$N°$ d'ordre : 3196

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Mourad ABOUZAID**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : **Mathématiques Pures**

****

Aspects effectifs d'analyse diophantienne

****

Soutenue le 3 Juillet 2006 à l'Institut de Mathématiques de Bordeaux

Après avis de :

F. AMOROSO	Professeur, Université de Caen	**Rapporteur**
M. HINDRY	Professeur, Université Paris 7	**Rapporteur**

Devant la commission d'examen composée de :

Yu. BILU	Professeur, Université Bordeaux 1	**co-Directeur**
H. COHEN	Professeur, Université Bordeaux 1	**Directeur**
P. DÉBES	Professeur, Université de Lilles 1	**Président du jury**
G. HANROT	Chargé de Recherches, INRIA Lorraine	
M. HINDRY	Professeur, Université Paris 7	**Rapporteur**

- 2006 -

Remerciements

Elle peut être longue la liste des gens qui m'ont aidé à arriver jusque là. tout d'abord ma famille, bien sûr. Mes parents et ma soeur, sans qui rien de tout cela n'aurait été possible. Un grand merci à vous donc. C'est de vous que me vient mon envie d'étudier, d'apprendre. Et c'est grace à vous que j'ai pu tenir jusqu'au bout.

Je passe rapidement sur mes instituteurs de l'école des Charmes, sur mes professeurs du collège Villeneuve et du lycée Mounier, ainsi que sur ceux du lycée Vaugelas même si c'est dans ce dernier qu'est véritablement né mon plaisir pour les mathématiques.

Merci aussi à Valéry, Anne, Anne, Guillemette, Marion, Sylvie, Olivier. Cette année de licence était formidable. Et même si vous êtes maintenant un peu loin (certain plus que d'autres...), eh bien quelque part, vous êtes toujours là.

Un grand merci également à l'Institut de Mathématiques de Bordeaux qui m'a accueilli pendent trois ans, que dis-je, quatre ans au sein de son équipe.

Merci aussi a Florent. Tu m'as supporté au bureau ET à la maison. Merci à Eric. Tu étais toujours là, même pour m'écouter raler. Merci à Fred, Lotte, et tous les habitués du Café. Votre musique et votre présence m'ont été d'un grand secours. Merci à Anne. Tu m'a écouté douter, et tu as su me remonter. Merci aussi Carine. Merci pour ton bureau, tes confidences, tes éclats de rire. Merci à Karene, à Matthieu, toujours présents. Merci enfin à M. Henri COHEN, qui a su me donner ma chance.

Je garde ces dernières lignes pour remercier tout particulièrement M. Yuri BILU, qui m'a guidé jusqu'au bout, tout au long de ces trois ans. Ta passion pour les mathématiques, ta clairvoyance et tes compétences m'ont permis de découvrir ce vaste monde qu'est la recherche. Ce fut un véritable plaisir et un honneur (je pèse mes mots...) de travailler à tes côtés. Merci aussi pour ta disponibilité, ton humour, et allez, je me lance... ton humanité.

Table des matières

Introduction

Cette thèse traite de trois problèmes diophantiens distincts. Le premier chapitre est consacré à l'étude des diviseurs premiers de suites d'entiers particulières. A la fin du XIX$^{\text{ième}}$ siècle, Lucas [17], [18] propose une étude poussée des nombres dits *de Lucas*. Les nombres de Lucas sont des suites d'entiers définies à partir de nombres algébriques réels α et β conjugués de degré 2. Outre les applications importantes de ces suites, en particulier pour l'approximation rapide d'entiers quadratiques ou pour des tests de primalité sur les nombres de Mersenne, Carmichael montre en 1913 que si (u_n) est une suite de Lucas, alors pour n assez grand, il apparaît un nouveau nombre premier dans la décomposition de chacun des entier $u_k,\ k \geqslant n$. En 1930, Lehmer ([16]) généralise les résultats de Lucas en définissant ses propres suites d'entiers. Ward ([32]) en 1955 puis , Durst [10] en 1965 donnent des bornes minimales pour le rang à partir duquel apparaissent ces nouveaux nombres premiers. Une nouvelle généralisation dûe à Schnizel ([21]) en 1962 donne des résultats analogues pour une classe plus générale de suites d'entiers (qui inclus en particulier les couples (α, β) complexes). Yu. Bilu, G. Hanrot et P. Voutier [3] donnent une borne supérieure pour le rang des nombres de Lucas généralisés n'admettant pas de nouveau diviseur premier et P. Voutier dresse dans [30] une liste des paires (α, β) donnant lieux à des suites dégénérées. L'objet du premier chapitre est de reprendre en détail les démonstrations faites dans [3] afin de combler les trous laissés par Voutier et de donner une liste complète des paires de Lucas et Lehmer dites défectueuses.

Le second chapitre est préparatoire. Dans celui-ci, nous mettons en place deux outils fondamentaux pour la résolution effective de certaines classes d'équations diophantiennes : les hauteurs de Weil et les séries de Puiseux.

Dans le troisième chapitre de cette thèse, on s'intéresse aux équations algébriques du type $F(x, y) = 0$ où le polynôme F vérifie $F(0, 0) = 0$. En 1929 Skolem [25] (voir également [24, page 90]) a montré, en utilisant une méthode dûe à Runge que sous cette hypothèse, l'équation

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

n'admettait qu'un nombre fini de solutions entières (α, β) de pgcd Δ fixé. Ce résultat est contenu dans un résultat beaucoup plus général de Siegel paru la même année (voir [22]), mais la méthode de Skolem, contrairement à celle de Siegel est effective. Elle permet en effet de donner des bornes *explicites* pour la taille des solutions de notre problème, ce qui a été fait par P. G. Walsh [31, Theorem 2, p. 159] en 1992. Le troisième chapitre de cette thèse est donc consacré à une amélioration conséquente de ces résultat, basée sur une méthode originale de Sprindzhuk [26, 27] simplifiée par Bilu et Masser [4]. Tout d'abord, à l'aide d'une généralisation de la notion de pgcd aux nombres algébriques, faisant intervenir les hauteurs de Weil (et grâce au caractère absolu de ces hauteurs), on étend ces résultat aux **solutions algébriques** de notre équation (et l'on peut même prendre F à coefficients

dans $\overline{\mathbb{Q}}$). D'autre part, on remplace l'inégalité de Walsh par une **égalité asymptotique**. Ces améliorations ont été faites sous l'hypothèse supplémentaire que $(0,0)$ est un point non singulier de la courbe définie par F. Mais comme on le verra à la fin de la section 3.1, cette hypothèse est purement technique et est amenée à disparaître.

Enfin, le quatrième et dernier chapitre de cette thèse est consacré à l'étude des équations de Thue généralisées. Celui-ci a en effet montré en 1909 que si $\phi(X,Y)$ était une forme homogène à coefficients entiers, irréductible sur $\mathbb{Q}$ et de degré $n \geqslant 3$, alors les équations $\phi(x,y) = A$ pour $A \in \mathbb{Z}$ n'admettaient chacune qu'un nombre fini de solutions entières. Une version effective de ce résultat sera donnée par Baker en 1968. Ainsi, celui-ci démontre que si $(\alpha,\beta) \in \mathbb{Z}^2$ vérifie $\phi(\alpha,\beta) = A$, alors

$$\max\{|\alpha|,|\beta|\} \leqslant \exp((nH)^{10^5})$$

où H est le maximum de $|A|$ et des valeurs absolues des coefficients de ϕ et Feldman en 1971 améliore ce résultat en montrant que les solutions $(\alpha,\beta) \in \mathbb{Z}^2$ de notre problème vérifient

$$\max\{|\alpha|,|\beta|\} \leqslant |A|^c$$

où c est une constante effective ne dépendant que de ϕ. Plusieurs auteurs ont amélioré ces résultats et les ont étendus aux solutions entières (et S-entières) dans un corps de nombres quelconque (voir par exemple [7]). Les méthodes de Thue et de Baker ont comme point de départ la factorisation du polynôme homogène $\phi(X,Y) = (X - \alpha_1 Y)\cdots(X - \alpha_n Y)$ dans une extension finie L de $\mathbb{Q}$. Le polynôme ϕ étant à coefficients rationnels, les nombres algébriques $\alpha_1,\ldots,\alpha_n$ sont conjugués, et ϕ apparaît comme étant la norme $\mathcal{N}_{L/\mathbb{Q}}(X - \alpha_1 Y)$. L'objet de ce quatrième chapitre est donc l'étude des équations du type

$$\mathcal{N}_{L/K}(F(x,y)) = A$$

où K est un corps de nombres donné, L est une extension finie de K de degré $n \geqslant 3$, F est un polynôme à coefficients dans L et $A \in K^*$.

Ce dernier chapitre est le fruit d'un travail effectué conjointement avec A. Berczes et Yu. Bilu.

Chapitre 1

Nombres de Lucas sans diviseur primitif

Une *paire de Lucas* est une paire (α, β) d'entiers algébriques racines d'un polynôme de degré deux à discriminant positif, tels que $\alpha+\beta$ et $\alpha\beta$ soient dans $\mathbb{Z}-\{0\}$, premiers entre eux et tels que α/β ne soit pas une racine de l'unité. A toute paire de Lucas (α, β) on associe une suite d'entiers $(u_n)_{n\in\mathbb{N}^*}$ dite de *nombres de Lucas*, définie par

$$\forall n \in \mathbb{N}^*, \;\; u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

En 1913, Carmichael se penche sur les travaux de Lucas en s'intéressant en particulier aux diviseurs primitifs des nombres de Lucas ([8]). Etant donnée une paire de Lucas (α, β) et un entier n, un diviseur premier de u_n sera dit *primitif* s'il ne divise pas le produit $(\alpha-\beta)^2 u_1 ... u_{n-1}$. En notant P l'application qui à un entier associe sont plus grand diviseur premier, Carmichael montre également que pour $n > 12$, on a

$$P(u_n) \geqslant n - 1.$$

Il en déduit que pour n assez grand, tout nombre u_n admet un diviseur primitif.

En 1930 dans [16], Lehmer généralise les résultats de Lucas en définissant ses propres suites : une *paire de Lehmer* est une paire (α, β) d'entiers algébriques, racines d'un polynôme de degré deux et de discriminant strictement positif, tels que $(\alpha+\beta)^2$ et $\alpha\beta$ soient dans $\mathbb{Z}-\{0\}$, premiers entre eux et tels que α/β ne soit pas une racine de l'unité. A toute paire de Lehmer (α, β) on associe une suite d'entiers $(\tilde{u}_n)_{n\in\mathbb{N}^*}$ dite de *nombres de Lehmer* définie par :

$$\forall n \in \mathbb{N}^*, \;\; \tilde{u}_n = \tilde{u}_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{si } n \text{ est impair,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{si } n \text{ est pair.} \end{cases}$$

Un diviseur premier de $\tilde{u}_n$ sera dit primitif s'il ne divise pas $(\alpha^2-\beta^2)^2 \tilde{u}_1 \dots \tilde{u}_{n-1}$.

En 1955, Ward [32] se penche a son tour sur les nombres de Lehmer, et comme Carmichael l'avait fait pour les nombres de Lucas, il montre que pour $n > 18$, tout nombre $\tilde{u}_n$ admet un diviseur primitif. Ce résultat sera amélioré par Durst qui montre en 1965 dans

[10] qu'il suffit de prendre $n > 12$.
En 1962, Schinzel [21] étend la définition des nombres de Lucas et Lehmer au cas des polynômes de degré deux à discriminant négatifs et montre là encore que pour tout couple (α, β) et pour tout n assez grand, u_n et $\tilde{u}_n$ admettent un diviseur primitif. Yu. Bilu, G. Hanrot et P.M. Voutier [3] ont montré que c'etait le cas dès que $n > 30$.

P. M. Voutier donne également dans [30] une liste exhaustive des paires de Lucas n-défectueuses pour $4 < n \leqslant 30,\ \ n \neq 6$ et des paires de Lehmer n-défectueuses pour $6 < n \leqslant 30,\ \ n \notin \{8, 10, 12\}$. (On dira qu'une paire (α, β) est n-défectueuse si le $n^{\text{ième}}$ terme de la suite associée à (α, β) ne possède pas de diviseur primitif.).

Remarque : toute paire de Lucas (α, β) est également une paire de Lehmer et :

$$u_n = \begin{cases} \tilde{u}_n & \text{si } n \text{ est impair,} \\ (\alpha+\beta)\tilde{u}_n & \text{si } n \text{ est pair.} \end{cases}$$

Ainsi, si (α, β) est une paire de Lucas et $n \in \mathbb{N}\backslash\{2\}$, tout nombre premier r est un diviseur primitif de u_n si et seulement si c'est un diviseur primitif de $\tilde{u}_n$ et une paire de Lucas (α, β) est n-défectueuse si et seulement si c'est une paire de Lehmer n-défectueuse.

Au vu de la forme des termes $u_n(\alpha, \beta)$ et $\tilde{u}_n(\alpha, \beta)$, il est naturel de considérer les polynômes cyclotomiques

$$\Phi_n(X, Y) = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (X - e^{2ik\pi/n}Y)$$

et leurs valeurs en (α, β). Ainsi, pour tout $n \in \mathbb{N}^*$ on a :

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta), \tag{1.1}$$

$$u_n = \prod_{d|n,\ d\neq 1} \Phi_d(\alpha, \beta), \ \ \tilde{u}_n = \prod_{d|n,\ d>2} \Phi_d(\alpha, \beta). \tag{1.2}$$

En particulier, pour tout $n \in \mathbb{N}^*$, $\Phi_n(\alpha, \beta)$ divise u_n et $\tilde{u}_n$.

Cela nous permettra, après une étude rapide de l'arithmétique des suites de Lucas et de Lehmer, d'énoncer un *critère cyclotomique* donnant des restrictions importantes et décisives concernant les paires de Lucas et Lehmer défectueuses. La deuxième partie sera consacrée à l'étude exhaustive des cas laissés de coté par Voutier.

1.1 Critère cyclotomique

1.1.1 Quelques lemmes préliminaires

Proposition 1.1.1 *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Alors :*

1. *Pour tout $m > 0$, on a $(\alpha\beta, \tilde{u}_m) = 1$.*
2. *Si d divise m, alors $\tilde{u}_d$ divise $\tilde{u}_m$ et $(\tilde{u}_m/\tilde{u}_d, \tilde{u}_d)$ divise m/d.*
3. *Pour tous entiers positifs m et n on a $(\tilde{u}_m, \tilde{u}_n) = \tilde{u}_{(m,n)}$.*
4. *Si un nombre premier r ne divise pas $\alpha\beta(\alpha^2 - \beta^2)^2$ alors r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}$.*
5. *Si un nombre premier r divise $\tilde{u}_m$ alors r divise $\tilde{u}_{mr}/\tilde{u}_m$. De plus, si $r > 2$, alors r divise exactement $\tilde{u}_{mr}/\tilde{u}_m$ (i.e. r^2 ne divise pas $\tilde{u}_{mr}/\tilde{u}_m$).*
6. *Si 4 divise $\tilde{u}_m$, alors 2 divise exactement $\tilde{u}_{2m}/\tilde{u}_m$.*
7. *Si un nombre premier $r > 2$ divise $(\alpha - \beta)^2$, alors r divise $\tilde{u}_r$.*
   De plus, si $r > 3$, alors r divise exactement $\tilde{u}_r$.
8. *Si un nombre premier r divise $(\alpha + \beta)^2$, alors r divise $\tilde{u}_{2r}$.*
   De plus, si $r > 3$, alors r divise exactement $\tilde{u}_{2r}$.

Preuve Pour cette preuve, on notera $N_1, N_2, \ldots, N_7$ des entiers algébriques dépendant de α, β et des indices des termes des suites (u_n), (v_n) et $(\tilde{u}_n)$ que l'on considère. Soit donc (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. On définit une nouvelle suite $(v_m)_{m\in\mathbb{N}^*}$:

$$\forall m \in \mathbb{N}^*,\ \ v_m = \begin{cases} (\alpha^m + \beta^m)/(\alpha + \beta) & \text{si } m \text{ est impair,} \\ \alpha^m + \beta^m & \text{si } m \text{ est pair.} \end{cases}$$

1 : Pour tout $m \in \mathbb{N}^*$ on a :

$$\begin{aligned} (\alpha + \beta)^{2m} &= \alpha^{2m} + \beta^{2m} + \alpha\beta N_0 = v_{2m} + \alpha\beta N_0 \\ &= (\alpha^{2m+1} + \beta^{2m+1})/(\alpha + \beta) + \alpha\beta N_1 = v_{2m+1} + \alpha\beta N_1 \end{aligned}$$

Or par hypothèse, $\alpha\beta$ et $(\alpha+\beta)^2$ sont premiers entre eux donc $\alpha\beta$ et v_m le sont également. De même pour tout m impair,

$$\tilde{u}_m = (\alpha^m - \beta^m)/(\alpha - \beta) = v_{m-1} + \alpha\beta N_2$$

et pour m pair,

$$\tilde{u}_m = (\alpha^m - \beta^m)/((\alpha - \beta)(\alpha + \beta)) = v_{m-1} + \alpha\beta N_3.$$

Donc pour tout m, $(\alpha\beta, v_m) = 1$ impose $(\alpha\beta, \tilde{u}_m) = 1$.

2 : Soient $m \in \mathbb{N}$ et d un diviseur de m. D'après (1.2) il est clair que $\tilde{u}_d$ divise $\tilde{u}_m$. D'autre part, comme $\alpha^m = (\beta^d + (\alpha^d - \beta^d))^{m/d}$ on a :

$$\frac{\alpha^m - \beta^m}{\alpha^d - \beta^d} = \sum_{k=1}^{m/d} \left(\begin{array}{c} m/d \\ k \end{array} \right) (\alpha^d - \beta^d)^{k-1} \beta^{m-kd}$$

En multipliant de chaque coté par α^{m-d} il vient :

$$\alpha^{m-d} \frac{\tilde{u}_m}{\tilde{u}_d} = \frac{m}{d} (\alpha\beta)^{m-d} + N_4 \tilde{u}_d \text{ si } m-d \text{ est pair}, \tag{1.3}$$

$$\alpha^{m-d}(\alpha+\beta) \frac{\tilde{u}_m}{\tilde{u}_d} = \frac{m}{d} (\alpha\beta)^{m-d} + N_5 \tilde{u}_d \text{ si } m-d \text{ est impair}. \tag{1.4}$$

Comme $(\alpha\beta, \tilde{u}_d) = 1$, l'assertion *2* est démontrée.

3 : Soient m et n deux entiers positifs. Il existe s et t dans $\mathbb{N}$ tels que

$$tm - sn = (m, n) = d. \tag{1.5}$$

Notons alors $m = dm'$, $n = dn'$, $k = tm$ et $l = sn$. D'après (1.5), $tm' - sn' = 1$ donc t et s, t et n', s et m' sont respectivement premiers entre eux. Ainsi $(k, l) = d$ et $k - l = (k, l)$. D'autre part $(\alpha^k - \beta^k)(\alpha^l + \beta^l) - (\alpha^k + \beta^k)(\alpha^l - \beta^l) = 2(\alpha\beta)^l(\alpha^{k-l} - \beta^{k-l})$ donc

$$\tilde{u}_k v_l - \tilde{u}_l v_k = 2(\alpha\beta)^l \tilde{u}_{k-l} \text{ si } k-l \text{ est pair}, \tag{1.6}$$

$$(\alpha+\beta)^2 \tilde{u}_k v_l - \tilde{u}_l v_k = 2(\alpha\beta)^l \tilde{u}_{k-l} \text{ si } k-l \text{ et } l \text{ sont impairs}, \tag{1.7}$$

$$\tilde{u}_k v_l - (\alpha+\beta)^2 \tilde{u}_l v_k = 2(\alpha\beta)^l \tilde{u}_{k-l} \text{ si } k-l \text{ et } k \text{ sont impairs}. \tag{1.8}$$

Si 2 ne divise pas $(\tilde{u}_k, \tilde{u}_l)$, d'après l'assertion *1*, $(\tilde{u}_k, \tilde{u}_l)$ divise $\tilde{u}_{k-l}$. Supposons donc que 2 divise $(\tilde{u}_k, \tilde{u}_l)$. Comme $\tilde{u}_{2k}/\tilde{u}_k = v_k$, d'après (1.3) et (1.4), comme $\alpha\beta$ et v_k sont premiers entre eux, 2 divise v_k si k est pair et $(\alpha+\beta)^2$ si k est impair. Il en va de même pour l donc dans tous les cas, comme $\alpha\beta$ est premier avec tous les $\tilde{u}_m$, $(\tilde{u}_k, \tilde{u}_l)$ divise $\tilde{u}_{k-l}$. Par ailleurs, comme $k-l$ divise k et l, $\tilde{u}_{k-l}$ divise $(\tilde{u}_k, \tilde{u}_l)$, d'où l'égalité.

4 : Soit r un nombre premier ne divisant pas $\alpha\beta(\alpha^2 - \beta^2)^2$. Si $r > 2$, on a

$$\begin{aligned}(\alpha^2 - \beta^2)^2 \tilde{u}_{r-1}\tilde{u}_{r+1} &= (\alpha^{r-1} - \beta^{r-1})(\alpha^{r+1} - \beta^{r+1}) \\ &= \alpha^{2r} + \beta^{2r} - (\alpha\beta)^{r-1}(\alpha^2 + \beta^2).\end{aligned}$$

Or comme r ne divise pas $\alpha\beta$, d'après le petit théorème de Fermat, il vient :

$$(\alpha-\beta)^2(\alpha+\beta)^2 \tilde{u}_{r-1}\tilde{u}_{r+1} \equiv 0 \mod r,$$

Et comme r est premier avec $(\alpha-\beta)^2(\alpha+\beta)^2$, r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}$.

