constante c_1, à savoir $\frac{2+\varepsilon}{2g(C)-2} = \frac{2+\varepsilon}{-\chi(U)}$. D'autres bornes complètement explicites ont été obtenues, par L. Szpiro [Sz] :

$$c_1 = \frac{8 \times 3^{2g+1}(g-1)^2}{2g-2} \text{ et } c_3' = c_1\,3^g(s + 1 + 3^{-3g})$$

et par H. Esnault et E. Viehweg [EV] :

$$c_1 = \frac{(2g-1)^2}{g-1} \text{ et } c_3' = c_1\, s,$$

où s désigne le nombre de fibres dégénérées du modèle minimal de C/K.

Dans le cas où la courbe U est de genre zéro et qu'elle a au moins trois points à l'infini, on peut se ramener au cas de la droite projective privée de 0, 1 et l'infini. Dans ce cas, le théorème 21 est essentiellement le théorème de Mason (lemme 2 de [Ma2]), analogue de la conjecture *abc*.

Théorème 23. *(abc-Mason)*
Soient $K = k(B)$ un corps de fonctions de gegre g_K et S un ensemble fini de places de K. Soient A, B, C des éléments non nuls de K tels que $A+B+C=0$ et $v(A) = v(B) = v(C)$ pour toute valuation v n'appartenant pas à S. Si $A/B \notin k$, alors

$$h\left(\frac{A}{B}\right) \leq 2g_K - 2 + \mathrm{card}(S).$$

Soient L/K une extension de corps de fonctions et S un ensemble fini de places de L. Soit P un point S-entier de $U = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Au point P nous lui associons le couple (u, v) de S-unités vérifiant $x(P) = u$. La fonction x étant de degré 1, nous prenons comme hauteur définie sur notre courbe $h_{L,U} = h_L \circ x$. On applique le théorème *abc* de Mason :

$$h_{L,U}(P) = h_L(u) \leq 2g_L - 2 + \mathrm{card}(S).$$

On constate qu'on peut choisir $c_1 = c_2 = 1\frac{1}{-\chi(U)}$ et $c_3 = 0$.

Dans le cas où le genre $g = g(C) = 1$, il suffit de traiter le cas avec un point "à l'infini". La courbe C est alors elliptique et nous pouvons nous ramener à une équation de la forme

$$y^2 = f(x),$$

où $f \in K[X]$ est un polynôme du troisième degré. Dans ce cas, plusieurs résultats sont connus (cf., par exemple, [Sc], [Ma1] et [HS1]).

Considérons le cas plus général des courbes dites superelliptiques. Soit U la courbe affine d'équation

$$y^m = f(x),$$

où f est un polynôme de $K[X]$ de degré n. Comme le morphisme $(x, y) \mapsto y$ est de degré n, prenons comme hauteur

$$h_{L,U} = \frac{h_L \circ y}{n}.$$

Si $m = 2$ la courbe est appelée hyperelliptique. Hindry et Silverman montrent (proposition 8.2 de [HS1]) le résultat suivant.

Proposition 5. *(Hindry-Silverman)*

Soient K un corps de fonctions de genre g_K et S un ensemble fini de places de K. Soit $f(X) = X^n + a_1 X^{n-1} + \ldots + a_n$ un polynôme de $O_{K,S}[X]$ dont le discriminant $\Delta \in O_{K,S}^*$. Si $x, y \in O_{K,S}$ vérifient l'équation

$$y^2 = f(x),$$

$$h_K(y) \leq 2n(2g - 2 + \mathrm{card}(S)) + \frac{h_K(\Delta)}{2(n-1)}.$$

La conclusion de la proposition 5 reste vraie pour m quelconque.

Proposition 6. *Soient K un corps de fonctions de genre g_K et S un ensemble fini de places de K. Soit $f(X) = X^n + a_1 X^{n-1} + \ldots + a_n$ un polynôme de $O_{K,S}[X]$ dont le discriminant Δ est une S-unité. Si $x, y \in O_{K,S}$ vérifient l'équation*

$$y^m = f(x), \tag{2.47}$$

alors

$$h_K(y) \leq 2\,n\,(2g_K - 2 + \mathrm{card}(S)) + \frac{1}{m(n-1)} h_K(\Delta).$$

Démonstration de la proposition 6.

Nous suivons la démonstration de la proposition 8.2 de [HS1].

Soient $x, y \in O_{K,S}$ vérifiant l'équation (2.48). Soient $e_1, \ldots, e_n$ les n racines de f dans une clôture $\overline{K}$ du corps K. Soit $\Delta = \prod_{i \neq j}(e_i - e_j)$ le discriminant du polynôme f. Supposons que Δ est une S-unité.

Pour $i \in \{1, \ldots, n\}$, choisissons des racines m-ièmes $u_i = (x - e_i)^{\frac{1}{m}}$ telles que $y = u_1 \ldots u_n$.

Soient $K' = K(u_1, \ldots, u_n)$ et $g_{K'}$ son genre. Soit S' l'ensemble des places de K' qui sont au-dessus de celles de S et $O_{K',S'}$ son groupe des S'-unités.

Notons μ_m le groupe des racines m-ièmes de l'unité qui sont dans K.

Alors, pour tout couple $(i, j) \in \{1, \ldots, n\}^2$, on a

$$\prod_{\zeta \in \mu_m} (u_i - \zeta u_j) = u_i^m - u_j^m = -e_i + e_j \in O_{K,S}^*,$$

et comme chaque terme $(u_i - \zeta u_j)$ est S-entier, alors $(u_i - \zeta u_j)$ est en fait une S-unité.

Soient $\zeta, \zeta', \zeta'' \in \mu_m$ tels que $\zeta'' \zeta = \zeta'$. Alors, pour tous $i, j, k \in \{0, \ldots, n\}$,

$$\zeta''(u_i - \zeta u_j) + (u_k - \zeta'' u_i) - (u_k - \zeta' u_j) = 0,$$

$$\text{et } \zeta''(u_i + \zeta u_j) - (u_k + \zeta'' u_i) + (u_k - \zeta' u_j) = 0.$$

En appliquant le théorème *abc* de Mason, théorème 23, aux deux équations, on obtient l'inégalité

$$\max\left\{ h_{K'}\left(\frac{u_i + \zeta u_j}{u_k - \zeta' u_j}\right), h_{K'}\left(\frac{u_i - \zeta u_j}{u_k - \zeta' u_j}\right)\right\} \leq 2g_{K'} - 2 + \mathrm{card}(S').$$

Posons $N_{K'} = 2g_{K'} - 2 + \mathrm{card}(S')$.

Par ailleurs, $\frac{2u_i}{u_k - \zeta' u_j} = \frac{u_i - \zeta u_j}{u_k - \zeta' u_j} + \frac{u_i + \zeta u_j}{u_k - \zeta' u_j}$, donc

$$h_{K'}\left(\frac{u_i}{u_k - \zeta' u_j}\right) \leq 2\, N_{K'}.$$

Comme $\Delta = \prod_{j \neq k}(e_j - e_k) = \prod_{j \neq k} \prod_{\zeta \in \mu_m}(u_k - \zeta u_j)$, alors

$$\prod_{j \neq k} \prod_{\zeta \in \mu_m} \frac{u_i}{u_k - \zeta u_j} = \frac{u_i^{mn(n-1)}}{\Delta} \quad \text{et} \quad \prod_{i=1}^{n} \prod_{j \neq k} \prod_{\zeta \in \mu_m} \frac{u_i}{u_k - \zeta u_j} = \frac{y^{mn(n-1)}}{\Delta^n}.$$

En utilisant les inégalités (2.31), nous en déduisons :

$$h_{K'}\left(\frac{y^{mn(n-1)}}{\Delta^n}\right) \leq 2mn^2(n-1)\, N_{K'}.$$

et encore

$$\begin{aligned} h_{K'}(y) &\leq \frac{1}{mn(n-1)} \left(h_{K'}\left(\frac{y^{mn(n-1)}}{\Delta^n}\right) + h_{K'}(\Delta^n) \right) \\ &\leq 2\, n\, N_{K'} + \frac{1}{m(n-1)} h_{K'}(\Delta). \end{aligned}$$

Pour conclure, nous appliquons la formule de Riemann-Hurwitz à l'extension K'/K qui n'est ramifiée qu'au-dessus de l'ensemble de places S :

$$N_{K'} = 2g_{K'} - 2 + \mathrm{card}(S') = [K' : K](2g_K - 2 + \mathrm{card}(S)),$$

et nous obtenons

$$h_K(y) \leq 2\, n\, (2g_K - 2 + \mathrm{card}(S)) + \frac{1}{m(n-1)} h_K(\Delta).$$

□

Avec la proposition 6, nous montrons le théorème suivant.