Pour $r = 2$, on a :

$$\tilde{u}_{r-1}\tilde{u}_{r+1} = \tilde{u}_3 = \alpha^2 + \alpha\beta + \beta^2 = (\alpha+\beta)^2 - \alpha\beta.$$

Donc si 2 ne divise ni $\tilde{u}_3$ ni $\alpha\beta$, alors 2 divise $(\alpha+\beta)^2$, ce qui prouve l'assertion *4*.

5 : Soient $m \in \mathbb{N}^*$ et r un nombre premier. Comme dans la preuve du *2*, on a :

$$\frac{\alpha^{rm} - \beta^{rm}}{\alpha^m - \beta^m} = \sum_{k=1}^{r-1} \left(\begin{array}{c} r \\ k \end{array} \right) (\alpha^m - \beta^m)^{k-1} \beta^{m(r-k)} + (\alpha^m - \beta^m)^{r-1}. \tag{1.9}$$

Or pour tout $k \in \{1, ..., r-1\}$, r divise $\left(\begin{array}{c} r \\ k \end{array} \right)$. De plus, $\alpha^m - \beta^m = N_6\tilde{u}_m$. Donc si r divise $\tilde{u}_m$ alors r divise $(\alpha^{rm} - \beta^{rm})/(\alpha^m - \beta^m) = \tilde{u}_{rm}/\tilde{u}_m$.

D'autre part, si $r > 2$, de (1.9) on tire également

$$\alpha^{m(r-1)}\frac{\tilde{u}_{rm}}{\tilde{u}_m} - r(\alpha^m - \beta^m)N_7 - (\alpha^m - \beta^m)^{r-1}\alpha^{m(r-1)} = r(\alpha\beta)^{m(r-1)}. \tag{1.10}$$

Donc si r divise $\tilde{u}_m$ alors r divise $\alpha^m - \beta^m$ et comme $(\alpha\beta, \tilde{u}_m) = 1$, r^2 ne peut diviser $\tilde{u}_{rm}/\tilde{u}_m$.

6 : soit $m \in \mathbb{N}^*$ tel que 4 divise $\tilde{u}_m$. Alors,

$$\frac{\alpha^{2m} - \beta^{2m}}{\alpha^m - \beta^m} = 2\beta^m + (\alpha^m - \beta^m).$$

Or si m est pair, $(\alpha^{2m} - \beta^{2m})/(\alpha^m - \beta^m) = \tilde{u}_{2m}/\tilde{u}_m$. Donc si 4 divise $\tilde{u}_m$ alors 4 divise $(\alpha^m - \beta^m)$ mais 4 ne divise pas $2\beta^m$ car $(\alpha\beta, \tilde{u}_m) = 1$. Donc 2 divise exactement $\tilde{u}_{2m}/\tilde{u}_m$. Par ailleurs, si m est impair, $(\alpha^{2m} - \beta^{2m})/(\alpha^m - \beta^m) = (\alpha+\beta)\tilde{u}_{2m}/\tilde{u}_m$. Donc si 2 ne divise pas $(\alpha+\beta)^2$, 2 divise exactement $\tilde{u}_{2m}/\tilde{u}_m$. Enfin, si 2 divise $(\alpha+\beta)^2$, alors 2 divise $\tilde{u}_4 = (\alpha+\beta)^2 - 2\alpha\beta$ et d'après l'assertion *3*, $(\tilde{u}_4, \tilde{u}_m) = 1$ donc 2 ne peut pas diviser $\tilde{u}_m$.

7 : soit r un nombre premier impair. En posant $m = 1$ dans l'équation (1.9) il vient :

$$\tilde{u}_r = \frac{\alpha^r - \beta^r}{\alpha - \beta} = \sum_{k=1}^{r-1} \left(\begin{array}{c} r \\ k \end{array} \right) (\alpha - \beta)^{k-1} \beta^{(r-k)} + (\alpha - \beta)^{r-1}.$$

Donc si r divise $(\alpha - \beta)^2$, r divise également $\tilde{u}_r$. De plus, si $r > 3$, r^2 divise tous les termes du second membre de l'équation précédente sauf pour $k = 1$. Donc r^2 ne peut diviser $\tilde{u}_r$.

8 : le raisonnement est le même que pour le cas précédent en posant $m = 2$. □

Corollaire 1.1.2 *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Pour tout nombre premier r qui ne divise pas $\alpha\beta$ il existe un entier positif m tel que r divise $\tilde{u}_m$.*

Preuve Soit r un nombre premier qui ne divise pas $\alpha\beta$. Alors d'après les assertions *4*, *7* et *8*, r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}\tilde{u}_r\tilde{u}_{2r}$. Il existe donc $m > 0$ tel que r divise $\tilde{u}_m$. □

Notons m_r le plus petit entier positif ayant cette propriété.

Corollaire 1.1.3 *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Alors pour tout entier r ne divisant pas $\alpha\beta$, on a*

$$r|\tilde{u}_m \Leftrightarrow m_r|m \tag{1.11}$$

Preuve ($\Leftarrow$) : d'après l'assertion *2*, si m_r divise m alors $\tilde{u}_{m_r}$ divise $\tilde{u}_m$. Or par définition, r divise $\tilde{u}_{m_r}$ donc r divise $\tilde{u}_m$.

($\Rightarrow$) : d'après l'assertion *3*, si r divise $\tilde{u}_m$ alors r divise $(\tilde{u}_{m_r}, \tilde{u}_m) = \tilde{u}_{(m_r,m)}$. Or m_r étant minimal, $m_r \leqslant (m_r, m)$, ce qui n'est possible que si m_r divise m. □

Corollaire 1.1.4 *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Alors pour tout entier r ne divisant pas $\alpha\beta$, on a*

$$m_r = r \text{ si } r > 2 \text{ et } r|(\alpha-\beta)^2, \tag{1.12}$$

$$m_r = 2r \text{ si } r|(\alpha+\beta)^2, \tag{1.13}$$

$$m_r|(r-1) \text{ ou } m_r|(r+1) \text{ sinon.} \tag{1.14}$$

Preuve (1.12) : si $r > 2$ et r divise $(\alpha-\beta)^2$ alors d'après l'assertion *7*, r divise $\tilde{u}_r$. De plus, d'après (1.11), m_r divise r donc $m_r = r$.

(1.14) : pour $r > 2$, si l'on est pas dans les cas (1.12) ou (1.13), d'après l'assertion *4*, r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}$. D'après (1.11), m_r divise donc $(r-1)$ ou $(r+1)$. D'autre part, pour $r = 2$, si 2 ne divise pas $(\alpha+\beta)^2$, alors 2 ne divise pas non plus $(\alpha-\beta)^2$ et toujours d'après l'assertion *4*, 2 divise $\tilde{u}_1\tilde{u}_3$.

(1.13) : si r divise $(\alpha+\beta)^2$, d'après l'assertion *8*, r divise $\tilde{u}_{2r}$. Ainsi, d'après (1.11), on a $m_r = r$ ou $m_r = 2r$. Montrons qu'alors r ne peut pas diviser $\tilde{u}_r$. Si $r = 2$, alors $\tilde{u}_2 = 1$ et il n'y a rien à faire. Si $r > 2$, on a

$$\alpha^r - \beta^r \equiv (\alpha-\beta)^r \mod r. \tag{1.15}$$

Or $(\alpha+\beta)^2$ et $\alpha\beta$ étant premiers entre eux, $((\alpha+\beta)^2, (\alpha-\beta)^2)$ divise 4 donc si r divise $(\alpha+\beta)^2$, il est premier avec $(\alpha-\beta)$. En divisant l'équation (1.15) il vient

$$\tilde{u}_r \equiv (\alpha-\beta)^{r-1} \not\equiv 0 \mod r.$$

Donc r ne divise pas $\tilde{u}_r$ et $m_r = 2r$. □

En particulier, si 2 ne divise pas $\alpha\beta$ alors

$$m_2 = \begin{cases} 4 & \text{si } 2|(\alpha^2-\beta^2)^2, \\ 3 & \text{sinon.} \end{cases} \tag{1.16}$$

et si 3 ne divise pas $\alpha\beta$ alors

$$m_3 = \begin{cases} 3 \text{ ou } 6 & \text{si } 3|(\alpha^2-\beta^2)^2, \\ 4 & \text{sinon.} \end{cases} \tag{1.17}$$

Proposition 1.1.5 *Soit (α,β) une paire de Lehmer et soit r un diviseur premier de $\Phi_n(\alpha,\beta)$, $n>2$. Alors r ne divise pas $\alpha\beta$ et il existe $k \geqslant 0$ tel que $n = m_r r^k$.*

Preuve Soient $n>2$ et r un diviseur premier de $\Phi_n = \Phi_n(\alpha,\beta)$. Comme Φ_n divise $\tilde{u}_n$, d'après l'assertion *1* de la proposition 1.1.1, r ne divise pas $\alpha\beta$. D'après le corollaire 1.1.3, m_r divise n. Il existe donc $t>0$ et $k \geqslant 0$ tels que $(t,r)=1$ et $n = m_r t r^k$. Supposons alors que $t>1$. Toujours d'après le corollaire 1.1.3, r divise $\tilde{u}_{n/t}$. De plus, comme $n/t<n$, l'entier Φ_n divise encore $\tilde{u}_n/\tilde{u}_{n/t}$ et donc r divise également $\tilde{u}_n/\tilde{u}_{n/t}$. D'après l'assertion *2* de la propostion 1.1.1, il vient alors que r divise $\frac{n}{n/t} = t$, ce qui est exclu. Donc $t=1$ et $n = m_r r^k$. □

1.1.2 Le critère cyclotomique

Rappelons que pour un entier n fixés, une paire de Lehmer (α,β) sera dite n-défectueuse si le $n^{\text{ième}}$ terme de la suite de Lehmer associée à (α,β) n'admet pas de diviseur primitif. D'autre part, pour n dans $\mathbb{N}^*$ notons $P(n)$ le plus grand diviseur premier de n et $P'(n) = P(n/(n,3))$. On peut alors énoncer le théorème suivant.

Théorème 1.1.6 (Critère cyclotomique) *Soit $n>4$ un entier distinct de 6 et 12. Une paire de Lehmer (α,β) est n-défectueuse si et seulement si $\Phi_n(\alpha,\beta) \in \{\pm 1, \pm P'(n)\}$. De plus, une paire de Lehmer (α,β) est 12-défectueuse si et seulement si $\Phi_{12}(\alpha,\beta) \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$.*

Preuve $(\Rightarrow)$: soit $n \in \mathbb{N}^*$ tel que $n>4$ et $n \neq 6$ et soit (α,β) une paire de Lehmer n-défectueuse. Pour tout diviseur premier r de Φ_n, on a $r|\tilde{u}_n$. D'après la proposition précédente, r ne divise pas $\alpha\beta$ et il existe $k \geqslant 0$ tel que $n = m_r r^k$. Comme $\tilde{u}_n$ n'admet pas de diviseur primitif, par minimalité de m_r il vient :

$$n = m_r r^k \text{ avec } k \geqslant 1, \tag{1.18}$$

ou

$$n = m_r \text{ et } r|(\alpha^2-\beta^2)^2. \tag{1.19}$$

D'après le corollaire 1.1.4, on a donc :

$$r = \begin{cases} P'(n) & \text{si } n \neq 12, \\ 2 \text{ ou } 3 & \text{si } n = 12. \end{cases} \tag{1.20}$$

Il nous reste à montrer que r divise exactement Φ_n. Pour cela, on distingue les cas (1.18) et (1.19) :

• $n = m_r r^k,\ \ k \geqslant 1$: tout d'abord, comme m_r divise n/r, d'après le corollaire 1.1.3, r divise $\tilde{u}_{n/r}$. On distingue alors les cas $r > 2$ et $r = 2$:

- Si $r > 2$, d'après l'assertion *5* de la proposition 1.1.1, il vient que r divise exactement $\tilde{u}_n/\tilde{u}_{n/r}$. Comme Φ_n divise également $\tilde{u}_n/\tilde{u}_{n/r}$, r divise exactement Φ_n.
- Si $r = 2$ et 2 ne divise pas $(\alpha^2 - \beta^2)^2$, d'après le corollaire 1.1.4, on a $m_2 = 3$ et donc $n = 3.2^k,\ \ k \geqslant 2$ (car $n \neq 6$). Par ailleurs, $\Phi_3 = \tilde{u}_3 = \alpha^2 + \beta^2 - \alpha\beta$. Donc comme 2 ne divise ni $\alpha\beta$ ni $\alpha^2 + \beta^2$, Φ_3 est pair. De plus, $\Phi_3 - \Phi_6 = 2\alpha\beta \equiv 2 \mod 4$. Donc 4 divise Φ_3 ou Φ_6 et donc 4 divise $\tilde{u}_3$ ou $\tilde{u}_6$. Dans tous les cas, 4 divise $\tilde{u}_6$ (car $3|6 \Rightarrow \tilde{u}_3|\tilde{u}_6$ d'après l'assertion *2* de la proposition 1.1.1). Enfin, toujours d'après l'assertion *2* de la proposition 1.1.1, comme 6 divise $n/2$, 4 divise également $\tilde{u}_{n/2}$ et d'après la proposition 1.1.1, *6*, 2 divise exactement $\tilde{u}_n/\tilde{u}_{n/2}$. Il en est donc de même pour Φ_n.
- Enfin, si $r = 2$ et $2|(\alpha^2 - \beta^2)^2$, d'après le corollaire 1.1.4, $m_2 = 4$ et donc $n = 2^k,\ \ k \geqslant 3$. On démontre par récurrence sur k que pour tout $k \geqslant 3$, 2 divise exactement Φ_{2^k}. En effet, comme 2 divise $(\alpha - \beta)^2(\alpha + \beta)^2$, 2 divise l'un des deux facteurs et donc 2 divise $\alpha^2 + \beta^2 = (\alpha - \beta)^2 + 2\alpha\beta = (\alpha + \beta)^2 - 2\alpha\beta$. Ainsi, 4 divise $(\alpha^2 + \beta^2)^2 = \alpha^4 + \beta^4 + 2(\alpha\beta)^2$. Donc comme $\alpha\beta \equiv 2 \mod 4$, 2 divise exactement $\Phi_8 = \alpha^4 + \beta^4$. On montre de même que si 2 divise $\alpha^{2^{k-1}} + \beta^{2^{k-1}} = \Phi_{2^k}$ alors 2 divise exactement $\alpha^{2^k} + \beta^{2^k} = \Phi_{2^{k+1}}$.

• $n = m_r$ et $r|(\alpha^2 - \beta^2)^2$: comme $n \notin \{3, 4, 6\}$, alors $r > 3$. D'après les assertions *7* et *8* de la proposition 1.1.1, r divise donc exactement $\tilde{u}_n = \tilde{u}_{m_r}$, ce qui termine la première partie de la démonstration.

($\Leftarrow$) : soit $n \in \mathbb{N}^*$ tel que $n > 4$ et $n \neq 6$ et soit (α, β) une paire de Lehmer telle que

$$\Phi_n \in \begin{cases} \{\pm 1, \pm P'(n)\} & \text{si } n \neq 12, \\ \{\pm 1, \pm 2, \pm 3, \pm 6\} & \text{si } n = 12. \end{cases} \tag{1.21}$$

Montrons qu'alors, (α, β) est n-défectueuse.

Soit r un diviseur premier de $\tilde{u}_n$. D'après (1.2), $\tilde{u}_n$ apparait comme étant un élement du groupe multiplicatif engendré par les $\{\Phi_m,\ \ m > 2,\ \ m|n\}$, $(\alpha + \beta)^2$ et $(\alpha - \beta)^2$. Donc r divise l'un de ces nombres. Mais alors r divise $(\alpha^2 - \beta^2)^2 \prod_{1 \leqslant k < n} \tilde{u}_k$ et ça n'est pas un diviseur primitif de $\tilde{u}_n$. De plus, si r divise Φ_n alors d'après (1.21), r vérifie (1.20). En particulier, $r|n$. Ainsi, si $m_r < n$ alors par définition de m_r, r n'est pas un diviseur primitif de $\tilde{u}_n$ et si $m_r = n$, d'après le corollaire 1.1.4, r divise $(\alpha^2 - \beta^2)^2$ ce qui prouve encore que r n'est pas un diviseur primitif de $\tilde{u}_n$ et qui termine la démonstration du théorème 1.1.6. □

1.2 Les paires de Lucas et Lehmer défectueuses

Dans la suite, les paires de Lehmer (α, β) défectueuses seront données par un couple (a, b) tel que $\alpha, \beta = \frac{\sqrt{a} \pm \sqrt{b}}{2}$. Par ailleurs, on notera $p = (\alpha+\beta)^2$ et $q = \alpha\beta \neq 0$. Ainsi, $a = p$ et $b = p - 4q$. De même, les paires de Lucas (α, β) défectueuses seront données par un couple (a, b) tel que $\alpha, \beta = \frac{a \pm \sqrt{b}}{2}$. Par ailleurs, on notera $m = \alpha + \beta = \sqrt{p}$ et $q = \alpha\beta \neq 0$. Ainsi, $a = m$ et $b = m^2 - 4q$.

1.2.1 Restrictions

Deux paires de Lucas (α_1, β_2) et (α_2, β_2) seront dites *équivalentes* si $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$. Deux paires de Lehmer (α_1, β_2) et (α_2, β_2) seront dites *équivalentes* si $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm i\}$. Si (α_1, β_2) et (α_2, β_2) sont deux paires de Lucas (resp. Lehmer) équivalentes, $u_n(\alpha_1, \beta_1) = \pm u_n(\alpha_2, \beta_2)$ (resp. $\tilde{u}_n(\alpha_1, \beta_1) = \pm \tilde{u}_n(\alpha_2, \beta_2)$). Ainsi, si une paire est n-défectueuse pour un n donné, il en est de même pour toute paire équivalente, et l'on pourra parfois choisir le signe de u_n (resp. $\tilde{u}_n$).

D'autre part, α/β n'étant pas une racine de l'unité, on a nécessairement

$$(p, q) \notin \{\pm(1, 1), \pm(2, 1), \pm(3, 1), \pm(4, 1)\} \tag{1.22}$$

En effet, si l'on note $\gamma = \alpha/\beta$, comme α et β sont les racines du polynôme $X^2 - \sqrt{p}X + q$, on vérifie rapidement que γ et γ^{-1} sont les racines du polynôme $qX^2 - (p - 2q)X + q \in \mathbb{Z}[X]$. Donc γ est un nombre algébrique de degré au plus 2 et p et q étant premiers entre eux, γ est une racine k-ième de l'unité si et seulement si $\phi(k) \leqslant 2$, i.e. $q = \pm 1$ et $|p - 2q| \leqslant 2$, ce qui correspond exactement aux cas exclus dans (1.22).
Clairement, si (α, β) est une paire de Lucas, quitte à changer (α, β) en une paire équivalente, on peut supposer $m > 0$ et comme $m = \sqrt{p}$, il vient :

$$(m, q) \notin \{(1, 1), (2, 1)\} \tag{1.23}$$

Enfin, d'après l'assertion *1* de la proposition 1.1.1, si (α, β) est une paire de Lehmer, on a :

$$(\tilde{u}_n, q) = (\Phi_n, q) = (p, q) = 1 \tag{1.24}$$

1.2.2 $n = 2$

Toute paire de **Lehmer** est 2-défectueuse car $\tilde{u}_2 = 1$.

Soit (α, β) une paire de **Lucas** 2-défectueuse. Comme $u_1 = 1$, tout nombre premier r divisant u_2 divise $(\alpha - \beta)^2$. Or avec les notations précédentes, il vient :

$$u_2 = \frac{\alpha^2 - \beta^2}{\alpha - \beta} = \alpha + \beta = m$$

et

$$(\alpha-\beta)^2=(\alpha+\beta)^2-4\alpha\beta=m^2-4q$$

Ainsi, m et q étant premiers entre eux, r ne peut qu'être égal a 2. Quitte à changer (α,β) en $(-\alpha,-\beta)$, on peut supposer que u_2 est positif. Il existe donc un entier naturel k tel que $u_2=2^k$. Le couple (a,b) associé à la paire (α,β) est donc de la forme $(2^k,4^k-4q)$.

On distingue alors les cas $k=0$ et $k\geqslant 1$:
- $k=0$: $(a,b)=(1,1-4q)$ et (1.23) impose $q\neq 1$.
- $k\geqslant 1$: $(a,b)=(2^k,4^k-4q)$ et (1.24) impose $q\equiv 1 \mod 2$.
  Pour $k=1$, (1.23) impose également $q\neq 1$.

1.2.3 $n=3$

Soit (α,β) une paire de **Lehmer** 3-défectueuse. On a $\tilde{u}_3=p-q$. Comme $\tilde{u}_1=\tilde{u}_2=1$, tout diviseur premier r de $\tilde{u}_3$ divise $(\alpha^2-\beta^2)^2=(\tilde{u}_3+q)(\tilde{u}_3-3q)$. D'après (1.24), on a donc nécessairement $r=3$. Quitte a remplacer (α,β) par $(i\alpha,i\beta)$, on peut supposer que $\tilde{u}_3>0$. Il existe donc $k\geqslant 0$ tel que $\tilde{u}_3=3^k$ et $p=3^k+q$.
$(a,b)=(p,p-4q)$ est donc de la forme $(3^k+q,3^k-3q)$.