Théorème 24. *Soient K un corps de fonctions de genre g_K, $f(X) = X^n + a_1 X^{n-1} + \ldots + a_n$ un polynôme de $K[X]$ et U la courbe d'équation*

$$y^m = f(x). \tag{2.48}$$

Pour toute extension L/K finie, et pour tout ensemble fini S de places de L, si $P \in U(O_{L,S})$, alors

$$h_{L,U}(P) \leq 2\, (2g_L - 2 + \mathrm{card}(S)) + c_3'\, [L : K],$$

où $h_{L,U} = \frac{h_L \circ y}{n}$ et le nombre $c_3' = 2\,\mathrm{card}(S_0) + \frac{h_K(\Delta)}{mn(n-1)}$ ne dépend que de la courbe U.

Si $m = 2$ et $n = 3$ la courbe U est elliptique. Dans ce cas, $\chi(U) = -1$ et on remarque que $c_1 = c_2 = 2 = \frac{2}{-\chi(U)}$. Pour m et n quelconques, $-\chi(U) = mn - m - n$.

Démonstration du théorème 24.

Soient $L = k(B')$ une extension de $K = k(B)$ de degré $[L : K]$ fini et S un ensemble fini de places de L. Soit $P = (x, y)$ un point S-entier de la courbe U.

Soit $S_0 \subset M_K$ le plus petit ensemble de places de K tel que le polynôme f soit à coefficients dans O_{K,S_0} et tel que le discriminant Δ soit une S_0-unité. L'ensemble S_0 est fini et ne dépend que de la courbe U. À l'extension de corps L/K correspond un morphisme de courbes $\varphi : B' \to B$. Posons $S_1 = S \cup \varphi^{-1}(S_0)$. Alors $f \in O_{L,S_1}[X]$ et $\Delta \in O^*_{L,S_1}$, ce qui nous permet d'appliquer la proposition 6 au corps L, à l'ensemble S_1 et au point P :

$$h_L(y) \leq 2n(2g_L - 2 + \operatorname{card}(S_1)) + \frac{1}{m(n-1)} h_L(\Delta). \tag{2.49}$$

Comme $\operatorname{card}(S_1) \leq \operatorname{card}(S) + [L : K] \operatorname{card}(S_0)$ et $h_L(\Delta) = [L : K]\, h_K(\Delta)$, et $h_{L,U}(P) = \frac{1}{n} h_L(y)$, on obtient

$$h_{L,U}(P) \leq 2(2g_L - 2 + \operatorname{card}(S)) + \left(2 \operatorname{card}(S_0) + \frac{h_K(\Delta)}{mn(n-1)}\right) [L : K].$$

□

Remarque. Soient h et h' deux hauteurs définies sur la courbe C associées a un diviseur de degré un. Supposons que pour tout point S-entier P on ait la borne

$$h(P) \leq c_1(2g_L - 2) + c_2 \operatorname{card}(S) + c_3.$$

Rappelons qu'en utilisant l'inégalité (2.32) nous pouvons nous ramener à

$$h'(P) \leq h(P) + c\sqrt{h(P)}.$$

Ceci implique la borne suivante :

$$h'(P) \leq (c_1 + \varepsilon)(2g_L - 2) + (c_2 + \varepsilon)\operatorname{card}(S) + c'_3.$$

Nos calculs montrent qu'on peut prendre, dans tous les cas, des constantes $c_1 = c_2 = 2 + \varepsilon$. Dans les exemples traités nous obtenons $\frac{2}{-\chi(U)}$, sauf dans le cas des courbes superelliptiques.

Ces bornes, ainsi que celle du théorème 22 de Vojta, sont l'analogue de la borne du théorème 13 (valable sur un corps de nombres et en admettant la conjecture *abc*). Il serait intéressant de savoir quelle est la meilleure constante possible.

Bibliographie

[Ba1] Baker, A. *Linear forms in the logarithms of algebraic numbers I*, Mathematika, 13 (1966), 204-216.

[Ba2] Baker, A. *Contributions to the theory of Diophantine equations, I : On the representation of integers by binary forms*, Philos. Trans. Roy. London Ser. A 263 (1968), 173-191.

[Ba3] Baker, A. *Transcendental Number Theory*, Cambridge Universy Press, Cambridge, 1975.

[BC] Baker, A. and Coates, J., *Integer points on curves of genus 1*, Proc. Cambridge Philos. Soc. 67 (1970), 595-602.

[BM] Baker, A. and Masser, D.W., *Transcendence theory : Advances and Applications Proceedings of a conference held in Cambridge in 1976*, Academic Press, London (1977).

[Be] Belyĭ, G.V., *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izveztija, Vol. 14, n°2 (1980).

[Bi] Bilu, Yuri F., *Quantitative Siegel's theorem for Galois coverings*, Compositio Math. 106 (1997), no. 2, 125-158.

[Bo1] Bombieri, E., *Effective diophantine approximation on* $\mathbf{G}_m$, Ann. Scuola Norm. Sup. Pisa (IV) 20 (1993), 61-89.

[Bo2] Bombieri, E., *Roth's Theorem and the abc-conjecture*, preprint ETH Zürich (1994).

[Bo-Co] Bombieri, E., Cohen, P.B., *Effective diophantine approximation on* $\mathbf{G}_m$ *II*, Ann. Scuola Norm. Sup. Pisa Cl. Sc. s. 4, 24 (1997), 205-225.

[Bu1] Bugeaud, Y., *Bornes effectives pour les solutions des équations en S-unités et des équations de Thue-Mahler*, J. Number Theory 71 (1998), 227-244.

[Bu2] Bugeaud, Y. *Fundamental systems of S-units with small height and their applications to Diophantine equations*, Publ. Math. Debrecen 56/3-4 (2000), 279-292.

[BG] Bugeaud, Y., Györy, K., *Bounds for the solutions of unit equations*, Acta Arith. 74 (1996), 273-292.

[DZ] Dvornicich, R., Zannier, U., *Fields Containing Values of Algebraic Functions*, Ann. Sc. Norm. Super. Pisa, Cl. Sci., IV. Ser. 21, No.3, 421-443 (1994).

[El] Elkies, N.D., *ABC implies Mordell*, Intern. Math. Research Notices 7 (1991), 99-109.

[EV] Esnault, H., Viehweg, E., *Effective bounds for semipositive sheaves and for the height of points of curves over complex function fields*, Compos. Math. 76, No.1/2 (1990), 69-85.

[Fa] Faltings, G., *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen*, Invent. Math. 73 (1983), 349-366.

[GS] Granville, A., Stucker, T.J., *It's as easy as abc*, Notices of the AMS, volume 49, number 10, (2002), 1224-1231.

[SGA] Grothendieck, A., *Revêtements étales et groupe fondamental*, Séminaire de géométrie algébrique du Bois Marie 1960/61 (SGA 1), Lecture Notes in Mathematics, 224, Springer-Verlag, Berlin-Heidelberg-New York, (1971).

[HS1] Hindry, M., Silverman, J.H., *The canonical height and integral points on elliptic curves*, Invent. Math. 93, No.2 (1988), 419-450.

[HS2] Hindry, M., Silverman, J.H., *Diophantine Geometry. An introduction*, Graduate texts in mathematics, Springer-Verlag, New York, 2000.

[La1] Lang, S., *Integral points on curves*, Publ. Math., Inst. Hautes Études Sci. 6, (1960) 319-335.

[La2] Lang, S., *Elliptic curves : Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften. 231. Berlin-Heidelberg-New York : Springer-Verlag (1978).

[La3] Lang, S., *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[La4] Lang, S., *Number theory III : Diophantine geometry*, Encyclopaedia of Mathematical Sciences, vol. 60. Springer-Verlag, Berlin (1991).