- $k=0$: $(a,b)=(1+q,1-3q)$ et (1.22) impose $q\neq 1$.
- $k\geqslant 1$: $(a,b)=(3^k+q,3^k-3q)$ et (1.24) impose $q\not\equiv 0 \mod 3$.
  Pour $k=1$, (1.22) impose également $q\neq 1$.

Soit (α,β) une paire de **Lucas** 3-défectueuse. On a $u_3=\tilde{u}_3=m^2-q$, mais contrairement au cas précédent, on ne peut pas supposer $u_3>0$. Donc $u_3=\varepsilon 3^k,\ \varepsilon=\pm 1,\ k\geqslant 0$. Ainsi, (a,b) est de la forme $(m,4\varepsilon 3^k-3m^2)$.

- $k=0$: si $\varepsilon=-1$, $(a,b)=(m,-4-3m^2)$.
  En particulier, $m=1$ **est permis.**
  Si $\varepsilon=1$, $(a,b)=(m,4-3m^2)$ et $q\neq 0$ impose $m>1$.
- $k\geqslant 1$: $(a,b)=(m,4\varepsilon 3^k-3m^2)$ et (1.24) impose $m\not\equiv 0 \mod 3$.
  Si $\varepsilon=k=1$, (1.23) impose également $m\neq 2$.
  En particulier, $\varepsilon=-1$ **permet** $(k,m)=(1,2)$

1.2.4 $n=4$

Soit (α,β) un paire de **Lehmer** 4-défectueuse. Comme $\tilde{u}_3=p-q$ et $\tilde{u}_4=p-2q$, il vient $(\tilde{u}_3,\tilde{u}_4)=1$ car $(p,q)=1$. Tout diviseur r de $\tilde{u}_4$ divise donc $(\alpha^2-\beta^2)^2=(\tilde{u}_4+2q)(\tilde{u}_4-2q)$. Donc $r=2$ et quitte a changer (α,β) en une paire équivalente, on peut supposer que $\tilde{u}_4=2^k,\ k\geqslant 0$. Le couple (a,b) est donc de la forme $(2^k+2q,2^k-2q)$.

- $k=0$: $(a,b)=(1+2q,1-2q)$ et (1.22) impose $q\neq 1$.

– $k \geqslant 1 : (a,b) = (2^k + 2q, 2^k - 2q)$ et (1.24) impose $q \equiv 1 \mod 2$.
Pour $k \in \{1,2\}$, (1.22) impose également $q \neq 1$.

Soit (α, β) un paire de **Lucas** 4-défectueuse. C'est également une paire de Lehmer 4-défectueuse donc le seul diviseur premier de $\tilde{u}_4 = m^2 - 2q$ est 2. Mais l'on ne peut plus choisir le signe de $\tilde{u}_4$, donc $\tilde{u}_4 = \varepsilon 2^k$, $\varepsilon \in \{\pm 1\}$, $k \geqslant 0$. Le couple (a,b) est donc de la forme $(m, \varepsilon 2^{k+1} - m^2)$.

– $k = 0 : (a,b) = (m, 2\varepsilon - m^2)$ et $2q = m^2 - \varepsilon$ impose $m \equiv 1 \mod 2$ et (1.23) impose $m \neq 1$.
– $k = 1 : (a,b) = (m, 4\varepsilon - m^2)$ et $2q = m^2 - 2\varepsilon$ impose $m \equiv 0 \mod 2$.
Si $\varepsilon = 1$, (1.23) impose également $m \neq 2$.
En particulier, $\varepsilon = -1$ **permet** $m = 2$**.**
– Si $k > 1$, $2q = m^2 - 2^k\varepsilon$ impose $m \equiv q \equiv 0 \mod 2$, ce qui est exclu.

1.2.5 $n = 5$

Soit (α, β) une paire de **Lehmer** 5-défectueuse. D'après le critère cyclotomique, $\Phi_5 = (p - \eta^2 q)(p - \overline{\eta}^2 q) \in \{\pm 1, \pm 5\}$, où $\eta = \frac{1+\sqrt{5}}{2}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{5})$. Si $\Phi_5 = \pm 1$, $p - \eta^2 q$ est une unité. Il existe donc $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta^2 q = \varepsilon_0 \eta^{\varepsilon k}$. Si $\Phi_5 = \pm 5$, 5 se ramifie dans $\mathbb{Q}(\sqrt{5})$ donc $(5) = \mathfrak{p}^2$ où $\mathfrak{p} = (\sqrt{5})$. En notant $(p - \eta^2 q) = \prod_{i=1}^{s} \mathfrak{a}_i^{e_i}$, il vient :

$$\prod_{i=1}^{s} (\mathfrak{a}_i \overline{\mathfrak{a}}_i)^{e_i} = \mathfrak{p}^2$$

Donc $s = 1$ et $\mathfrak{a}_1 = \overline{\mathfrak{a}}_1 = \mathfrak{p}$ et il existe $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta^2 q = \varepsilon_0 \sqrt{5} \eta^{k\varepsilon}$. Quitte a changer (α, β) en une paire équivalente, on a donc :

$$p - \eta^2 q = -\varepsilon(\varepsilon \eta^{\varepsilon})^k \tag{1.25}$$

ou

$$p - \eta^2 q = -\sqrt{5}(\varepsilon \eta^{\varepsilon})^k \tag{1.26}$$

En considérant les équations conjuguées dans $\mathbb{Q}(\sqrt{5})$, il vient :
– (1.25) donne $p = \phi_{k-2\varepsilon}$, $q = \phi_k$, où (ϕ_k) est la suite de Fibonacci.
Ainsi, $(a,b) = (\phi_{k-2\varepsilon}, \phi_{k-2\varepsilon} - 4\phi_k)$ et (1.22) impose $k \geqslant 3$.
– (1.26) donne $p = \psi_{k-2\varepsilon}$, $q = \psi_k$, où (ψ_k) est définie par $\psi_0 = 2, \psi_1 = 1, \psi_{k+2} = \psi_{k+1} + \psi_k$. On a alors $(a,b) = (\psi_{k-2\varepsilon}, \psi_{k-2\varepsilon} - 4\psi_k)$ et (1.22) impose $k \neq 1$.

1.2.6 $n = 6$

Soit (α, β) une paire de **Lehmer** 6-défectueuse. On a $\tilde{u}_6 = p^2 - 4pq + 3q^2$. De plus, $(\tilde{u}_5, \tilde{u}_6) = 1$. En effet, $\tilde{u}_5 = p^2 - 3pq + q^2$, donc tout diviseur r de $(\tilde{u}_5, \tilde{u}_6)$ divise

$\tilde{u}_6 - \tilde{u}_5 = q(2q-p)$. D'après (1.24), r divise $p-2q$ donc r divise $(p-2q)^2 - \tilde{u}_6 = q^2$ et $r = 1$ toujours d'après (1.24). De même, $\tilde{u}_4 = p - 2q$, donc $(\tilde{u}_4, \tilde{u}_6) = 1$. Ainsi, comme $\Phi_6 = p - 3q$ divise $\tilde{u}_6$, tout diviseur r de Φ_6 divise $(\alpha^2-\beta^2)^2\tilde{u}_3 = (\Phi_6+3q)(\Phi_6-q)(\Phi_6+2q)$. Toujours d'après (1.24), il vient $r \in \{2,3\}$. Quitte à changer (α,β) en une paire équivalente, il existe donc $l, k \geqslant 0$ tels que $\Phi_6 = 2^k 3^l$ et (a,b) est de la forme $(2^k3^l+3q, 2^k3^l-q)$.

- $l = k = 0 : (a,b) = (1+3q, 1-q)$ et (1.22) impose $q \neq 1$.
- $l = 0,\ k \geqslant 1 : (a,b) = (2^k+3q, 2^k-q)$ et $p = 2^k+3q$ impose $p \equiv q \mod 2$, donc (1.24) impose $q \equiv 1 \mod 2$.
  Pour $k = 1$, (1.22) impose $q \neq -1$.
- $l \geqslant 1,\ k = 0 : (a,b) = (3^l+3q, 3^l-q)$. $p = 3^l+3q$ impose $q \not\equiv 0 \mod 3$.
  Pour $l = 1$, (1.22) impose $q \neq -1$.
- $l \geqslant 1,\ k \geqslant 1 : (a,b) = (2^k3^l+3q, 2^k3^l-q)$ et $p = 2^k3^l+3q$ impose $q \equiv \pm 1 \mod 6$.

Soit (α,β) une paire de **Lucas** 6-défectueuse. C'est également une paire de Lehmer 6-défectueuse, mais comme plus haut, on ne peut choisir le signe de Φ_6. Donc $\Phi_6 = \varepsilon 2^k 3^l = m^2 - 3q$ et (a,b) est de la forme $(m, \frac{1}{3}(\varepsilon 2^{k+2}3^l - m^2))$.

- $l = 0,\ k = 0 : m^2 = \varepsilon + 3q \equiv \varepsilon \mod 3$ et comme -1 n'est pas un carré modulo 3, il vient $\varepsilon = 1$ et $m \not\equiv 0 \mod 3$. De plus, $q = \frac{1}{3}(m^2-1)$ donc (1.22) impose $m \neq 1$ et $m \neq 2$. On a donc $(a,b) = (m, \frac{1}{3}(4-m^2))$ avec $m \geqslant 4,\ m \not\equiv 0 \mod 3$.
- $l = 0,\ k \geqslant 1 : m^2 - 3q = 2^k\varepsilon$, donc $m \equiv q \mod 2$ et (1.24) impose $m \equiv 1 \mod 2$. De plus, $m^2 \equiv (-1)^k\varepsilon \mod 3$ donc $\varepsilon = (-1)^k$ et $m \not\equiv 0 \mod 3$.
  On a donc $(a,b) = (m, \frac{1}{3}((-2)^{k+2} - m^2))$, $m \equiv \pm 1 \mod 6$ et pour $k = 1$, (1.23) impose $m \neq 1$.
- $l = 1 : (a,b) = (m, 2^{k+2}\varepsilon - \frac{m^2}{3})$ et $m^2 = \varepsilon 3.2^k + 3q$ impose $m \equiv 0 \mod 3$.
  Pour $k \geqslant 1$, $m \equiv q \mod 2$ donc (1.24) impose $m \equiv 1 \mod 2$, i.e. $m \equiv 3 \mod 6$.
- $l > 1 : m \equiv 0 \mod 3$ donc 9 divise $3q = m^2 - \varepsilon 2^k 3^l$ et donc 3 divise (m,q) ce qui est exclu.

1.2.7 $n = 8$

Soit (α,β) une paire de **Lehmer** 8-défectueuse. D'après le critère cyclotomique, $\Phi_8 = (p - q\eta\sqrt{2})(p - q\overline{\eta}\sqrt{2}) \in \{\pm 1, \pm 2\}$, où $\eta = 1+\sqrt{2}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$. Comme dans le cas $n = 5$, comme 2 se ramifie dans $\mathbb{Q}(\sqrt{2})$, quitte a changer (α,β) en une paire équivalente, il existe $\varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tel que

$$p - q\eta\sqrt{2} = -\varepsilon(\varepsilon\eta^\varepsilon)^k \tag{1.27}$$

ou

$$p - q\eta\sqrt{2} = -\sqrt{2}(\varepsilon\eta^\varepsilon)^k \tag{1.28}$$

En considérant les équations conjuguées dans $\mathbb{Q}(\sqrt{2})$, il vient :

– l'équation (1.27) donne $p = \rho_{k-\varepsilon},\ \ q = \pi_k$, où (ρ_k) est définie par $\rho_0 = \rho_1 = 1$ et $\rho_{k+2} = 2\rho_{k+1} + \rho_k$ et (π_k) est donnée par $\pi_0 = 0,\ \ \pi_1 = 1$ et $\pi_{k+2} = 2\pi_{k+1} + \pi_k$. Donc $(a, b) = (\rho_{k-\varepsilon}, \rho_{k-\varepsilon} - 4\pi_k)$.
– l'équation (1.28) donne $p = 2\pi_{k-\varepsilon},\ \ q = \rho_k$ et $(a, b) = (2\pi_{k-\varepsilon}, 2\pi_{k-\varepsilon} - 4\rho_k)$.
Dans les deux cas, (1.22) impose $k \geqslant 2$.

1.2.8 $n = 10$

Pour tout couple (α, β), $\Phi_{10}(\alpha, \beta) = \Phi_5(-\alpha, \beta)$. Ainsi, si (α, β) est une paire de **Lehmer** 10-défectueuse, d'après le critère cyclotomique, il vient :

$$\Phi_{10}(\alpha, \beta) = \Phi_5(-\alpha, \beta) = (p' - \eta^2 q')(p' - \overline{\eta}^2 q') \in \{\pm 1, \pm 5\}$$

où $q' = -\alpha\beta = -q$ et $p' = (-\alpha + \beta)^2 = p + 4q$.
D'après l'étude du cas $n = 5$, on a donc :
– $p = p' + 4q' = \phi_{k-2\varepsilon} + 4\phi_k,\ \ q = -q' = -\phi_k$. Donc $(a, b) = (\phi_{k-2\varepsilon} + 4\phi_k, \phi_{k-2\varepsilon})$ et (1.22) impose $k \geqslant 3$.
– $p = p' + 4q' = \psi_{k-2\varepsilon} + 4\psi_k,\ \ q = -q' = -\psi_k$. Donc $(a, b) = (\psi_{k-2\varepsilon} + 4\psi_k, \psi_{k-2\varepsilon})$ et (1.22) impose $k \neq 1$.

1.2.9 $n = 12$

Soit (α, β) une paire de **Lehmer** 12-défectueuse. D'après le critère cyclotomique,

$$\Phi_{12} = (p - q\eta)(p - q\overline{\eta}) \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

où $\eta = 2 + \sqrt{3}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{3})$. Si $\Phi_{12} = \pm 1$, $p - \eta q$ est une unité. Il existe donc $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0 \eta^{\varepsilon k}$. Si $\Phi_{12} = \pm 3$, comme 3 se ramifie dans $\mathbb{Q}(\sqrt{3})$, il existe $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0 \sqrt{3} \eta^{\varepsilon k}$. Si $\Phi_{12} = \pm 2$, en notant $\theta = 1 + \sqrt{3}$, on a $\overline{\theta} = \theta\overline{\eta}$. Donc 2 se ramifie dans $\mathbb{Q}(\sqrt{3})$ et comme pour le cas $n = 5$, $p - \eta q$ est associé a θ. Il existe donc $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0 \theta \eta^{\varepsilon k}$. Enfin, si $\Phi_{12} = \pm 6$, il existe $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0 \theta \sqrt{3} \eta^{\varepsilon k}$. Quitte a remplacer (α, β) par une paire équivalent, on a donc :

$$p - \eta q = -\varepsilon \eta^{\varepsilon k} \tag{1.29}$$

$$p - \eta q = -\sqrt{3} \eta^{\varepsilon k} \tag{1.30}$$

$$p - \eta q = -\varepsilon \theta \eta^{\varepsilon k} \tag{1.31}$$

ou

$$p - \eta q = -\sqrt{3} \theta \eta^{\varepsilon k} \tag{1.32}$$

En considérant les équations conjuguées, il vient $p = \zeta^{(i)}_{k-\varepsilon},\ \ q = \zeta^{(i)}_k,\ \ i \in \{0, 1, 2, 3\}$ où les suites $(\zeta^{(i)}_k)$ sont définies par $\zeta^{(i)}_{k+1} = 4\zeta^{(i)}_k - \zeta^{(i)}_{k-1}$ et les valeurs initiales suivantes :

i	0	1	2	3
$\zeta_0^{(i)}$	0	1	ε	1
$\zeta_1^{(i)}$	1	2	$2\varepsilon+1$	$3\varepsilon+2$

Par ailleurs, $p-4q=\zeta_{k-\varepsilon}^{(i)}-4\zeta_k^{(i)}=-\zeta_{k+\varepsilon}^{(i)}$. Donc $(a,b)=(\zeta_{k-\varepsilon}^{(i)},-\zeta_{k+\varepsilon}^{(i)})$ et (1.22) impose $(i,k)\notin\{(0,0),(0,1),(1,0),(2,0)\}$ et si $\varepsilon=-1$, $(i,k)\neq(2,1)$.

1.3 Conclusion

On a démontré le théorème suivant :

Théorème 1.3.1 *Toute paire de Lucas est* 1*-défectueuse et toute paire de Lehmer est* 1*- et* 2*-défectueuse.*
Pour $n\in\{2,3,4,6\}$, à équivalence près, toute paire de Lucas n-défectueuse est de la forme $((a+\sqrt{b})/2,(a-\sqrt{b})/2)$ où (a,b) est donné dans la table ci- dessous.

n	(a,b)	
2	$(1,1-4q)$, $q\neq 1$	$(2^k,4^k-4q)$, $k>0$, $q\equiv 1 \mod 2$, $(k,q)\neq(1,1)$
3	$(m,-4-3m^2)$,	$(m,4.3^k\varepsilon-3m^2)$, $m\not\equiv 0 \mod 3$, $k>0$, $(\varepsilon,k,m)\neq$
	$(m,4-3m^2)$, $m>1$	$(1,1,2)$
4	$(m,2\varepsilon-m^2)$, $m\equiv 1 \mod 2$, $m\neq 1$	$(m,4\varepsilon-m^2)$, $m\equiv 0 \mod 2$, $(\varepsilon,m)\neq(1,2)$
6	$(m,(4-m^2)/3)$, $m\not\equiv 0 \mod 3$, $m>3$	$(m,((-2)^{k+2}-m^2)/3)$, $k>0$, $m\equiv\pm1 \mod 6$, $(k,m)\neq(1,1)$
	$(m,4\varepsilon-m^2/3)$, $m\equiv 0 \mod 3$	$(m,2^{k+2}\varepsilon-m^2/3)$, $k>0, m\equiv 3 \mod 6$

Pour $n\in\{3,4,5,6,8,10,12\}$, à équivalence près, toute paire de Lehmer n-défectueuse est de la forme $((\sqrt{a}+\sqrt{b})/2,(\sqrt{a}-\sqrt{b})/2)$ où (a,b) est donné dans la table ci- dessous.

n	(a,b)	
3	$(1+q,1-3q)$, $q\neq 1$	$(3^k+q,3^k-3q)$, $k>0$, $q\not\equiv 0 \mod 3$, $(k,q)\neq(1,1)$
4	$(1+2q,1-2q)$, $q\neq 1$	$(2^k+2q,2^k-2q)$, $k>0$, $q\equiv 1 \mod 2$, $(k,q)\notin\{(1,1),(2,1)\}$
5	$(\phi_{k-2\varepsilon},\ \phi_{k-2\varepsilon}-4\phi_k)$, $k>2$	$(\psi_{k-2\varepsilon},\psi_{k-2\varepsilon}-4\psi_k)$, $k\neq 1$
6	$(1+3q,1-q)$, $q\neq 1$	$(2^k+3q,2^k-q)$, $k>0$, $q\equiv 1 \mod 2$, $(k,q)\neq(1,-1)$
	$(3^l+3q,3^l-q)$, $l>0$, $q\not\equiv 0 \mod 3$, $(l,q)\neq(1,-1)$	$(2^k3^l+3q,2^k3^l-q)$, $k,l>0$, $q\equiv\pm1 \mod 6$
8	$(\rho_{k-\varepsilon},\rho_{k-\varepsilon}-4\pi_k)$, $k>1$	$(2\pi_{k-\varepsilon},2\pi_{k-\varepsilon}-4\rho_k)$, $k>1$
10	$(\phi_{k-2\varepsilon}+4\phi_k,\phi_{k-2\varepsilon})$, $k>2$	$(\psi_{k-2\varepsilon}+4\psi_k,\psi_{k-2\varepsilon})$, $k\neq 1$
12	$(\zeta_{k-\varepsilon}^{(i)},-\zeta_{k+\varepsilon}^{(i)})$, $(i,k)\notin\{(0,0),(0,1),(1,0),(2,0)\}$, $(i,k,\varepsilon)\neq(2,1,-1)$	

Rappelons que les suites (ϕ_k) *et* (ψ_k) *sont définies au paragraphe 1.2.5, les suites* (ρ_k) *et* (π_k) *sont définies au paragraphe 1.2.7 et les suites* $(\zeta_k^{(i)})$, $i = 0, 1, 2, 3$ *sont définies au paragraphe 1.2.9.*

Chapitre 2

Hauteurs de Weil et séries de Puiseux

Dans le second chapitre, nous mettons donc en place deux outils fondamentaux pour la résolution effective de certaines classes d'équations diophantiennes. Nous rappelons tout d'abord la définition des hauteurs logarithmiques de Weil pour les nombres algébriques et les polynômes à coefficients algébriques. L'une des principales propriétés de ces hauteurs de Weil est son caractère absolu. La normalisation choisie pour les valeurs absolues sur un corps de nombres donné nous assure en effet que la hauteur de Weil d'un nombre algébrique ou d'un polynôme à coefficients algébriques ne dépend pas du corps de nombre dans lequel on se place. Par ailleurs, à partir des définitions, on obtient rapidement des propriétés fondamentales pour les hauteurs de polynômes (hauteur de la somme, hauteur du produit,...) ainsi que pour les hauteur de certains nombres algébriques associés à ces polynômes (hauteur d'une racine,...). Enfin, nous développons également dans ce second chapitre la notion de séries de Puiseux associées à une équation algébrique $F(x,y)=0$. Un théorème de Puiseux (voir par exemple [12]) nous dit en effet que le corps des séries de Puiseux $\cup_{n\in\mathbb{N}^*}\overline{\mathbb{Q}}((X^{1/n}))$ est algébriquement clos. Ainsi, pour un polynôme $F(X,Y)$ à coefficients algébriques, il existe un polynôme $\phi(X)\in\overline{\mathbb{Q}}[X]$ et $\nu=\deg_Y F$ séries de Puiseux $\mathcal{Y}_1(X),\dots,\mathcal{Y}_\nu(X)$ telles que

$$F(X,Y)=\phi(X)\prod_{i=1}^{\nu}(Y-\mathcal{Y}_i(X)).$$

D'autre part, si le polynôme F est à coefficients dans un corps de nombres K donné, le corps engendré par les coefficients des séries de Puiseux associées est une extension finie de K de degré inférieur ou égal à ν. Enfin, des versions effectives d'un théorème d'Eisenstein dûes à Dwork et Van de Poorten [11] nous permettent de contrôler les coefficients des séries $\mathcal{Y}_i(X)$ en fonction du polynôme F et donc les rayons de convergence de ces séries pour les métriques induites par les différentes valuations du corps de nombres dans lequel on travaille.