[MvF] Frankenhuysen, M. van, *The ABC conjecture implies Roth's theorem and Mordell's conjecture*, Matemática Contemporânea, Vol. 16 (1999), 45-72.

[Mah1] Mahler, K., *Zur Approximation algebraischer Zahlen*, Math. Ann. 107 (1933), 691-730.

[Mah2] Mahler, K., *Über die rationalen Punkte auf Kurven vom Geschlecht Eins.*, J. reine angew. Math. 170 (1934), 168-178.

[Ma1] Mason, R.C., *The hyperelliptic equation over function fields*, Math. Proc. Cambridge Philos. Soc. 93, no. 2 (1983), 219-230.

[Ma2] Mason, R.C., *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Note Series 96, Cambridge University Press, Cambridge, 1984.

[Mas] Masser, D.W., *On abc and discriminants*, Proceedings of the American Mathematical Society, Volume 130, Number 11, (2002), 3141-3150.

[Mat] Matiyasevich, Yu., *Hilbert's Tenth Problem : What was done and what is to be done*, Proceedings of the workshop, Ghent University, Belgium, November 2-5, 1999. Providence, RI : American Mathematical Society (AMS). Contemp. Math. 270, 1-47 (2000).

[M-B] Moret-Bailly, L., *Hauteurs et classes de Chern sur les surfaces arithmétiques*, Astérisque 183, (1990), 37-58.

[Oe] Oesterlé, J., *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki, 40ème annéee, n°694, février 1998.

[P1] Poulakis, D., *Points entiers sur les courbes hyperelliptiques*, Acta Arith. 62, No.1, 25-43 (1992).

[P2] Poulakis, D., *Points entiers et modèles de courbes algébriques*, Monatsh. Math. 118, No.1-2, 111-143 (1994).

[P3] Poulakis, D., *Bounds for the size of integral points on curves of genus zero*, Acta Math. Hung. 93, n°4, 327-346 (2001).

[Sc] Schmidt, W.M., *Thue's equation over function fields*, J. Austral. Math. Soc. Ser. A 25 (1978), no. 4, 385-422.

[Se1] Serre, J.-P., *Lectures on Mordell-Weil theorem*, Vieweg (1990).

[Se2] Serre, J.-P., *Quelques appliquations du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. n°54, (1981), 323-401.

[Si1] Siegel, C.L., *Approximation algebraischer Zahlen*, Math. Z. 10 (1921), 173-213.

[Si2] Siegel, C.L., *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc. 1 (1926), 66-68.

[Si3] Siegel, C.L., *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss. 1 (1929) 41-69 (Ges. Abh., I, 209-266).

[S-T] Stewart, C.L., Tijdeman R., *On the Oesterlé-Masser Conjecture*, Monatsh. Math., 102, (1986), 251-257.

[S-Y] Stewart, C.L., Yu, Kunrui, *On the abc conjecture, II*, Duke Math. J. 108 (2001), n°1, 169-181.

[Sz] Szpiro, L., *Propriétés numériques du faisceau dualisant rélatif*, Seminaire sur les pinceaux de courbes de genre au moins deux, Astérisque 86 (1981), 44-78.

[Th] Thue, A., *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math., 135 (1909), 284-305.

[Vo] Vojta, P., *On algebraic points on curves*, Compos. math. 78 (1991), no. 1, 29-36.

[Wa1] Waldschmidt, M., *A lower bound for linear forms in logarithms*, Acta Arith. 37 (1980), 257-283.

[Wa2] Waldschmidt, M., *Minoration de combinaison linéaire de logarithmes de nombres algébriques*, Canadian J. Math. 45 (1993), 176-224.

[Wa3] Waldschmidt, M., *Open Diophantine Problems*, Prépublications de l'Institut de Mathématiques de Jussieu, 282, Mars 2001.

[Yu1] Yu, Kunrui, *Linear forms in p-adic logarithms, III*, Compositio Math. 91 (1994), 241-276.

[Yu2] Yu, Kunrui, *p-adic logarithmic forms and group varieties, I*, J. Reine Angew. Math. 502, (1998), 29-92.

[Yu3] Yu, Kunrui, *p-adic logarithmic forms and group varieties, II*, Acta Arith. 89 (1999), 337-378.