2.1 Hauteurs logarithmiques de Weil

Dans toute la suite, la lettre K désignera un corps de nombre de degré d. Pour un corps de nombres K donné, on notera $\mathcal{M}_K$ l'ensemble de ses valuations, normalisées de façon à étendre les valuations de $\mathbb{Q}$. Précisément, si $v \in \mathcal{M}_K$ est une place infinie correspondant à un plongement réel σ de K ou à une paire de plongements complexes conjugué $(\sigma, \overline{\sigma})$, pour tout $\alpha \in K$, la valeur absolue v-adique de α sera donnée par $|\alpha|_v = |\alpha^\sigma|$ où $|\cdot|$ est la valeur absolue sur $\mathbb{C}$, alors que si v est une valuation finie prolongeant une valuation p-adique de $\mathbb{Q}$, on aura $|p|_v = p^{-1}$. Pour une valuation $v \in \mathcal{M}_K$ donnée, on notera K_v le complété de K pour la métrique induite par v et l'on notera d_v le degré $[K_v : \mathbb{Q}_v]$. On notera également $\mathcal{M}_K^\infty$ l'ensemble des places infinies de K et $\mathcal{M}_K^0$ l'ensemble des valuations finies. Ainsi normalisées, les valuations satisfont la formule du produit suivante :

$$\forall\, \alpha \in K^*, \qquad \prod_{v \in \mathcal{M}_K} |\alpha|_v^{d_v/d} = 1.$$

D'autre part, pour un nombre algébrique $\alpha \in K$ et pour une valuation $v \in \mathcal{M}_K$, on notera

$$\|\alpha\|_v = \max\{1, |\alpha|_v\}.$$

On peut donc ainsi définir la *hauteur logarithmique absolue de Weil* d'un nombre algébrique α :

$$h(\alpha) = \sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log \|\alpha\|_v.$$

On peut également définir deux *hauteurs locales* de α en une place v de K :

$$h_v^+(\alpha) = \frac{d_v}{d} \log \|\alpha\|_v$$
$$h_v^-(\alpha) = -\frac{d_v}{d} \log \min\{1, |\alpha|_v\}.$$

Grâce à la formule du produit, on a $h(\alpha) = \sum_{v \in \mathcal{M}_K} h_v^+(\alpha) = \sum_{v \in \mathcal{M}_K} h_v^-(\alpha)$. De même, pour un sous-ensemble S de $\mathcal{M}_K$, on définit deux hauteurs locales de α en S comme étant

$$h_S^+(\alpha) = \sum_{v \in S} h_v^+(\alpha)$$
$$h_S^-(\alpha) = \sum_{v \in S} h_v^-(\alpha).$$

Enfin, étant donné un polynôme F dont les coefficients $\{a_{ij}\}$ sont dans K, pour toute valuation $v \in \mathcal{M}_K$ on notera $|F|_v = \max_{ij}\{|a_{ij}|_v\}$ et $\|F\|_v = \max_{ij}\{1, |a_{ij}|_v\}$. La *hauteur affine* de F désignera alors la quantité

$$h_{\mathbb{A}}(F) = \sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log \|F\|_v,$$

et la *hauteur projective* de F sera

$$h_{\mathbb{P}}(F) = \sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log |F|_v.$$

(Lorsque le type de hauteur ne sera pas précisé, on pourra utiliser l'une ou l'autre indifféremment).

Notons qu'à l'aide de la formule du produit, il est facile de voir que la hauteur d'un nombre algébrique ou d'un polynôme à coefficients algébriques ne dépend pas du corps dans lequel on se place. D'autre part, pour tout polynôme F à coefficients algébriques, on a clairement $h_{\mathbb{P}}(F) \leqslant h_{\mathbb{A}}(F)$ pour tout nombre algébrique α on a $h(\alpha) = h_{\mathbb{P}}(X-\alpha) = h_{\mathbb{A}}(X-\alpha)$.

Enonçons maintenant quelques propriétés des hauteurs de Weil.

Proposition 2.1.1 *Soient $F_1(X), \ldots, F_r(X)$ des polynômes à coefficients dans un corps de nombres K. Alors pour toute valuation finie $v \in \mathcal{M}_K$ on a*

$$|F_1 \cdots F_r|_v = |F_1|_v \cdots |F_r|_v,$$

et pour toute place infinie $v \in \mathcal{M}_K$ on a

$$e^{-(N_1+\cdots+N_r)}|F_1|_v \cdots |F_r|_v \leqslant |F_1 \cdots F_r|_v \leqslant 2^{N_1+\cdots+N_r}|F_1|_v \cdots |F_r|_v, \tag{2.1}$$

où $N_i = \deg F_i \qquad (i = 1, \ldots, r)$.

Preuve Dans le cas où v est fini, c'est un résultat classique ; voir par exemple, [15, III, Section 2]. Dans le cas où v est infinie, le membre de gauche de (2.1) est l'inégalité $(*)$ dans la preuve de la proposition B.7.3 de [23] avec $m = 1$. Le membre de droite est la proposition B.7.4 (a) dans [23] avec $n = 1$. □

De la proposition précédente, on obtient rapidement une estimation pour la hauteur projective d'un produit de polynômes.

Proposition 2.1.2 *Soient $F_1(X), \ldots, F_r(X)$ des polynômes à coefficients algébriques. Alors*

$$h_{\mathbb{P}}(F_1)+\cdots+h_{\mathbb{P}}(F_r)-(N_1+\cdots+N_r) \leqslant h_{\mathbb{P}}(F_1 \cdots F_r) \leqslant h_{\mathbb{P}}(F_1)+\cdots+h_{\mathbb{P}}(F_r)+(N_1+\cdots+N_r)\log 2,$$

où $N_i = \deg F_i$ for $i = 1, \ldots, r$).

En particulier, si un polynôme $G(X)$ divise un polynôme $F(X)$ alors

$$h_{\mathbb{P}}(G) \leqslant h_{\mathbb{P}}(F) + \deg F$$

Preuve En passant au logarithme, en sommant sur toutes les places de K et en remarquant que $\sum_{v\in\mathcal{M}_K^\infty} d_v = d$, on obtient le résultat souhaité. □

Puisque le hauteur d'un nombre algébrique α est égal à la hauteur du polynôme $X-\alpha$, on déduit de la proposition 2.1.2 le résultat suivant.

Proposition 2.1.3 *Soit $F(X)$ un polynôme de degré N, à coeffcients algébriques et soit α une racine de F. Alors*

$$h(\alpha) \leqslant h(F) + N.$$

Énonçons maintenant quelques propriétés sur les hauteurs de polynômes en deux variables.

Proposition 2.1.4 *Soient $F_1(X,Y),\dots,F_r(X,Y)$ des polynômes à coefficients algébriques. Alors*

$$h_{\mathbb{A}}(F_1+\cdots+F_r) \leqslant h_{\mathbb{A}}(F_1)+\cdots+h_{\mathbb{A}}(F_r)+\log r$$

Proof Montrons cela pour $r=2$, le cas général se traitant exactement de la même façon. Soit v une place de K. Si v est finie, on a

$$\|F_1+F_2\|_v \leqslant \max\{1,|F_1|_v,|F_2|_v\} \leqslant \max\{1,|F_1|_v\}\max\{1,|F_2|_v\}$$

et si v est infinie, on a

$$\|F_1+F_2\|_v \leqslant \max\{1,|F_1|_v+|F_2|_v\} \leqslant 2\max\{1,|F_1|_v\}\max\{1,|F_2|_v\}.$$

Ainsi,

$$h_{\mathbb{A}}(F_1+F_2) \leqslant h_{\mathbb{A}}(F_1)+h_{\mathbb{A}}(F_2)+\log 2.$$

□

Proposition 2.1.5 *Soient $F_1(X,Y),\dots,F_r(X,Y)$ des polynômes à coefficients algébriques.*

1. *Notons $\mu_i = \deg_X F_i$ et $\nu_i = \deg_Y F_i$, $(i=1,\dots,r)$. Alors*

$$h_{\mathbb{A}}(F_1\cdots F_r) \leqslant \sum_{i=1}^{r}(h_{\mathbb{A}}(F_i)+\mu_i+\nu_i)+2r.$$

2. *Soient N_1 et N_2 des nombres entiers tels que $\deg_X(F_1\cdots F_r)\leqslant N_1$ et $\deg_Y(F_1\cdots F_r)\leqslant N_2$. Alors*

$$h_{\mathbb{P}}(F_1)+\cdots+h_{\mathbb{P}}(F_r) \leqslant h_{\mathbb{P}}(F_1\cdots F_r)+N_1+N_2$$

En particulier, si un polynôme $G(X,Y)$ divise un polynôme $F(X,Y)$ alors

$$h_{\mathbb{P}}(G) \leqslant h_{\mathbb{P}}(F)+\deg F$$

Proposition 2.1.6 *Soient $F_1(X,Y)$ et $F_2(X,Y)$ deux polynômes à coefficients algébriques, tels que*

$$\mu_i = \deg_X F_i, \quad \nu_i = \deg_Y F_i \qquad (i = 1, 2).$$

Soit également $R(X)$ leur résultant par rapport à la variable Y. Alors si $R(X)$ n'est pas identiquement nul, on a

$$h_{\mathbb{P}}(R) \leqslant \nu_1 h_{\mathbb{P}}(F_2) + \nu_2 h_{\mathbb{P}}(F_1) + (\mu_1\nu_2 + \mu_2\nu_1) + (\nu_1 + \nu_2)\log(\nu_1 + \nu_2).$$

Proof Soit K un corps de nombres contenant les coefficients de F_1 et F_2. Notons

$$F_i(X,Y) = a_{i\nu_i}(X)Y^{\nu_i} + \cdots + a_{i1}(X)Y + a_{i0}(X) \qquad (i = 1, 2),$$

où $a_{ik}(X) \in K[X]$. En écrivant le résultant sous la forme d'un déterminant (voir par exemple [14, Chapter IV, Section 8]), le polynôme $R(X)$ apparaît comme une somme de $(\nu_1 + \nu_2)!$ polynômes en X, chacun de ces polynômes étant soit nul, soit composé de ν_2 facteurs pris parmis les $\pm a_{1k}(X)$ et ν_1 facteurs pris parmis les $\pm a_{2k}(X)$. En notant $u(X)$ l'un de ces termes, d'après la proposition 2.1.1, il vient

$$|u|_v \leqslant |F_1|_v^{\nu_2} |F_2|_v^{\nu_1}$$

pour une place finie v de K et

$$|u|_v \leqslant 2^{\mu_1\nu_2 + \mu_2\nu_1} |F_1|_v^{\nu_2} |F_2|_v^{\nu_1}$$

pour une place infinie. Ainsi,

$$|R|_v \leqslant |F_1|_v^{\nu_2} |F_2|_v^{\nu_1}$$

pour une place finie v de K et

$$|R|_v \leqslant (\nu_1 + \nu_2)! 2^{\mu_1\nu_2 + \mu_2\nu_1} |F_1|_v^{\nu_2} |F_2|_v^{\nu_1}$$

pour une place infinie. En passant au logarithme et en sommant sur toutes les places $v \in \mathcal{M}_K$, on obtient

$$\begin{aligned} h(R) \leqslant & \nu_2 h(F_1) + \nu_1 h(F_2) + \log((\nu_1 + \nu_2)! 2^{\mu_1\nu_2 + \mu_2\nu_1}) \\ \leqslant & \nu_2 h(F_1) + \nu_1 h(F_2) + (\mu_1\nu_2 + \mu_2\nu_1) + (\nu_1 + \nu_2)\log(\nu_1 + \nu_2). \end{aligned}$$

□

Proposition 2.1.7 *Soit $F(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ tel que $\mu = \deg_X F$ et $\nu = \deg_Y F$ et soient α, β deux nombres algébriques.*

1. *On a $h(F(\alpha,\beta)) \leqslant h_{\mathbb{P}}(F) + \mu h(\alpha) + \nu h(\beta) + \log((\mu+1)(\nu+1))$.*
2. *Si $F(\alpha,\beta) = 0$ et $F(\alpha, Y)$ n'est pas identiquement nul, alors*

$$h(\beta) \leqslant h_{\mathbb{P}}(F) + \mu h(\alpha) + \nu + \log(\mu + 1).$$

3. *Soit $F_1(X,Y) = F(X + \alpha, Y + \beta)$. Alors*

$$h(F_1) \leqslant h(F) + \mu h(\alpha) + \nu h(\beta) + \mu + \nu + \log(\mu + 1) + \log(\nu + 1).$$

Proof Soit K un corps de nombres contenant les coefficients de F et les nombres α and β.

1. Pour toute place $v \in \mathcal{M}_K$ on a
$$|F(\alpha,\beta)|_v \leq |F|_v \max\{1,|\alpha|_v^\mu\}\max\{1,|\beta|_v^\nu\}$$
si v est finie, et
$$|F(\alpha,\beta)|_v \leqslant (\mu+1)(\nu+1)|F|_v \max\{1,|\alpha|_v^\mu\}\max\{1,|\beta|_v^\nu\}$$
si v est infinie. En passant au logarithme et en sommant sur toutes les places $v \in \mathcal{M}_K$, on obtient résultat souhaité.
2. Notons $f(Y) = F(\alpha, Y)$. Alors
$$|f|_v \leqslant \begin{cases} |F|_v \max\{1,|\alpha|_v\}^\mu & \text{si } v \text{ est finie,} \\ (\mu+1)|F|_v \max\{1,|\alpha|_v\}^\mu & \text{si } v \text{ est infinie.} \end{cases}$$
Ainsi, $h(f) \leqslant h(F) + \mu h(\alpha) + \log(\mu+1)$. Mais β étant une racine de f, la proposition 2.1.3 nous donne le résultat souhaité.
3. En développant le polynôme F_1, on obtient
$$F_1(X,Y) = \sum_{\substack{0\leqslant k\leqslant m \\ 0\leqslant \ell\leqslant \nu}} \sum_{\substack{k\leqslant i\leqslant \mu \\ \ell\leqslant j\leqslant \nu}} a_{ij}\binom{i}{k}\binom{j}{\ell}\alpha^{i-k}\beta^{j-\ell}X^kY^\ell$$
où les (a_{ij}) sont les coefficients de F. Ainsi,
$$|F_1|_v \leqslant \begin{cases} |F|_v \max\{1,|\alpha|_v^\mu\}\max\{1,|\beta|_v^\nu\} & \text{si } v \text{ est finie,} \\ (\mu+1)(\nu+1)2^{\mu+\nu}|F|_v \max\{1,|\alpha|_v^\mu\}\max\{1,|\beta|_v^\nu\} & \text{sinon.} \end{cases}$$
En passant au logarithme et en sommant sur toutes les places $v \in \mathcal{M}_K$, on obtient le résultat souhaité. □

2.2 Séries de Puiseux et théorème d'Eisenstein

2.2.1 Séries de Puiseux en 0

Soit $F(X,Y)$ un polynôme à coefficients dans un corps de nombres K donné. Si F vérifie
$$F(0,0) = 0, \qquad \partial_Y F(0,0) \neq 0, \tag{2.2}$$
d'après le théorème de Puiseux il existe une unique série formelle $\mathcal{Y}(X) \in K[[X]]$ telle que $\mathcal{Y}(0) = 0$ et $F(X, \mathcal{Y}(X)) = 0$. Des versions numériques modernes du théorème d'Eisenstein permettent d'estimer les coefficients de cette série en termes de F (voir par exemple [11]). Mais sous les hypothèses 2.2, Hindry et Silvermann [23, Proposition E.9.1] donnent une meilleur estimation pour les coefficients de $\mathcal{Y}$.

Théorème 2.2.1 *Soit* $\mathcal{Y}(X) = \sum_{k\geqslant 1} a_k X^k \in K[[X]]$ *la série formelle vérifiant* $F(X, \mathcal{Y}(X)) = 0$. *Alors pour toute place* v *de* K *et pour tout* $k \geqslant 1$, *on a*

$$|a_k|_v \leqslant \begin{cases} \dfrac{|F|_v^{2k}}{|\partial_Y F(0,0)|_v^{2k}} & \text{si } v \text{ est finie,} \\ (2\mu+2\nu)^{11k}\dfrac{|F|_v^{2k}}{|\partial_Y F(0,0)|_v^{2k}} & \text{sinon.} \end{cases} \tag{2.3}$$

Ainsi, en notant

$$A_v = \begin{cases} \dfrac{|F|_v^{2k}}{|\partial_Y F(0,0)|_v^{2k}} & \text{si } v \text{ est finie,} \\ (2\mu+2\nu)^{11k}\dfrac{|F|_v^{2k}}{|\partial_Y F(0,0)|_v^{2k}} & \text{sinon,} \end{cases}$$

pour toute valuation $v \in \mathcal{M}_K$ on a $A_v \geqslant 1$ avec égalité presque toujours. D'autre part, pour tout $k \geqslant 1$, on a

$$|a_k|_v \leqslant A_v^k. \tag{2.4}$$

Enfin, on a

$$\begin{aligned} \sum_{v\in\mathcal{M}_K} \frac{d_v}{d}\log A_v =& 2\sum_{v\in\mathcal{M}_k}\frac{d_v}{d}\log|F|_v - 2\sum_{v\in\mathcal{M}_k}\frac{d_v}{d}\log|\partial_Y F(0,0)|_v + 11\log(2\mu+2\nu) \\ =& 2h(F) + 11\log(2\mu+2\nu). \end{aligned}$$

2.2.2 Séries de Puiseux générales

Sans supposer (2.2), il existe toujours des développements de Puiseux pour le polynôme F, mais ces développements peuvent alors être ramifiés. Les résultats que nous établissons dans cette section sont établis au voisinage de l'infini plutôt qu'au voisinage de 0 car c'est ce dont nous aurons besoin dans le quatrième chapitre. Ainsi, il existe un polynôme $\phi(X) \in K[X]$, une extension finie $\widetilde{K}$ de K et ν séries formelles $\mathcal{Y}_1(X), \ldots, \mathcal{Y}_\nu(X) \in \cup_{n\in\mathbb{N}^*}\widetilde{K}((X^{-1/n}))$ telles que

$$F(X,Y) = \phi(X)\prod_{i=1}^{\nu}\left(Y - \mathcal{Y}_i(X)\right).$$

Pour chaque série $\mathcal{Y}_i$, notons e_i le plus petit entier tel que $\mathcal{Y}_i(X) = \sum_{k\geqslant -k_i} a_{ik}X^{-k/e_i} \in \widetilde{K}((X^{-1/e_i}))$. Le théorème suivant nous donne une borne pour les coefficients a_{ik} des séries $\mathcal{Y}_i(X)$, $i = 1, 2, \ldots, \nu$.

Théorème 2.2.2 (Eisenstein) *Pour toute valuation* $v \in \mathcal{M}_K$ *il existe des nombres réels* A_v, $A'_v \geqslant 1$ *presque tous égaux à* 1 *tels que*

$$\sum_{v\in\mathcal{M}_K}\frac{d_v}{d}\log A_v \leqslant 2\nu h_{\mathbb{P}}(F) + O(\nu(\nu + \log 3\mu\nu)) \tag{2.5}$$

$$\sum_{v\in\mathcal{M}_K}\frac{d_v}{d}\log A'_v \leqslant h_{\mathbb{P}}(F)+O(\log\nu) \tag{2.6}$$

et tels que pour toute place w de $\widetilde{K}$ divisant v, et pour tout $i\in\{1,\dots,\nu\}$, on ait

$$|a_{ik}|_w \leqslant A'_v A_v^{\mu+k/e_i}, \qquad (k\geqslant -k_i). \tag{2.7}$$

Preuve Soit $\widetilde{F}(X,Y)=X^{\mu}F(X^{-1},Y)$. Pour tout $i\in\{1,\dots,\nu\}$, on note $\widetilde{\mathcal{Y}}_i(X)=\mathcal{Y}_i(X^{-1})$. En appliquant le théorème 2.1 de [5] à $\widetilde{G}(X,Y)$ et aux séries $\widetilde{\mathcal{Y}}_1(X),\dots,\widetilde{\mathcal{Y}}_\nu(X)$, on obtient pour tout $i=1,\dots,\nu$ et pour tout $v\in\mathcal{M}_K$ des nombres réels $A_{i,v}$ et $A'_{i,v}$ vérifiant (2.5), (2.6) et (2.7). En notant $A_v=\max_i\{A_{i,v}\}$ et $A'_v=\max_i\{A'_{i,v}\}$ on obtient le résultat voulu. □

2.2.3 Convergence des séries de Puiseux à l'infini

Considérons maintenant un couple $(\alpha,\beta)\in\overline{\mathbb{Q}}^2$ tel que $F(\alpha,\beta)=0$. Le théorème 2.2.2 nous donne deux propriétés concernant la convergence des séries $\mathcal{Y}_i(X)$ en $X=\alpha$. Notons d'abord $\varepsilon=\mathrm{ppcm}(e_1,\dots,e_\nu)$ et fixons une ε-ième racine de α dans $\overline{\mathbb{Q}}$. Cela détermine une e_i-ième racine de α pour tout $i\in\{1,\dots,\nu\}$. Dans la suite, cette racine sera notée α^{1/e_i}.

Proposition 2.2.1 (convergence locale) *Soit $(\alpha,\beta)\in\overline{\mathbb{Q}}^2$ tel que $F(\alpha,\beta)=0$ et $\phi(\alpha)\neq 0$. Pour toute valuation v de $\widetilde{K}(\alpha,\beta)$ telle que $|\alpha|_v>A_v$, la série $\sum a_{ik}(\alpha^{1/e_i})^{-k}$ converge v-adiquement pour tout $i\in\{1,\dots,\nu\}$ et si l'on note $\mathcal{Y}_i^{(v)}(\alpha)$ sa somme, il existe $i\in\{1,\dots,\nu\}$ tel que $\mathcal{Y}_i^{(v)}(\alpha)=\beta$*

Proof D'après le théorème 2.2.2, si $|\alpha|_v>A_v$, la série $\mathcal{Y}_i^{(v)}(\alpha)$ converge absolument. Ainsi, le polynôme $\phi(\alpha)\prod_{i=1}^{\nu}(Y-\mathcal{Y}_i^{(v)}(\alpha))$ n'est autre que $F(\alpha,Y)$. Mais alors, β étant une racine de ce polynôme, on obtient le résultat souhaité. □

Proposition 2.2.2 (global convergence) *Soit S un sous ensemble fini de $\mathcal{M}_K$ et soit $(\alpha,\beta)\in\mathcal{O}_S\times K$ tel que $F(\alpha,\beta)=0$ et $\phi(\alpha)\neq 0$. Alors soit*

$$h(\alpha)\leqslant 2\nu h_{\mathbb{P}}(F)+O(\nu(\nu+\log 3\mu\nu))$$

soit il existe une valuation $v\in S$ et un indice $i\in\{1,\dots,\nu\}$ tels que $\mathcal{Y}_i^{(w)}(\alpha)=\beta$ pour toute place $w\in\mathcal{M}_{\widetilde{K}}$, $w|v$.

Proof Comme α est un S-entier, on a

$$h(\alpha)=\sum_{v\in S}\frac{d_v}{d}\log\|\alpha\|_v.$$

Soit alors v_0 une valuation de S telle que $|\alpha|_{v_0}=\max_{v\in S}\{|\alpha|_v\}$. Alors, soit $|\alpha|_{v_0}\leqslant A_{v_0}$, ce qui nous donne le premier cas, soit $|\alpha|_{v_0}>A_{v_0}$ et d'après la proposition 2.2.1, on obtient le second cas. □

2.2.4 Puissances d'une série de Puiseux

Dans les chapitres suivants, on sera amenés à utiliser des séries du type $G(X, \mathcal{Y}(X))$ où G est un polynôme donné et $\mathcal{Y}$ une série de Puiseux fixée. Les théorèmes ci-dessus nous permettent d'estimer les coefficients des séries de Puiseux. La proposition suivante nous aidera à estimer les coefficients des séries du type $G(X, \mathcal{Y}(X))$.

Proposition 2.2.3 *Pour tout $r \in \mathbb{N}^*$, notons $\mathcal{Z}_r(x) = \mathcal{Y}(x)^r = \sum_{k\geqslant 0} b_k^{(r)} x^k$. Si pour toute valuation $v \in \mathcal{M}_K$ il existe des nombres réels A_v, $A'_v \geqslant 1$ et un entier μ tels que pour tout $k \geqslant 0$ on ait $|a_k|_v \leqslant A'_v A_v^{\mu+k}$, alors pour toute valuation v de K et pour tout $k \geqslant 0$ on a*

$$|b_k^{(r)}|_v \leqslant \begin{cases} A_v'^r A_v^{r\mu+k} & \text{si } v \text{ est finie,} \\ \binom{r+k-1}{k} A_v'^r A_v^{r\mu+k} & \text{sinon.} \end{cases} \tag{2.8}$$

Preuve On montre cela par récurrence sur r. C'est clair pour $r = 1$. Supposons donc que (2.8) est vrai pour un $r \in \mathbb{Z}^{\geqslant 1}$. Alors

$$\mathcal{Z}_{r+1}(x) = \mathcal{Y}(x)^{r+1} = \sum_{k\geqslant 0} \left(\sum_{i=0}^{k} a_i b_{k-i}^{(r)} \right) x^k.$$

Pour toute valuation finie $v \in \mathcal{M}_K$ on a donc

$$|b_k^{(r+1)}|_v \leqslant \max_i \{A'_v A_v^{\mu+i} A_v'^r A_v^{r\mu+k-i}\} = A_v'^{r+1} A_v^{(r+1)\mu+k}$$

et pour toute valuation infinie, on a

$$\begin{aligned} |b_k^{(r+1)}|_v &\leqslant \sum_{i=0}^{k} |a_i|_v |b_{k-i}^{(r)}|_v \leqslant A_v'^{r+1} A_v^{(r+1)\mu+k} \sum_{i=0}^{k} \binom{r+k-i-1}{r-1} \\ &= \binom{r+k}{r} A_v'^{r+1} A_v^{(r+1)\mu+k}. \end{aligned}$$

Dans tous les cas, on a démontré (2.8) au rang $r+1$. □

Chapitre 3

Diophantine equations and gcd

In 1929, Skolem [25] (see also [24, page 90]) proved, using a method of Runge that if $F(x, y)$ was an irreducible polynomial with integral coefficients satisfying $F(0, 0) = 0$, the equation $F(x, y) = 0$ had only finitely many solutions $(\alpha, \beta) \in \mathbb{Z}^2$ with bounded $\gcd(\alpha, \beta)$. Unfortunately, Skolem's result was overshadowed by the seminal theorem of Siegel [22], proved the same year : the equation $F(x, y) = 0$ has only finitely many solutions unless the plane curve defined by this equation is rational.

Still, Skolem's approach, when it applies, has an important advantage. While the argument of Siegel is ineffective, that is, it does not imply any explicit bound for the solutions of our equation, the method of Skolem allows one, in principle, to bound the solutions with $\gcd(\alpha, \beta) = \Delta$ explicitly in terms of the polynomial F and the number Δ.

Indeed, in 1992, P. G. Walsh [31, Theorem 2, p. 159] gave an explicit version of Skolem's result. He proved that if F is a polynomial as above, then the integral solutions (α, β) of $F(x, y) = 0$ with $\gcd(\alpha, \beta) = \Delta$ satisfy

$$|\alpha| \leqslant (\mu^6\nu^6(\mu + 1)^{\nu-1}\Delta^{\mu\nu}H^{\nu})^{2\mu^6\nu^6}$$

and similarly for β. Here μ and ν are the degrees of F in X and Y, respectively, and H is the maximum of absolute values of the coefficients of F. In the special case when F defines a plane curve of genus 0 and $(0, 0)$ is a non-singular point of this curve, D. Poulakis [29] slightly refined the estimate of Walsh, proving that the solutions were bounded by $c(\mu, \nu)\Delta^{2\nu}H^{230\mu^2\nu^6}$,

In this chapter, we improve on the work of Walsh and Poulakis in two directions. First of all, we show that, with a suitable generalization of the notion of gcd, the assertion holds for a polynomial with any algebraic coefficients and for **algebraic solutions** α, β, not just for the solutions in rational integers.

Second, we not only estimate α and β in terms of Δ (and F), but we obtain a sort of **asymptotic equality when** $h(\alpha)$ tends to infinity. For instance, our Theorem 3.1.3 implies that in the particular case $\alpha, \beta \in \mathbb{Z}$ we have $\log|\alpha|$ approximately equal to $\nu \log \Delta$ and $\log|\beta|$ to $\mu \log \Delta$.

We do not make any restriction on the genus of the curve given by F but, to simplify some arguments, we assume that $(0, 0)$ is a non-singular point of our curve. But this

assumption is purely technical : a suitable refinement of our method allows one to drop it, see the end of Subsection 3.1.

Skolem and Walsh used the methods of Runge. Poulakis used a rational parametrization of the genus 0 curve. Our argument is based on the method of Sprindzhuk [26, 27] in the simplified form due to Bilu and Masser [4].

Let $F(X, Y)$ be a polynomial with algebraic coefficients such that $(0, 0)$ is a non-singular point of the curve defined by F. In the first section of this chapter, we define the logarithmic gcd of two algebraic numbers and we give the explicit asymptotic equality satisfied by the solutions of the equation $F(x, y) = 0$. In Section 3.3, we prove Theorem 3.1.1 and in the last section, we state an explicit version of the quasi-equivalence of heights, which allows us to symmetrize Theorem 3.1.1.

3.1 Main results

In this chapter, the locals heights we will use will always be the "minus" ones. That is

$$\begin{aligned} h_v &= h_v^-, \qquad v \in \mathcal{M}_K \\ h_S &= h_S^-, \qquad S \subset \mathcal{M}_K. \end{aligned}$$

As announced, we need first to generalize the notion of gcd to algebraic numbers. Then, let α and β be non-zero algebraic numbers and let K be a number field containing α and β. We define the logarithmic gcd of α and β to be

$$\operatorname{lgcd}(\alpha, \beta) = \sum_{v \in \mathcal{M}_K} \min\{h_v(\alpha), h_v(\beta)\}.$$

(One can quickly check that if α and β belong in $\mathbb{Z}$ we have $\operatorname{lgcd}(\alpha, \beta) = \log|\gcd(\alpha, \beta)|$.)

The main result of this chapter is the following.

Theorem 3.1.1 *Let $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be an absolutely irreducible polynomial with $\mu = \deg_X F$ and $\nu = \deg_Y F$. Assume that*

$$F(0, 0) = 0, \qquad \partial_Y F(0, 0) \neq 0. \tag{3.1}$$

Let ε satisfy $0 < \varepsilon \leqslant 1$. Then for all $(\alpha, \beta) \in \overline{\mathbb{Q}}^* \times \overline{\mathbb{Q}}$ such that $F(\alpha, \beta) = 0$ we have either

$$h(\alpha) \leqslant 27\mu\nu^5\varepsilon^{-2}h(F) + 171\mu\nu^5\varepsilon^{-2}\log(2\mu + 2\nu) \tag{3.2}$$

or

$$|h(\alpha) - \nu \operatorname{lgcd}(\alpha, \beta)| \leqslant \varepsilon h(\alpha) + 41\nu^3\varepsilon^{-1}h(F) + 275\nu^3\varepsilon^{-1}\log(2\mu + 2\nu). \tag{3.3}$$

Let $F(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ be an absolutely irreducible polynomial and let (α_k, β_k) be a sequence of algebraic points on the plane curve $F(x,y) = 0$. It is well known that, when $h(\alpha_k)$ tends to infinity, we have an asymptotic equality $\mu h(\alpha_k) \sim \nu h(\beta_k)$. This property is called **the quasi-equivalence of heights**. As a consequence of Theorem 3.1.1 we obtain a quantitative version of this property.

Corollary 3.1.2 *Let $F(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ be an absolutely irreducible polynomial and let μ, ν and ε be as in Theorem 3.1.1. Then for any couple $(\alpha,\beta) \in \overline{\mathbb{Q}}^2$ such that $F(\alpha,\beta) = 0$, we have either*

$$\max\{h(\alpha), h(\beta)\} \leqslant 56M^8\varepsilon^{-2}h(F) + 420M^{10}\varepsilon^{-2}\log(4M), \tag{3.4}$$

or

$$\left|\frac{h(\alpha)}{\nu} - \frac{h(\beta)}{\mu}\right| \leqslant \varepsilon h(\alpha) + 330M^5\varepsilon^{-1}h(F) + 2606M^7\varepsilon^{-1}\log(4M), \tag{3.5}$$

where $M = \max\{\mu,\nu\}$.

Habegger [13] recently suggested another explicit version of quasi-equivalence of heights on a curve.

An obvious disadvantage of Theorem 3.1.1 is that it is non-symmetric in X and Y. Using Corollary 3.1.2, we obtain the following symmetric statement.

Theorem 3.1.3 *Let $F(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ be an absolutely irreducible polynomial such that $(0,0)$ is a non-singular point of the curve $F(X,Y) = 0$. Then for any solution $(\alpha,\beta) \in \overline{\mathbb{Q}}^* \times \overline{\mathbb{Q}}$ of $F(X,Y) = 0$, we have either* (3.4) *holds or*

$$\max\{|h(\alpha)-\nu\Delta|, |h(\beta)-\mu\Delta|\} \leqslant \varepsilon h(\alpha)+742M^7\varepsilon^{-1}h(F)+5762M^9\varepsilon^{-1}\log(2\mu+2\nu), \tag{3.6}$$

where $\Delta = \mathrm{lgcd}(\alpha,\beta)$ and $M = \max\{\mu,\nu\}$.

Remark that by specifying the parameter ε, one can obtain the familiar square root form for the error term in the asymptotic estimates (3.3), (3.5) and (3.6). For instance, in Theorem 3.1.1, taking

$$\varepsilon = 15\sqrt{\frac{\mu\nu^5(h(F)+\log(2\mu+2\nu))}{h(\alpha)}},$$

we obtain the following.

Corollary 3.1.4 *In the set-up of Theorem 3.1.1, we have either*

$$h(\alpha) \leqslant 225\mu\nu^5(h(F)+\log(2\mu+2\nu)),$$

or

$$|h(\alpha) - \nu\mathrm{lgcd}(\alpha,\beta)| \leqslant 40\mu^{1/2}\nu^{5/2}\sqrt{h(\alpha)(h(F)+\log(2\mu+2\nu))}.$$

One can do similarly for Corollary 3.1.2 and Theorem 3.1.3.

We remark in conclusion that the non-singularity assumption can be dropped. In this case $|h(\alpha) - \nu\mathrm{lgcd}(\alpha,\beta)|$ and $|h(\beta) - \mu\mathrm{lgcd}(\alpha,\beta)|$ should be replaced by $|rh(\alpha) - \nu\mathrm{lgcd}(\alpha,\beta)|$ and $|rh(\beta) - \mu\mathrm{lgcd}(\alpha,\beta)|$ where

$$r = \sum_P \min\left\{\mathrm{ord}_P(x), \mathrm{ord}_P(y)\right\}.$$

Here the sum extends to the algebraic points P of the plain curve $F(x,y) = 0$ with $x(P) = y(P) = 0$. (We have $r = 1$ if and only if $(0,0)$ is a non-singular point.) We plan to pursue this in a forthcoming article.

3.2 Absolute Siegel lemma

In the sequel, we need the *Absolute Siegel's lemma*, due to Roy and Thunder [20]. The following is an adaptation of Theorem 2.2 from [20].

Theorem 3.2.1 *Let $L_1, ..., L_\mu \in \overline{\mathbb{Q}}[x_1, ..., x_\nu]$ be μ linear forms. Then, if $\nu > \mu$, there exists a nonzero $\underline{c} \in \overline{\mathbb{Q}}^\nu$ such that*

$$L_1(\underline{c}) = ... = L_\mu(\underline{c}) = 0 \tag{3.7}$$

and

$$h(\underline{c}) \leqslant (\nu - \mu)^{-1}(h(L_1) + ... + h(L_\mu)) + (\nu - \mu)\log 2.$$

Proof Let V be the subspace of $\overline{\mathbb{Q}}^\nu$ of dimension $m = \nu - \mu$ defined by (3.7). According to Section 1 of [20], we can define the height of V as follows : if $\dim V = 1$, then $h(V)$ is the height of any non zero element of V. If $\dim V = m > 1$, then $h(V)$ is the height of the d-th exterior power $\bigwedge^m(V)$ which is a one-dimensional space. According to Theorem 1.1 of [20] we have $h(V) = h(V^\perp)$ and lemma 4.7 implies that $h(V^\perp) \leqslant h(L_1) + \cdots + h(L_\mu)$. Theorem 2.2 from [20] then implies that V contains a non-zero vector $\underline{c}$ satisfying

$$h(\underline{c}) \leqslant d^{-1}h(V) + m\log 2 \leqslant m^{-1}(h(L_1) + \cdots + h(L_\mu)) + m\log 2. \qquad \square$$

3.3 Proof of Theorem 3.1.1

Let K be a number field containing all the algebraic numbers of the problem and let $\mathcal{M}_K$ be the set of the places of K. From Section 2.2.1, there exists a series $\mathcal{Y}(X) = \sum_{k\geqslant 1} a_k X^k \in K[[X]]$ associated to F, and real numbers $\{A_v,\ v \in \mathcal{M}_K\}$ such that

$$\sum_{v\in\mathcal{M}_K} \frac{d_v}{d}\log A_v = 2h(F) + 11\log(2\mu + 2\nu) \tag{3.8}$$

and

$$|a_k|_v \leqslant A_v^k, \tag{3.9}$$

for every $v \in \mathcal{M}_K$ and $k \geqslant 1$.

3.3.1 An auxiliary polynomial

First, with Absolute Siegel's lemma (Theorem 3.2.1), we construct an auxiliary polynomial with controlled height which order of vanishing at the point $(0,0)$ is high.

Proposition 3.3.1 *Let N be a positive integer, and let δ be a real number satisfying $0 < \delta \leq 1$. Then there exists a non-zero polynomial $G(X,Y) \in \overline{\mathbb{Q}}$ with $\deg_X G \leqslant N$ and $\deg_Y G \leqslant \nu - 1$ satisfying the following properties :*

$$\mathrm{ord}_0 G(X, \mathcal{Y}(X)) \geqslant \nu N(1-\delta), \tag{3.10}$$

$$h(G) \leqslant 2\nu N\delta^{-1}h(F) + 15\nu N\delta^{-1}\log(2\mu + 2\nu). \tag{3.11}$$

Here $\mathcal{Y}(X)$ is the Puiseux expansion defined in Section 2.2.1.

Proof Write

$$G(X,Y) = \sum_{\substack{0\leq i\leq N\\ 0\leq j\leq n-1}} G_{ij}X^iY^j$$

with yet unknown algebraic coefficients G_{ij}. Denote by $\underline{c}$ the $\nu(N+1)$-dimensional vector of these coefficients, ordered somehow. Then

$$G(X, \mathcal{Y}(X)) = \sum_{r=0}^{\infty} L_r(\underline{c})X^r,$$

where

$$L_r = G_{r0} + \sum_{i=0}^{\min\{N,r\}} \sum_{j=1}^{\nu-1} b_{r-i}^{(j)} G_{ij},$$

the algebraic numbers $b_{r-i}^{(j)}$ being those defined in Proposition 2.2.3. We view L_r as linear forms in variables G_{ij} with algebraic coefficients. Condition (3.10) can be stated as

$$L_r(\underline{c}) = 0 \qquad (0 \leqslant r \leqslant \nu N(1-\delta)). \tag{3.12}$$

We wish to apply Theorem 3.2.1 to this system of linear equations in $\underline{c}$. Using Proposition 2.2.3, we find that for any finite valuation v, we have

$$|L_r|_v = \max_{i,j}\{1, |b_{r-i}^{(j)}|_v\} \leqslant A_v^r \leqslant A_v^{\nu N},$$

and for any infinite valuation v, we have

$$|L_r|_v = \max_{i,j}\{1, |b_{r-i}^{(j)}|_v\} \leqslant \max_{i,j} \binom{r-i+j-1}{r-i} A_v^r \leqslant 2^{2\nu N} A_v^{\nu N},$$

so that by (3.8) we have

$$h(L_r) \leqslant 2\nu N h(F) + 13\nu N \log(2\mu + 2\nu),$$

for all $0 \leqslant r \leqslant \nu N(1-\delta) - 1$.

Applying Theorem 3.2.1, we find a non-zero solution $\underline{c}$ of (3.12) satisfying

$$h(\underline{c}) \leqslant (\nu(1+N\delta))^{-1}(h(L_1) + ... + h(L_{\lfloor \nu N(1-\delta)\rfloor})) + n(1+N\delta)\log 2.$$

This proves the proposition. □

3.3.2 v-adic convergence and partial height

Let S be the subset of $\mathcal{M}_K$ defined by

$$S = \left\{ v \in \mathcal{M}_K \ : \ |\alpha|_v \begin{array}{cc} \leqslant & (2A_v)^{-1} \quad \text{if } v \text{ is infinite,} \\ < & A_v^{-1} \quad \text{otherwise.} \end{array} \right\}$$

By (3.9), for each $v \in S$ the series $\sum a_k \alpha^k$ converges for the v-metric. We will denote by $\mathcal{Y}_v(\alpha)$ its sum and set

$$T = \{v \in S, \ \mathcal{Y}_v(\alpha) = \beta\}.$$

Lemma 3.3.2 *We have*

$$h_S(\alpha) \leqslant h(\alpha) \leqslant h_S(\alpha) + 2h(F) + 12\log(2\mu + 2\nu).$$

Proof By inclusion the first inequality is clear. For the second one, an explicit calculus of $h_{\mathcal{M}_k \setminus S}(\alpha)$ gives us

$$\begin{aligned} h_{\mathcal{M}_K \setminus S}(\alpha) &= -\sum_{v \in \mathcal{M}_K \setminus S} \frac{d_v}{d} \log \min\{1, |\alpha|_v\} \\ &\leqslant \sum_{v \in \mathcal{M}_K^\infty \setminus S} \frac{d_v}{d} \log A_v + \sum_{v \in \mathcal{M}_K^0 \setminus S} \frac{d_v}{d} \log 2A_v \\ &\leqslant \sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log A_v + \log 2 \\ &\leqslant 2h(F) + 12\log(2\mu + 2\nu). \qquad \square \end{aligned}$$

3.3.3 A bound for $|h(\alpha) - \nu h_T(\alpha)|$

Proposition 3.3.3 *Either*

$$h(\alpha) \leqslant 27\mu\nu^3\varepsilon^{-2}h(F) + 171\mu\nu^3\varepsilon^{-2}\log(2\mu + 2\nu), \tag{3.13}$$

or

$$\nu h_T(\alpha) \leqslant (1+\varepsilon)h(\alpha) + 32\nu\varepsilon^{-1}h(F) + 230\nu\varepsilon^{-1}\log(2\mu + 2\nu). \tag{3.14}$$

Proof Let N be a positive integer satisfying

$$N \geqslant \max\{\mu, \nu\}$$

and let δ satisfy $0 < \delta \leqslant 1$, both N and δ to be specified latter. Let $G(X, Y)$ be the auxiliary polynomial constructed in Proposition 3.3.1. By extending the field K we may assume that it contains the coefficients of G. The rest of the proof split into two cases.

The case $G(\alpha, \beta) = 0$**.** Since $F(\alpha, \beta) = 0$ as well, the polynomials $F(\alpha, Y)$ and $G(\alpha, Y)$ have a common root β. Then α is a root of the resultant $R(X) = \mathrm{Res}_Y(F(X, Y), G(X, Y))$ and by Propositions 2.1.3 and 2.1.6 we have

$$\begin{aligned} h(\alpha) \leqslant & h(R) + \mu(\nu - 1) + \nu N \\ \leqslant & \nu(h(F) + h(G)) + 2(\mu(\nu - 1) + \nu N) + (2\nu - 1)\log(2\nu - 1) \\ \leqslant & \nu(1 + 2\nu N\delta^{-1})h(F) + 13\nu^2 N\delta^{-1}\log(2\mu + 2\nu) + 4\nu N + 2\nu\log(2\nu) \qquad (3.15) \\ \leqslant & 3\nu^2 N\delta^{-1}h(F) + 19\nu^2 N\delta^{-1}\log(2\mu + 2\nu). \end{aligned}$$

(We used the condition $N \geqslant \mu$ for (3.15)).

The case $G(\alpha, \beta) = \gamma \neq 0$**.** In this case Proposition 2.1.7 implies that

$$\begin{aligned} h(\gamma) \leqslant & h(G) + Nh(\alpha) + (\nu - 1)h(\beta) + \log((N + 1)\nu) \\ \leqslant & (N + (\nu - 1)\mu)h(\alpha) + 3\nu N\delta^{-1}h(F) + 19\nu N\delta^{-1}\log(2\mu + 2\nu). \end{aligned} \tag{3.16}$$

On the other side, write

$$\mathcal{Z}(X) = G(X, \mathcal{Y}(X)) = \sum_{k \geqslant \nu N(1-\delta)} b_k X^k.$$

By Proposition 2.2.3, for any finite place v of K we have

$$|b_k|_v \leqslant |G|_v A_v^k,$$

for all $k \geqslant \nu N(1 - \delta)$. Moreover, if v is a place of S, we have $A_v|\alpha|_v < 1$ so that the series $\sum b_k\alpha^k$ converges in v-metric and its sum $\mathcal{Z}_v(\alpha)$ satisfies

$$|\mathcal{Z}_v(\alpha)|_v \leqslant |G|_v(A_v|\alpha|_v)^{\nu N(1-\delta)}$$

and for any infinite place v, while $N \geqslant \nu$ we have

$$|b_k|_v \leqslant |G|_v \sum_{i=0}^{N} \sum_{j=1}^{\nu-1} |b_{k-i}^{(j)}|_v \leqslant \binom{\nu+k}{\nu-1} |G|_v A_v^k$$

for all $k \geqslant \nu N(1-\delta)$. A short computation shows that for any positive integers ν and $k \geqslant \nu$ we have $\binom{\nu+k}{\nu-1} \leqslant (6k)^\nu$.

By the definition of the set S, for any infinite $v \in S$ we have $A_v|\alpha|_v \leqslant 1/2$. Hence the series $\sum b_k \alpha^k$ converges in the v-metric and its sum $\mathcal{Z}_v(\alpha)$ satisfies

$$\begin{aligned}|\mathcal{Z}_v(\alpha)|_v &\leqslant \sum_{k \geqslant \nu N(1-\delta)} (6k)^\nu |G|_v (A_v|\alpha|_v)^k \leqslant 6^\nu |G|_v (A_v|\alpha|_v)^{\nu N(1-\delta)} \sum_{k \geqslant 0} (k+\nu N)^\nu 2^{-k} \\ &\leqslant 4(24\nu^2 N)^\nu |G|_v (A_v|\alpha|_v)^{\nu N(1-\delta)}.\end{aligned}$$

Furthermore, for v in the set T defined in Section 3.3.2, we have $\mathcal{Z}_v(\alpha) = G(\alpha, \beta) = \gamma$. Then

$$\begin{aligned}h(\gamma) \geqslant h_T(\gamma) \geqslant& \nu N(1-\delta)(h_T(\alpha) - 2h(F)) - h(G) \\ &- 11\nu N(1-\delta)\log(2\mu + 2\nu) - \log(4(24\nu^2 N)^\nu) \\ \geqslant& \nu N(1-\delta) h_T(\alpha) - 4\nu N \delta^{-1} h(F) - 32\nu N \delta^{-1} \log(2\mu + 2\nu).\end{aligned}$$

Combining this with (3.16), we get

$$\nu h_T(\alpha) \leqslant \frac{1}{1-\delta}\left(1 + \frac{\mu(\nu-1)}{N}\right) h(\alpha) + \frac{7\nu}{\delta(1-\delta)} h(F) + \frac{51\nu}{\delta(1-\delta)} \log(2\mu + 2\nu).$$

We can now choose N and δ in order to get the expected bounds. First we choose $\delta = \varepsilon/3$ so that $\delta < 1/3$ and $1 - \delta \geqslant 2/3$. Secondly, to have $\frac{1}{1-\delta}\left(1 + \frac{\mu(\nu-1)}{N}\right) \leqslant (1+\varepsilon)$, we must choose $N \geqslant \frac{\mu(\nu-1)}{\delta(2-3\delta)}$ so that $\nu/(N(1-\delta) \leqslant 2\delta < 1$. Then, if $G(\alpha, \beta) \neq 0$, we have

$$\nu h_T(\alpha) \leqslant (1+3\delta) h(\alpha) + 21\nu(2\delta)^{-1} h(F) + 153\nu(2\delta)^{-1} \log(2\mu + 2\nu).$$

On the other hand, if $G(\alpha, \beta) = 0$, choosing $N \leqslant \mu\nu/\delta$ gives us

$$h(\alpha) \leqslant 27\mu\nu^3\varepsilon^{-2} h(F) + 171\mu\nu^3\varepsilon^{-2} \log(2\mu + 2\nu).$$

Note that an integer satisfying the bounds for N is $N = \lfloor \mu\nu/\delta \rfloor$ and that it gives the announced bound for $\nu h_T(\alpha)$. □

Proposition 3.3.4 *Either* (3.2) *holds or we have*

$$\nu h_T(\alpha) \geqslant (1-\varepsilon) h(\alpha) - 34\nu^3\varepsilon^{-1} h(F) - 242\nu^3\varepsilon^{-1} \log(2\mu + 2\nu). \tag{3.17}$$

Proof Let $\rho(X)$ be the resultant $\mathrm{Res}_Y(F(X,Y),\partial_Y F(X,Y))$. If $\rho(\alpha) = 0$, then by Propositions 2.1.3 et 2.1.6, we have $h(\alpha) \leqslant \nu(h(F) + h(\partial_Y F)) + 2\mu\nu\log 2$. But $h(\partial_Y F) \leqslant h(F) + \log\nu$, so that

$$h(\alpha) \leqslant 2\nu h(F) + \nu\log\nu$$

which is better than (3.2). We can now assume that $\rho(\alpha)$ is nonzero and we can enlarge the field K so tha the polynomial $F(\alpha, Y)$ splits into linear factors. Let us put

$$F(\alpha,Y) = \phi\prod_{i=1}^{\nu}(Y-\beta_i).$$

We can now apply Proposition 3.3.3 with ε/ν instead of ε : let $\beta = \beta_1$ and for i from 1 to n, we put $T_i = \{v \in S,\ \mathcal{Y}_v(\alpha) = \beta_i\}$. The set T_i form a partition of S so that

$$h_S(\alpha) = h_{T_1}(\alpha) + \cdots + h_{T_\nu}(\alpha).$$

If (3.2) is not true then Proposition 3.3.3 gives

$$\nu h_{T_i}(\alpha) \leqslant \left(1+\frac{\varepsilon}{\nu}\right)h(\alpha) + 32\nu^2\varepsilon^{-1}h(F) + 230\nu^2\varepsilon^{-1}\log(2\mu+2\nu)$$

so that by Lemma 3.3.2 we have

$$\begin{aligned} h_T(\alpha) =& h_S(\alpha) - h_{T_2}(\alpha) - \cdots - h_{T_\nu}(\alpha) \\ \geqslant& \frac{1-\varepsilon}{\nu}h(\alpha) - 34\nu^2\varepsilon^{-1}h(F) - 242\nu^2\varepsilon^{-1}\log(2\mu+2\nu) \end{aligned}$$

which gives us the wanted bound. □

Combining Propositions 3.3.3 and 3.3.4 we get the following propotion :

Proposition 3.3.5 *Either* (3.2) *holds or we have*

$$|h(\alpha) - \nu h_T(\alpha)| \leqslant \varepsilon h(\alpha) + 34\nu^3\varepsilon^{-1}h(F) + 242\nu^3\varepsilon^{-1}\log(2\mu+2\nu). \tag{3.18}$$

3.3.4 A bound for $|\mathrm{lgcd}(\alpha,\beta) - h_T(\alpha)|$

In this subsection, we prove the following proposition :

Proposition 3.3.6 *Let F be a polynomial with algebraic coefficients, and let K, μ, and ν be as in Theorem 3.1.1. Let also be S and T the subsets of $\mathcal{M}_K$ defined at the beginning of Subsection 3.3.2. Then*

$$|\mathrm{lgcd}(\alpha,\beta) - h_T(\alpha)| \leqslant 7h(F) + 33\nu\log(2\mu+2\nu).$$

Proof The **lower bound** is relatively easy. Recall first that for every place v in S, we have

$$|\alpha|_v \begin{cases} \leqslant & (2A_v)^{-1} \quad \text{if } v \text{ is infinite,} \\ < & A_v^{-1} \quad \text{if } v \text{ is finite} \end{cases}$$

and the series $\sum a_k \alpha^k$ converges for the v-metric. Hence, if v is infinite, we have

$$|\mathcal{Y}_v(\alpha)|_v \leqslant |\alpha|_v \sum_{k\geqslant 1} |a_k|_v |\alpha|_v^{k-1} \leqslant |\alpha|_v \sum_{k\geqslant 1} A_v^k |\alpha|_v^{k-1} \leqslant |\alpha|_v A_v \sum_{k\geqslant 1} 2^{1-k} \leqslant 2A_v |\alpha|_v, \quad (3.19)$$

and

$$|\mathcal{Y}_v(\alpha)|_v = |\alpha|_v \left| \sum_{k\geqslant 1} a_k \alpha^{k-1} \right|_v \leqslant |\alpha|_v \max_{k\geqslant 1} |a_k|_v |\alpha|_v^{k-1} \leqslant A_v |\alpha|_v \quad (3.20)$$

if v is finite. In particular, for any place v in T, we have

$$|\beta|_v \leqslant \begin{cases} 2A_v |\alpha|_v & \text{if } v \text{ is infinite,} \\ A_v |\alpha|_v & \text{otherwise.} \end{cases}$$

Then for any v in T, we have

$$h_v(\beta) \geqslant \begin{cases} h_v(\alpha) - \frac{d_v}{d} \log 2A_v & \text{if } v \text{ is infinite,} \\ h_v(\alpha) - \frac{d_v}{d} \log A_v & \text{otherwise.} \end{cases}$$

Let us put $\Delta = \operatorname{lgcd}(\alpha, \beta)$. We have

$$\begin{aligned} \Delta &= \sum_{v\in\mathcal{M}_K} \min\{h_v(\alpha), h_v(\beta)\} \geqslant \sum_{v\in T} \min\{h_v(\alpha), h_v(\beta)\} \\ &\geqslant \sum_{v\in T} h_v(\alpha) - \sum_{v\in\mathcal{M}_K^0} \frac{d_v}{d} \log(A_v) - \sum_{v\in\mathcal{M}_K^\infty} \frac{d_v}{d} \log(2A_v). \end{aligned}$$

This gives us a lower bound for $\Delta - h_T(\alpha)$:

$$\Delta - h_T(\alpha) \geqslant -2h(F) - 12\log(2\mu + 2\nu). \quad (3.21)$$

The upper bound is more advanced. It relies in the following statement.

Proposition 3.3.7 *In the set-up of Proposition 3.3.6, there is a partition $S = T \amalg U \amalg V$ such that*

$$\begin{aligned} h_U(\alpha) &\leqslant 4h(F) + 12\log(2\mu + 2\nu) + \log(\nu 2^{\nu+4}) \\ h_V(\beta) &\leqslant h(F) + \log(\nu 2^{\nu+3}) \end{aligned}$$

To prove this proposition, we need the following lemma.

Lemma 3.3.8 *Let K be a field with a valuation v and let $f(Y) \in K[Y]$ be a polynomial of degree ν.*

1. *For any root β of f, we have*

$$|\beta|_v \geqslant \begin{cases} \dfrac{|f(0)|_v}{|f|_v} & \text{if } v \text{ is finite,} \\ \dfrac{|f(0)|_v}{\nu|f|_v} & \text{otherwise.} \end{cases}$$

2. *Let β and γ be two distinct roots of f. Then*

$$\max\{|\beta|_v, |\gamma|_v\} \geqslant c_v(\nu)\frac{|f'(0)|_v}{|f|_v}$$

where $c_v(\nu) = \dfrac{1}{(\nu+1)2^{\nu+2}}$ if v is infinite, and $c_v(\nu) = 1$ if v is finite.

Proof

1. Let β be a root of $f(Y) = \sum_{i=0}^{\nu} b_i Y^i$ and let v be a place of K. If $|\beta|_v \geqslant 1$, the result is clear because $f(0)$ is one of the coefficients of f. Let us assume that $|\beta|_v < 1$. Since β is a root of f, we get

$$|f(0)|_v = |b_0|_v = \left|\sum_{i=1}^{\nu} b_i\beta^i\right|_v,$$

so that

$$|f(0)|_v \leqslant \begin{cases} |f|_v|\beta|_v & \text{if } v \text{ is finite,} \\ \nu|f|_v|\beta|_v & \text{otherwise.} \end{cases}$$

2. Let β and γ be two distinct roots of f. If $|\beta|_v \geqslant 1$ this is done. Let us assume that $|\beta|_v < 1$ and let $g(X) = \dfrac{f(X+\beta)}{X}$ which roots are $\beta - \beta_i$ for $i = 2 \dots \nu$. As in Proposition 2.1.7, we have

$$|g|_v \leqslant \begin{cases} |f|_v & \text{if } v \text{ is finite,} \\ (\nu+1)2^{\nu}|f|_v & \text{otherwise} \end{cases}$$

Moreover, by the definition of g we have

$$g(0) = f'(0) + \sum_{k=1}^{\nu-1} \frac{\beta^k}{k!} f^{(k+1)}(0) = f'(0) + \sum_{k=1}^{\nu-1} (k+1)b_k\beta^k, \tag{3.22}$$

Let us assume that v is infinite. By (3.22), we get

$$|f'(0)|_v \leqslant |g(0)|_v + \sum_{k=1}^{\nu-1} |(k+1)b_k\beta^k|_v \leqslant |g(0)|_v + \nu^2|f|_v|\beta|_v,$$

so that $|g(0)|_v \geqslant |f'(0)|_v/2$ as soon as $|\beta|_v \leqslant |f'(0)|_v/(2\nu^2|f|_v)$. Applying the first part of the lemma to polynomial g we get

$$|\gamma-\beta|_v \geqslant \frac{|g(0)|_v}{\nu|g|_v} \geqslant \frac{1}{(\nu+1)2^{\nu+1}}\frac{|f'(0)|_v}{|f|_v}$$

as soon as $|\beta|_v \leqslant |f'(0)|_v/(2\nu^2|f|_v)$ and

$$|\gamma|_v \geqslant \frac{1}{(\nu+1)2^{\nu+2}}\frac{|f'(0)|_v}{|f|_v}$$

if $|\beta|_v \leqslant \dfrac{1}{(\nu+1)2^{\nu+2}}\dfrac{|f'(0)|_v}{|f|_v}$.
Similarly, is v is finite, we have

$$|(k+1)\beta^k b_k|_v = |\beta|_v^k|b_k|_v \leqslant |\beta|_v|b_k|_v < |f'(0)|_v\frac{|b_k|_v}{|f|_v} \leqslant |f'(0)|_v,$$

when $|\beta|_v < |f'(0)|_v/|f|_v$. Then $|g(0)|_v = |f'(0)|_v$ and if we apply the first part of the lemma to g once again, we get

$$|\gamma-\beta|_v \geqslant \frac{|g(0)|_v}{|g|_v} \geqslant \frac{|f'(0)|_v}{|f|_v}$$

such that $|\gamma|_v \geqslant |f'(0)|_v/|f|_v$ as soon as $|\beta|_v \leqslant |f'(0)|_v/|f|_v$. □

Proof of Proposition 3.3.7 . We first define U as the union of two subsets U_1 and U_2 of $S\backslash T$. Let $f(Y) = F(\alpha, Y)$ and $L = \partial_Y F(0,0)$ so that $f'(0) = L + a_{11}\alpha + \cdots + a_{m1}\alpha^m$ and put

$$U_1 = \left\{ v \in S\backslash T \ / \ \begin{array}{ll} |f'(0)|_v \neq |L|_v & \text{if } v \text{ is finite,} \\ |f'(0)|_v \leqslant \frac{|L|_v}{2} & \text{otherwise.} \end{array} \right\}$$

Then for any infinite place v in U_1, we have

$$|L|_v = \left| f'(0) - \sum_{i=1}^{m} a_{i1}\alpha^i \right|_v \leqslant \frac{|L|_v}{2} + m|\alpha|_v|F|_v,$$

since $|\alpha|_v < 1$. Hence $|L|_v \leqslant 2\mu|\alpha|_v|F|_v$ and $|\alpha|_v \geqslant \frac{|L|_v}{2\mu|F|_v}$.

Similarly, for any finite place v in U_1, we have

$$|f'(0)|_v \leqslant \max_i\{|L|_v, |a_{i1}\alpha^i|_v\},$$

and this inequality is an equality if the maximum is strict. Since $|f'(0)|_v \neq |L|_v$, for some $i \in \{1,\ldots,m\}$, we have $|a_{i1}\alpha^i|_v \geqslant |L|_v$ and then $|\alpha|_v \geqslant \frac{|L|_v}{|F|_v}$. Taking the log and summing up over all the places of U_1 we get

$$h_{U_1}(\alpha) \leqslant h(F) + \log(2\mu). \tag{3.23}$$

Furthermore, for any place v in $S\backslash(T\cup U_1)$ we have $|f'(0)|_v = |L|_v$ and $|f|_v \leqslant |F|_v$ if v is finite and $|f'(0)|_v > |L|_v/2$ and $|f|_v \leqslant m|F|_v$ otherwise. We now keep the places of $S\backslash T$ which satisfy $|\beta|_v \leqslant |Y_v(\alpha)|_v$ to build U_2 and we note V the last ones.

By Lemma 3.3.8, for any place v in U_2 we have $|Y_v(\alpha)|_v \geqslant c_v(\nu)\dfrac{|L|_v}{|F|_v}$ and inequalities (3.19) and (3.20) give us

$$|\alpha|_v \geqslant \begin{cases} \dfrac{1}{(\nu+1)2^{\nu+3}}\dfrac{|L|_v}{A_v|F|_v} & \text{if } v \text{ is infinite,} \\ \dfrac{|L|_v}{A_v|F|_v} & \text{otherwise.} \end{cases}$$

Taking the log and summing up over all the places of U_2 we get

$$h_{U_2}(\alpha) \leqslant h(F) + \sum_{v\in U_2}\frac{d_v}{d}\log(A_v) + \log((\nu+1)2^{\nu+3}) \leqslant 3h(F) + 15\nu\log(2\mu+2\nu).$$

Similarly, for any place v of V, we have $|\beta|_v \geqslant c_v(\nu)\dfrac{|L|_v}{|F|_v}$ and

$$h_V(\beta) \leqslant h(F) + \log(\nu 2^{\nu+3}) \leqslant h(F) + 5\nu\log(2\mu+2\nu).$$

Writing if $U = U_1 \amalg U_2$ we get

$$h_U(\alpha) = h_{U_1}(\alpha) + h_{U_2}(\alpha) \leqslant 4h(F) + 16\nu\log(2\mu+2\nu),$$

which proves Proposition 3.3.7. □

Now we are ready to complete the proof of Proposition 3.3.6. Using the partition $S = T \amalg U \amalg V$, we get :

$$\begin{aligned}\Delta =& \sum_{v\in T}\min\{h_v(\alpha),h_v(\beta)\} + \sum_{v\in U}\min\{h_v(\alpha),h_v(\beta)\} \\ &+ \sum_{v\in V}\min\{h_v(\alpha),h_v(\beta)\} + \sum_{v\in\mathcal{M}_K\backslash S}\min\{h_v(\alpha),h_v(\beta)\} \\ \leqslant& h_T(\alpha) + h_U(\alpha) + h_V(\beta) + h_{\mathcal{M}_K\backslash S}(\alpha) \\ \leqslant& h_T(\alpha) + 7h(F) + 33\nu\log(2\mu+2\nu),\end{aligned}$$

Recall that $h_{\mathcal{M}_K\backslash S}(\alpha)$ was estimated in lemma 3.3.2. Combined with (3.21) we get

$$|\Delta - h_T(\alpha)| \leqslant 7h(F) + 33\nu\log(2\mu+2\nu).$$

This proves Proposition 3.3.6. □

Proof of Theorem 3.1.1. Combining Propositions 3.3.5 and 3.3.6, we obtain that if (3.2) is not true, then

$$\begin{aligned}|h(\alpha) - \nu\Delta| \leqslant& |h(\alpha) - \nu h_T(\alpha)| + \nu|h_T(\alpha) - \Delta| \\ \leqslant& \varepsilon h(\alpha) + 41\nu^3\varepsilon^{-1}h(F) + 275\nu^3\varepsilon^{-1}\log(2\mu+2\nu).\end{aligned}$$

Which proves Theorem 3.1.1. □

3.4 Quasi-equivalence of heights and symmetrization of Theorem 3.1.1

3.4.1 Proof of Corollary 3.1.2

Let F be as above. We need a "small" solution (α_0, β_0) of $F(x, y) = 0$: let $\rho_Y(X)$ and $\rho_X(Y)$ be respectively the resultants $\mathrm{Res}_Y(F, \partial_Y F)$ and $\mathrm{Res}_X(F, \partial_X F)$. An algebraic number γ will be called *bad* either if it is a root of $\rho_Y(X)$ or if $\rho_X(Y)$ and $F(\gamma, Y)$ have a common root. There are at most $\mu(2\mu\nu + \nu + 1)$ bad algebraic numbers so that we can choose a good rational integer α_0 with

$$h(\alpha_0) \leqslant \log(\mu(2\mu\nu + \nu + 1)/2 + 1) \leqslant 2\log(2\mu + 2\nu). \tag{3.24}$$

Let $\beta_0 \in \overline{\mathbb{Q}}$ be a root of $F(\alpha_0, Y)$. Then by Proposition 2.1.7, we have

$$h(\beta_0) \leqslant h(F) + \mu h(\alpha_0) + \nu + \log(\mu + 1). \tag{3.25}$$

Now put $F_1(X, Y) = F(X + \alpha_0, Y + \beta_0)$. By Proposition 2.1.7, we have

$$\begin{aligned} h(F_1) \leqslant & h(F) + \mu h(\alpha_0) + \nu h(\beta_0) + \mu + \nu + \log(\mu + 1) + \log(\nu + 1) \\ \leqslant & 2\nu h(F) + 9\mu\nu^2 \log(2\mu + 2\nu). \end{aligned} \tag{3.26}$$

Now, let $(\alpha, \beta) \in \overline{\mathbb{Q}}^2$ be a solution of the equation $F(x, y) = 0$. The polynomial F_1 vanishes in $(\alpha - \alpha_0, \beta - \beta_0)$ and satisfies the hypotheses of Theorem 3.1.1 with respect both X and Y. Then, either one of the two following conditions is satisfied

$$\begin{aligned} h(\alpha - \alpha_0) \leqslant & 27\mu\nu^5\varepsilon^{-2} h(F_1) + 171\mu\nu^5\varepsilon^{-2}\log(2\mu + 2\nu) \\ \leqslant & 54\mu\nu^6\varepsilon^{-2} h(F) + 414\mu^2\nu^7\varepsilon^{-2}\log(2\mu + 2\nu), \end{aligned} \tag{3.27}$$

$$\begin{aligned} h(\beta - \beta_0) \leqslant & 27\mu^5\nu\varepsilon^{-2} h(F_1) + 171\mu^5\nu\varepsilon^{-2}\log(2\mu + 2\nu) \\ \leqslant & 54\mu^5\nu^2\varepsilon^{-2} h(F) + 414\mu^6\nu^3\varepsilon^{-2}\log(2\mu + 2\nu), \end{aligned} \tag{3.28}$$

or we have

$$\begin{cases} |h(\alpha - \alpha_0) - \nu\Delta_0| \leqslant \varepsilon h(\alpha - \alpha_0) + 41\nu^3\varepsilon^{-1} h(F_1) + 275\nu^3\varepsilon^{-1}\log(2\mu + 2\nu) \\ |h(\beta - \beta_0) - \mu\Delta_0| \leqslant \varepsilon h(\beta - \beta_0) + 41\mu^3\varepsilon^{-1} h(F_1) + 275\mu^3\varepsilon^{-1}\log(2\mu + 2\nu), \end{cases} \tag{3.29}$$

where $\Delta_0 = \mathrm{lgcd}(\alpha - \alpha_0, \beta - \beta_0)$.

But if (3.28) is true, then by (3.24), (3.25) and (3.26), we get

$$\begin{aligned} h(\beta) \leqslant & h(\beta - \beta_0) + h(\beta_0) + 1 \\ \leqslant & 55\mu^5\nu^2\varepsilon^{-2} h(F) + 418\mu^6\nu^3\varepsilon^{-2}\log(2\mu + 2\nu) \end{aligned}$$

and by Proposition 2.1.7, we have

$$\begin{aligned} h(\alpha) &\leqslant h(F) + \nu h(\beta) + \mu + \log(\nu+1) \\ &\leqslant 56\mu^5\nu^3\varepsilon^{-2}h(F) + 420\mu^6\nu^4\varepsilon^{-2}\log(2\mu+2\nu). \end{aligned}$$

We use the same arguments if (3.27) holds, in which case the resulting estimates are even slightly better. Thus if one of (3.27) and (3.28) holds, then

$$\max\{h(\alpha), h(\beta)\} \leqslant 56M^8\varepsilon^{-2}h(F) + 420M^{10}\varepsilon^{-2}\log(4M),$$

where $M = \max\{\mu, \nu\}$.

On the other hand, if (3.29) is true, then by (3.24), (3.25) and (3.26), we have

$$|h(\alpha - \alpha_0) - \nu\Delta_0| \leqslant \varepsilon h(\alpha) + 82\nu^4\varepsilon^{-1}h(F) + 647\mu\nu^5\varepsilon^{-1}\log(2\mu+2\nu)$$

and

$$|h(\beta - \beta_0) - \mu\Delta_0| \leqslant \varepsilon h(\alpha) + 82\mu^3\nu\varepsilon^{-1}h(F) + 647\mu^4\nu^2\varepsilon^{-1}\log(2\mu+2\nu).$$

Then

$$\begin{aligned} \left|\frac{h(\alpha)}{\nu} - \frac{h(\beta)}{\mu}\right| \leqslant& \left|\frac{h(\alpha)}{\nu} - \frac{h(\alpha-\alpha_0)}{\nu}\right| + \left|\frac{h(\alpha-\alpha_0)}{\nu} - \Delta_0\right| + \\ & \left|\frac{h(\beta)}{\mu} - \frac{h(\beta-\beta_0)}{\mu}\right| + \left|\frac{h(\beta-\beta_0)}{\mu} - \Delta_0\right| \\ \leqslant& 2\varepsilon h(\alpha) + 165\mu^2\nu^3\varepsilon^{-1}h(F) + 1303\mu^3\nu^4\varepsilon^{-1}\log(2\mu+2\nu). \end{aligned}$$

The result follows by taking $\varepsilon/2$ instead of ε. □

3.4.2 Proof of Theorem 3.1.3

Let (α, β) be a solution of $F(x, y) = 0$. By Theorem 3.1.2, if (3.4) is not true, then (3.5) is satisfied. Moreover, since $(0, 0)$ is a non-singular point of $\{F(x, y) = 0\}$, either $\partial_X F(0, 0)$ or $\partial_Y F(0, 0)$ is non-zero. Without lost of generality, we may assume that $\partial_Y F(0, 0) \neq 0$ and we can apply Theorem 3.1.1.

If (3.2) is true, then by Proposition 2.1.7, we have

$$h(\beta) \leqslant 28\mu^2\nu^5\varepsilon^{-2}h(F) + 173\mu^2\nu^5\varepsilon^{-2}\log(2\mu+2\nu),$$

which together with (3.2) implies (3.4). And if (3.3) holds, then Corollary 3.1.2 implies

$$\begin{aligned} \left|\frac{h(\beta)}{\mu} - \Delta\right| &\leqslant \left|\frac{h(\beta)}{\mu} - \frac{h(\alpha)}{\nu}\right| + \left|\frac{h(\alpha)}{\nu} - \Delta\right| \\ &\leqslant 2\varepsilon h(\alpha) + 371\mu^2\nu^3\varepsilon^{-1}h(F) + 2881\mu^3\nu^4\varepsilon^{-1}\log(2\mu+2\nu). \end{aligned}$$

which together with (3.3) implies (3.6) by taking $\varepsilon/(2\mu)$ instead of ε. □

Chapitre 4

Generalized Thue's equation

Let K be a number field and let L be a finite extension of K such that $[L : K] = n \geqslant 3$. We denote be $\mathcal{N}_{L/K}$ the norm $L \to K$ (we might omit L/K if there is no ambiguity). Let also $\mathcal{M}_K$ be the set of valuations of K and let S be a finite subset of $\mathcal{M}_K$ containing the infinite places. For a given polynomial $F(X, Y) \in L[X, Y]$ and for a given $A \in K^*$, we will explicitly bound the S-integral solutions (α, β) of the equation

$$\mathcal{N}_{L/K}(F(x, y)) = A. \tag{4.1}$$

Before giving the main result of this chapter, we need to exclude some "pathological" cases. Indeed, if (F, A) is such that $F(X, Y) = \alpha + (X - Y)H(X, Y)$ for some $\alpha \in L$ with $\mathcal{N}(\alpha) = A$ and for some polynomial $H \in L[X, Y]$, the line $\{x = y\}$ is solution of our problem and we can not expect bounding the solutions. In the same way, if we have $F(X, Y) = X - \sqrt{2}Y + (X^2 - 2Y^2 - 1)H(X, Y)$ for some polynomial $H \in \mathbb{Q}(\sqrt{2})[X, Y]$, any rational solution of $x^2 - 2y^2 = 1$ is a solution of $\mathcal{N}(F(x, y)) = 1$ and once again, we cannot expect getting bounds for the solutions of our problem. Then, in the first section, we give the two "bad" types of couples (F, A) which generalize the counter-examples given above.

In the second section of this chapter, we fix a solution $(\alpha, \beta) \in \mathcal{O}_S^* \times \mathcal{O}_S$ of our equation and an absolutely irreducible factor $G(X, Y)$ of $\mathcal{N}(F(X, Y)) - A$ associated to (α, β). Then we consider a special subgroup of the multiplicative group of non-zero rational functions on the curve defined by G. Depending on the rank $\rho \leqslant n - 1$ of this subgroup, we treat our problem by different methods. The cases $\rho < 2$ is treated in Section 4.3 by elementary methods while the case $\rho \geqslant 2$ is treated in the final sections of this chapter, using Baker's method. We first construct a special power series $\mathcal{Z}(X)$ from the Puiseux' series associated to G and in the last section, we use versions of Baker's inequality established by K. Yu [33] and E. M. Matveev [19] to obtain an inequality

$$h(\alpha) = O(\log(h(\alpha) + 1))$$

where the implicit constant explicitly depends on F, S, K and L.

4.1 Pathological cases and main theorem

Case 1 A couple (F, A) will be called a bad couple of **type I** if there exists a polynomial $G(X, Y) \in K[X, Y]$ and $\gamma \in L$ such that $\mathcal{N}_{L/K}(\gamma) = A$ and $G(X, Y)$ divides $F(X, Y) - \gamma$.

Case 2 A couple (F, A) will be called a bad couple of **type II** if there exists
- a subfield L_0 of L over K such that $[L_0 : K] = 2$
- polynomials $\phi(X, Y) \in L_0[X, Y]$ and $G(X, Y) \in K[X, Y]$
- a couple $(\gamma, \delta) \in L^* \times K^*$

such that

1. $\mathcal{N}_{L_0/K}(\phi) \equiv \delta \mod G$,
2. $F \equiv \gamma\phi \mod G$,
3. $\delta^{n/2}\mathcal{N}_{L/K}(\gamma) = A$.

Then we have the following theorem

Theorem 4.1.1 *Let $(F, A) \in L[X, Y] \times K^*$ be a couple not of bad type I or II. Then for any the solutions $(\alpha, \beta) \in \mathcal{O}_S^* \times \mathcal{O}_S$ of*

$$\mathcal{N}_{L/K}(F(x, y)) = A,$$

the heights $h(\alpha)$ and $h(\beta)$ are effectively bounded in terms of F, K, L and S.

The effective bounds of this theorem can be made explicit. For this, see Remark 4.5.6 at the end of this chapter.

4.2 First steps

Let $(\alpha, \beta) \in \mathcal{O}_S^* \times \mathcal{O}_S$ be a solution of (4.1) and let $v_0 \in S$ such that

$$|\alpha|_{v_0} = \max_{v \in S}\{|\alpha|_v\}.$$

There is an irreducible polynomial $G(X, Y) \in K[X, Y]$ dividing $\mathcal{N}(F(X, Y)) - A$ and such that $G(\alpha, \beta) = 0$. By proposition 2.1.4, we have

$$h_{\mathbb{A}}(\mathcal{N}F - A) \leqslant h_{\mathbb{A}}(\mathcal{N}F) + \log 2.$$

Moreover, by proposition 2.1.2, we have

$$h_{\mathbb{A}}(\mathcal{N}F) \leqslant n(h_{\mathbb{A}}(F) + N + 2)$$

and

$$h_{\mathbb{P}}(G) \leqslant h_{\mathbb{P}}(\mathcal{N}F - A) + nN.$$

Then, since the affine height is always greater than (or equal to) the projective height, the projective height of G is bounded in terms of $h_{\mathbb{A}}(F)$ and n in the following way :

$$h_{\mathbb{P}}(G) \leqslant nh_{\mathbb{A}}(F) + 5nN. \tag{4.2}$$

4.2.1 Puiseux series for G

Let us apply results of Section 2.2.2 to the polynomial G defined above. There are integers $e_1, \dots, e_\nu$ and Puiseux' series $\mathcal{Y}_i(X) = \sum_{k \geqslant -k_i} a_{ik} X^{-k/e_i}$ with coefficients in a finite extension $\widetilde{K}$ of K and a polynomial $\phi(X) \in K[X]$ such that

$$G(X,Y) = \phi(X) \prod_{i=1}^{\nu} (Y - \mathcal{Y}_i(X)).$$

Put $\varepsilon = \operatorname{lcm}\{e_1, \dots, e_\nu\}$ and fix an ε-th root of α. That fixes an e_i-th root of α for any $i = 1, \dots, \nu$, which we denote by α^{1/e_i}. By Theorem 2.2.2, for any valuation $v \in \mathcal{M}_K$ there exists real numbers A_v and $A'_v \geqslant 1$ such that

$$\sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log A_v \leqslant 2nNh_{\mathbb{P}}(G) + O(n^2N^2) \leqslant 2n^2Nh_{\mathbb{A}}(F) + O(n^2N^2), \tag{4.3}$$

$$\sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log A'_v \leqslant h_{\mathbb{P}}(G) + O(1 \log(nN)) \leqslant nh_{\mathbb{A}}(F) + O(nN), \tag{4.4}$$

and for any place w of $\widetilde{K}$ over v, and for any $i \in \{1, \dots, \nu\}$, we have

$$|a_{ik}|_w \leqslant A'_v A_v^{\mu + k/e_i}, \qquad (k \geqslant -k_i). \tag{4.5}$$

If $\phi(\alpha) = 0$, by Propositions 2.1.3 and 2.1.2 we have

$$h(\alpha) \leqslant h_{\mathbb{P}}(\phi) + \deg \phi \leqslant h_{\mathbb{P}}(G) + \mu \leqslant nh_{\mathbb{A}}(F) + 6nN.$$

On the other hand, if $\phi(\alpha) \neq 0$, by Proposition 2.2.2, either we get

$$h(\alpha) \leqslant \sum_{v \in \mathcal{M}_K} \frac{d_v}{d} \log A_v \leqslant 2n^2Nh_{\mathbb{A}}(F) + O(n^2N^2)$$

or there is a series $\mathcal{Y}_{i_0} = \sum_{k \geqslant -k_{i_0}} a_k X^{-k/e_{i_0}} \in \{\mathcal{Y}_1, \dots, \mathcal{Y}_\nu\}$ such that for every $w \in \mathcal{M}_{\widetilde{K}}$ over v_0 we have $\mathcal{Y}_{i_0}^{(w)}(\alpha) = \beta$. Fix i_0 and put $\mathcal{Y} = \mathcal{Y}_{i_0}$, $k_{i_0} = k_0$ and $e = e_{i_0}$. Let us also denote by $\widetilde{L}$ the field over L containing the coefficients a_k of $\mathcal{Y}(X)$. It is well known that $[\widetilde{L} : L] \leqslant n$ so that $[\widetilde{L} : K] \leqslant dn^2$.

4.2.2 Function field

We can assume that the polynomial G defined above is not only irreducible over K but absolutely irreducible. Indeed, let $G_1(X,Y)$ be the absolutely irreducible factor of $G(X,Y)$ such that $G_1(\alpha,\beta)=0$ and assume that $G_1(X,Y)$ is not of the form $\gamma G_2(X,Y)$ with $G_2(X,Y)\in K[X,Y]$ and $\gamma\in\overline{K}^*$. Then, there exists $\sigma\in\mathrm{Gal}(\overline{K}/K)$ such that $G_1^\sigma(X,Y)$ is not proportional to $G_1(X,Y)$. Since G_1 is absolutely irreducible, the resultant $R(X)=\mathrm{Res}_Y(G_1(X,Y),G_1^\sigma(X,Y))$ is non-zero. Now, since $G_1^\sigma(\alpha,\beta)=0$ we also have $G_1^\sigma(\alpha,\beta)=0$ so that α appears as a root of $R(X)$. By Propositions 2.1.2 and 2.1.6, we get

$$h(\alpha)\leqslant 2nNh(F)+20nN^2.$$

Assume now that $G_1(X,Y)=\gamma G_2(X,Y)$ for some polynomial $G_2\in K[X,Y]$ and $\gamma\in\overline{K}^*$. Then G_2 divides G and since G is irreducible over K, we have $G_2=G$ times a constant, and G is absolutely irreducible.

Let $\mathcal{K}$ be the fraction field of the integral domain $K[X,Y]/(G(X,Y))$ and let x be the image of X by the projection $K[X,Y]\to K[X,Y]/(G(X,Y))$. Since $\deg_Y G\geqslant 1$ (otherwise, by Proposition 2.1.3, the work is done), we can assume that the function x is transcendent over K. Then, there exists a function $y\in\mathcal{K}$ such that $G(x,y)=0$ and $\mathcal{K}=K(x,y)$. Let M be the Galois closure of L over K and put $\Gamma=\mathrm{Gal}(M/K)$. Let $F(X,Y)=F_1(X,Y),\ldots,F_n(X,Y)$ conjugates of $F(X,Y)$ under Γ and put $z=z_1=F(x,y),\ldots,z_n=F_n(x,y)$. Finally, let $\mathcal{R}=<\overline{\mathbb{Q}}^*,z_1,\ldots,z_n>$ be the multiplicative group generated by the constants and the functions $z_1,...,z_n$. The quotient $\mathcal{R}/\overline{\mathbb{Q}}^*$ is a finitely generated free abelian group, and its rank ρ will give us the different approaches of our problem.

4.3 $\rho<2$

If all elements of $\mathcal{R}/\overline{\mathbb{Q}}^*$ are multiplicatively dependent, the function z is constant. This implies that

$$F(X,Y)\equiv F(\alpha,\beta)\mod G.$$

Since $\mathcal{N}(F(\alpha,\beta))=A$, the pair (F,A) is bad of type I with $\gamma=F(\alpha,\beta)$.

Assume now that $\rho=1$. Then for every $k=2,\ldots,n$ there exists co prime integers p_k, q_k and a constant λ_k such that $z^{p_k}=\lambda_k z_k^{q_k}$.

First Case. If we have $|p_kq_k|\geqslant 2$ for some k in $\{1,\ldots,n\}$, say, for $k=2$ and put $p=p_2$, $q=q_2$ and $\lambda=\lambda_2$. Then we have

$$F(\alpha,\beta)^p=\lambda F_2(\alpha,\beta)^q. \tag{4.6}$$

Lemma 4.3.1 *Let γ and γ_2 be algebraic numbers, conjugate over $\overline{\mathbb{Q}}$. If there is a constant λ and rational integers p and q, $p\neq\pm q$ such that $\gamma^p=\lambda\gamma_2^q$, then we have*

$$h(\gamma)=h(\gamma_2)\leqslant h(\lambda).$$

Proof Let K be a Galois extension of $\mathbb{Q}$ containing γ and γ_2. Let $\sigma \in \mathrm{Gal}(K/Q)$ such that $\gamma = \gamma^\sigma$ and let $m = \mathrm{ord}(\sigma)$. By hypothesis, we have $\gamma^p = \lambda\gamma^{\sigma q}$ and a quick induction shows that we have

$$\gamma^{p^m} = \lambda^\theta \gamma^{q^m}$$

where the formal exponent θ is $p^{m-1} + \sigma p^{m-2}q + \cdots + q^{m-1}$. Then $\gamma^{p^m - q^m} = \lambda^\theta$ and

$$|p^m - q^m| h(\gamma) \leqslant \frac{p^m - q^m}{p - q} h(\lambda)$$

so that the result follows. □

Applied to $\gamma = F(\alpha, \beta)$ and $\gamma_2 = F_2(\alpha, \beta)$ we get that

$$h(\gamma) \leqslant h(\lambda). \tag{4.7}$$

On the other hand, there is a rational integer $\alpha_0 \in \{0, \ldots, nN\}$ such that $G(\alpha_0, Y)$ is not zero. We have $h(\alpha_0) \leqslant \log nN$ and if $\beta_0 \in \overline{\mathbb{Q}}$ is a root of the polynomial $G(\alpha_0, Y)$, by Proposition 2.1.7 we have

$$h(\beta_0) \leqslant h_{\mathbb{P}}(G) + \mu h(\alpha_0) + \nu + \log(\mu + 1) \leqslant n h_{\mathbb{A}}(F) + O(nN \log nN).$$

Then if p and q are non negative, by (4.6) we get that $F(X, Y)^p \equiv \lambda F_2(X, Y)^q \mod G$ and applied to (α_0, β_0) we get

$$F(\alpha_0, \beta_0)^p = \lambda F_2(\alpha_0, \beta_0)^q$$

so that by Proposition 2.1.7 we get

$$h(\lambda) \leqslant (p + q) h(F(\alpha_0, \beta_0)) \leqslant (p + q)(2nN h_{\mathbb{A}}(F) + O(nN^3 \log n)). \tag{4.8}$$

Finally, let Q be a zero of z. We have $\mathrm{ord}_Q(z) \leqslant \deg z \leqslant 2nN^2$ and by (4.6) we have $p \,\mathrm{ord}_Q(z) = q \,\mathrm{ord}_Q(z)$. Then since p and q are co prime, p and q divide $\mathrm{ord}_Q z$ and

$$\max\{p, q\} \leqslant 2nN^2.$$

Combined with (4.7) and (4.8) we get

$$h(\gamma) \leqslant 2n^2 N^3 h_{\mathbb{A}}(F) + O(n^2 N^5 \log n).$$

Then, by definition of γ, α is a common root of polynomials $G(X, \beta)$ and $F(X, \beta) - \gamma$. Then it is a root of the Y-resultant of $G(X, Y)$ and $F(X, Y) - \gamma$ and by Proposition 2.1.6, we get

$$h(\alpha) \leqslant 4n^3 N^4 h_{\mathbb{A}}(F) + O(n^2 N^5 \log n).$$

(The height of the polynomial $F(X, Y) - \gamma$ is controlled by Proposition 2.1.4)

Second Case. If we have $|p_k q_k| = 1$ for all $k \in \{1, \ldots, n\}$, we can assume that $q_1 = \ldots = q_n = 1$ and that $p_k = \pm 1$ for $k \in \{1, \ldots, n\}$. Then we can assume that n is even and half of the p_k's are -1 (if not, since $z_1 \cdots z_n = A$, a non-zero power of z is constant and so is z, then the couple (F, A) is bad of type I). Recall that M is the Galois closure of L over K and $\Gamma = \mathrm{Gal}(M/K)$. Put

$$\Gamma_0 = \{\sigma \in \Gamma,\ z^\sigma = \lambda z\}$$

and let L_0 be the subfield of M fixed by Γ_0 (denoted by M^{Γ_0}). It is clear that $[L_0 : K] = [\Gamma : \Gamma_0] = 2$ and if we put $H = \{\sigma \in \Gamma,\ \sigma_{|_L} = id\}$ we have $H < \Gamma$ and $M^H = L$ so that $L_0 \subset L$. Let us now assume that $\deg F = \deg_Y F$ (we will show at the end of this paragraph that this assumption is free). We have $F_i(X, Y) = Y^N + \ldots$ for every $i = 1, \ldots, n$ and $G(X, Y) = Y^\nu + \ldots$. There is polynomials $Q(X, Y)$ and $R(X, Y)$ such that $\deg_Y R < N$ and $F = GQ + R$. Let γ be a non zero coefficient of R. We have $F/\gamma = GQ/\gamma + R/\gamma$ and for every $\sigma \in \Gamma_0$ such that $z^\sigma = \lambda z$ we have

$$(F/\gamma)^\sigma = G(Q/\gamma)^\sigma + (R/\gamma)^\sigma = G\widetilde{Q} + \lambda R/\gamma.$$

Then $(R/\gamma)^\sigma = \lambda R/\gamma$ and since one of the coefficients of R/γ is 1, we have $\lambda = 1$ and $(R/\gamma)^\sigma = R/\gamma$. This is true for every $\sigma \in \Gamma_0$ so that the polynomial $\phi = R/\gamma$ has its coefficients in L_0. Finally, for every $\tau \notin \Gamma_0$ the polynomial is constant mod G and since $F \equiv \gamma\phi \mod G$, the polynomial $\mathcal{N}_{L_0/K}(\phi) = \phi\phi^\tau$ is constant mod G. That means that the couple (F, A) is bad of type II with $\delta = \mathcal{N}_{L_0/K}(\phi(\alpha, \beta))$.

Remark 4.3.2 In this argument, we can assume that $\deg F = \deg_Y F$ without loss of generality. Indeed, write $F(X, Y) = F_N(X, Y) +$ *terms of lower degree* where $F_N(X, Y)$ is the homogeneous part of degree N of F. Then for any $\alpha \in L$ we have $F_N(X + \alpha Y, Y) = F_N(\alpha, 1)Y^N +$ *terms of lower degree*. But there is $\alpha \in \{0, \ldots, N\}$ such that $F_N(\alpha, 1)$ does not vanish, and the polynomial $\widetilde{F}(X, Y) = F(X + \alpha Y, Y)/F_N(\alpha, 1)$ satisfies

$$\widetilde{F}(X, Y) = Y^N + a_{N-1}(X)Y^{N-1} + \ldots + a_0(X). \tag{4.9}$$

Furthermore, since α is rational, if $(\widetilde{F}, A)$ is bad of type II, so is (F, A).

4.4 $\rho \geqslant 2$

Let $\mathcal{Y}(X)$ be the Puiseux' series defined at the end of Section 4.2.1. For $i = 1, \ldots, \nu$ put

$$\mathcal{Z}_i(X) = F_i(X, \mathcal{Y}(X)) = \sum_{k \geqslant -\kappa_i} b_{ik} X^{-k/e}, \qquad b_{i,-\kappa_i} \neq 0.$$

If $\rho \geqslant 2$, we can assume that the functions z_1 and z_2 are multiplicatively independent modulo $\overline{\mathbb{Q}}^*$ so that the series

$$\mathcal{Z}(X) = \mathcal{Z}_1(X)^{\kappa_2} \mathcal{Z}_2(X)^{-\kappa_1} = \sum_{k \geqslant 0} b_k X^{-k/e}, \qquad b_0 \neq 0,$$

is non constant.

Proposition 2.2.3 will now allow us to bound the coefficients of $\mathcal{Z}_1(X)$ and $\mathcal{Z}_2(X)$ and then $\mathcal{Z}(X)$. Write firts

$$\begin{aligned}\mathcal{Z}_1(X) &= \sum_{i,j} a_{ij} X^i \mathcal{Y}(X)^j \\ &= \sum_{i,j} a_{ij} X^{i+jk_0/e} \left(\sum_{k\geqslant 0} a'_k X^{-k/e} \right)^j\end{aligned}$$

where a_{ij} are the coefficients of F and $a'_k = a_{k-k_0}$ for $k = 0, 1, \ldots$ By Proposition 2.2.3, for any $j = 0, \ldots, \deg_Y F$ and for any valuation $v \in \mathcal{M}_K$, the coefficients $a_k^{'(j)}$ of $\left(\sum_{k\geqslant 0} a'_k X^{-k/e}\right)^j$ satisfy

$$\left| a_k^{'(j)} \right|_w \leqslant \begin{cases} A_v'^N A_v^{nN^2+k} & \text{if } v \text{ is finite,} \\ A_v'^N (2A_v)^{nN^2+k} & \text{otherwise,} \end{cases}$$

where $w \in \mathcal{M}_L$ divides v. Then, expending $\mathcal{Z}_1$ we get

$$|b_{1k}|_w \leqslant \begin{cases} \|F\|_w A_v'^N A_v^{3nN^2+k} \text{ if } v \text{ is finite,} \\ (k+1)^2 \|F\|_w A_v'^N (2A_v)^{3nN^2+k} \text{ otherwise,} \end{cases} \tag{4.10}$$

for any $w \in \mathcal{M}_L$ and $v \in \mathcal{M}_L$, $w|v$. Moreover, since F et F_2 are conjugate, we have the same inequalities for the coefficients b_{2k} of $\mathcal{Z}_2(X)$.

Write now

$$\mathcal{Z}(X) = \left(\sum_{k\geqslant 0} b'_{1k} X^{-k/e} \right)^{\kappa_2} \left(\sum_{k\geqslant 0} b'_{2k} X^{-k/e} \right)^{-\kappa_1}$$

where $b'_{ik} = b_{i,k-\kappa_i}$, $i = 1, 2$. Expending this series, we get that

$$b_k = b_{20}^{'-\kappa_1-1} \sum_{\ell=0}^{k} \sum_{j=0}^{\ell} (-1)^\ell \binom{\kappa_1 + \ell - 1}{\kappa_1 - 1} b'_{2,\ell-j+1} b_{1,k-\ell}^{'(\kappa_2)}.$$

where the coefficients $b_{1,k-\ell}^{'(\kappa_2)}$ are like in Proposition 2.2.3. Still by Proposition 2.2.3, we get

$$|b_{1k}^{'(\kappa_2)}|_w \leqslant \begin{cases} \|F\|_w^{2nN^2} A_v'^{2nN^3} A_v^{6n^2N^4+k} & \text{if } v \text{ is finite,} \\ (k+1)^{4nN^2} \|F\|_w^{2nN^2} A_v'^{2nN^3} (4A_v)^{6n^2N^4+k} & \text{otherwise,} \end{cases}$$

so that

$$|b_k|_w \begin{cases} |b'_{20}|_w^{-\kappa_1-1} \|F\|_w^{3nN^2} A_v'^{3nN^3} A_v^{10n^2N^4+2k} & \text{if } v \text{ is finite,} \\ (k+1)^{5nN^2} |b'_{20}|_w^{-\kappa_1-1} \|F\|_w^{3nN^2} A_v'^{3nN^3} (4A_v)^{10n^2N^4+2k} & \text{otherwise.} \end{cases} \tag{4.11}$$

Combined with (4.10), (2.5) and (2.6), we get that

$$h(b_k) \leqslant (50n^4N^5 + 5(k+1)n^3N^3)h_{\mathbb{A}}(F) + O((k+1)n^3N^6), \qquad (k = 0, 1, \ldots). \quad (4.12)$$

Recall now that $v_0 \in S$ is such that $|\alpha|_{v_0} = \max_{v\in S}\{|\alpha|_v\})$. If $|\alpha|_{v_0} \leqslant 32^e A_v^{2e}$, by definition of v_0, we get

$$h(\alpha) \leqslant |S|\frac{d_{v_0}}{d}\log 32^e A_v^{2e} \leqslant 4|S|n^3N^2h_{\mathbb{A}}(F) + O(|S|n^3N^3).$$

Let us now assume that $|\alpha|_{v_0} > 32^e A_v^{2e}$. Then, by Theorem 2.2.2, the series $\sum_k b_k\alpha^k$ converges absolutley in the v_0-metric and if we denote by $\mathcal{Z}(\alpha)$ its sum, by (4.11), we have

$$\begin{aligned}|\mathcal{Z}(\alpha) - b_0|_{v_0} &\leqslant |\alpha|_{v_0}^{-1/e}\sum_{k\geqslant 0}|b_{k+1}|_{v_0}\alpha|_{v_0}^{-k/e}\\ &\leqslant \frac{|\alpha|_{v_0}^{-1/e}}{|b'_{20}|_{v_0}^{\kappa_1+1}}4^{17n^2N^4}\|F\|_{v_0}^{3nN^2}A_v'^{3nN^3}A_v^{12n^2N^4}\sum_{k\geqslant 0}k^{5nN^2}2^{-k}.\end{aligned}$$

A quick study of the series $\sum_{k\geqslant 0}k^{5nN^2}2^{-k}$ shows that it is bounded by $(40nN^2)^{5nN^2}$ so that

$$|\mathcal{Z}(\alpha) - b_0|_{v_0} \leqslant C_1|\alpha|_{v_0}^{-1/e}$$

where $C_1 = (40nN^2)^{5nN^2}4^{17n^2N^4}\|F\|_{v_0}^{3nN^2}A_v'^{3nN^3}A_v^{12n^2N^4}\exp(3nN^2h(b_{2,-\kappa_2}))$ and by definition of v_0, we get

$$|\mathcal{Z}(\alpha) - b_0|_{v_0} \leqslant C_1\exp\left(-\frac{d}{nN|S|d_{v_0}}h(\alpha)\right). \quad (4.13)$$

Remark 4.4.1 In the next chapter, we will need to estimate $\log C_1$. By (4.10), (2.5) and (2.6), we get

$$h(b_{2,-\kappa_2}) \leqslant 12dn^3N^3h_{\mathbb{A}}(F) + O(dn^3N^4)$$

and

$$\log C_1 \leqslant 66dn^4N^5h_{\mathbb{A}}(F) + O(dn^4N^6). \quad (4.14)$$

4.5 Baker's method

If $\mathcal{Z}(\alpha) = b_0$, we can bound $h(\alpha)$ explicitly. Indeed, in this case, we have

$$\alpha^{1/e} = -\frac{1}{b_1}\sum_{k\geqslant 1}b_{k+1}\alpha^{-(k-1)/e}$$

so that

$$|\alpha|_{v_0}^{1/e} \leqslant \frac{1}{|b_1|_{v_0}}\sum_{k\geqslant 1}|b_{k+1}|_{v_0}|\alpha|_{v_0}^{-(k-1)/e} \leqslant \sum_{k\geqslant 1}|b_{k+1}|_{v_0}|\alpha|_{v_0}^{-(k-1)/e}\exp(h(b_1)).$$

Recall now that we assumed that $|\alpha|_{v_0} \geqslant 32^e A_{v_0}^{2e}$. Then by (4.11) we get

$$|\alpha|_{v_0}^{1/e} \leqslant 32 A_{v_0}^2 C_1 \exp(h(b_1))$$

and by definition of v_0, we have

$$h(\alpha) \leqslant nN|S|\frac{d_{v_0}}{d}(\log C_1 + 2\log A_{v_0} + \log 32 + h(b_1)).$$

But $\log A_{v_0}$ is controlled by (4.3), $\log C_1$ by (4.14) and $h(b_1)$ is controlled by (4.12) so that

$$h(\alpha) \leqslant 128|S|dn^5N^6h_{\mathbb{A}}(F) + O(|S|dn^5N^7).$$

Let us now assume that $|\mathcal{Z}(\alpha) - b_0|_{v_0} \neq 0$. We will apply Baker's method to $b_0^{-1}\mathcal{Z}(\alpha) - 1$.

4.5.1 Baker's inequalities

Proposition 4.5.1 *Let K be a number field of degree d, and let v be a valuation on K. Let $\theta_0, \ldots, \theta_r$ be elements of K^* and let $\ell_0, \ldots, \ell_r$ be rational integers such that $\theta_0^{\ell_0} \cdots \theta_r^{\ell_r} - 1$ does not vanish.*

1. *If v is finite, and if we denote by $\mathfrak{p}$ the prime ideal of $\mathcal{O}_K$ associated to v we have*

$$|\theta_0^{\ell_0} \cdots \theta_r^{\ell_r} - 1|_v > \exp\left(-(10^{20}r^4d^7)^r \frac{p^d}{\log p} h_0 \cdots h_r \log \Lambda\right) \tag{4.15}$$

   where p is the prime lying under $\mathfrak{p}$, $h_i = \max\{h(\theta_i), \log p\}$, $i = 0, \ldots, r$ and $\Lambda = \max\{|\ell_0|, \ldots, |\ell_r|\}$.

2. *If v is infinite, we have*

$$|\theta_0^{\ell_0} \cdots \theta_r^{\ell_r} - 1|_v > \exp(-(10^{20}r^6d^3)^r h_0' \cdots h_r'(\log \Lambda + 1) - 1) \tag{4.16}$$

   where $h_i' = \max\{dh(\theta_i), |\log \theta_i|, 0.16\}$, $i = 0, \ldots, r$ and $\Lambda = \max\{|\ell_0|, \ldots, |\ell_r|\}$.

Proof 1. If v is finite, K. Yu [33] gives us an upper bound for $\mathrm{ord}_{\mathfrak{p}}(\theta_0^{\ell_0} \cdots \theta_r^{\ell_r} - 1)$.

2. If v is infinite, Matveev [19] gives us a lower bound for $|\log(\theta_0^{\ell_0} \cdots \theta_r^{\ell_r})|$. □

4.5.2 Adapted units

Let K be a number field of degree d over $\mathbb{Q}$ and let $S = \{v_0, \dots, v_r\}$ a finite subset of $\mathcal{M}_K$ containing all the infinite places. For a fundamental system of S-units $\eta_1, \dots, \eta_r$ we denote by $R(S) = R_K(S)$ the *S-regulator* of K, that is the absolute value of the matrix

$$[d_{v_i} \log |\eta_i|_{v_i}]_{1 \leqslant i,j \leqslant r}. \tag{4.17}$$

It is well defined and equal to the usual regulator $R = R_K$ when S is made of the infinite places.

Proposition 4.5.2 *There exists a fundamental system of S-units $\eta_1, \dots, \eta_r$ such that*

$$h(\eta_1) \cdots h(\eta_r) \leqslant (r+1)^{2r} d^{-r} R(S), \tag{4.18}$$
$$h^*(\eta_1) \cdots h^*(\eta_r) \leqslant (r+1)^{2r} \zeta(d)^r R(S), \tag{4.19}$$
$$(\zeta(d)d)^{-1} \leqslant h(\eta_i) \leqslant (r+1)^{2r} \zeta(d)^{r-1} R(S). \tag{4.20}$$

Here $h^*(\eta) = \max\{1, h(\eta)\}$ and $\zeta(d) = 1201 \left(\frac{\log d'}{\log\log d'}\right)^3$ with $d' = \max\{d, 3\}$. Furthermore, if $[\lambda_{ij}]_{1 \leqslant i,j \leqslant r}$ is the inverse matrix of (4.17), then

$$|\lambda_{ij}| \leqslant (r+1)^{2r} \zeta, \qquad (1 \leqslant i, j \leqslant r). \tag{4.21}$$

Proof See Bugeau and Győry [6, Lemma 1]. Note that the left hand inequality in (4.20) is a well-known result of Dobrowolski [9].

Corollary 4.5.3 *Suppose that $\eta = \eta_1^{\ell_1} \cdots \eta_r^{\ell_r}$, $\ell_1, \dots, \ell_r \in \mathbb{Z}$ where $\eta_1, \dots, \eta_r$ are from Proposition 4.5.2. Then*

$$\Lambda \leqslant (r+1)^{2r+2} \zeta(d) h(\eta)$$

where $\Lambda = \max\{|\ell_1|, \dots, |\ell_r|\}$.

Proof Straightforward from (4.20) and (4.21).

Proposition 4.5.4 *For any $\gamma \in K$ there exists an S-unit η such that $\omega = \gamma\eta^{-1}$ satisfies*

$$\sum_{\substack{v \in S \\ v \neq v_0}} \frac{d_v}{d} |\log |\omega|_v| \leqslant (r+1)^{2r+1} \zeta(d)^{r-1} R(S). \tag{4.22}$$

Proof This is Proposition 4.1.3 in [5]. □

4.5.3 Applications

Let S_L be the subset of $\mathcal{M}_L$ containing the extensions of the places of S to L. Let also p' be the biggest prime number lying under a place of S and put $\widehat{p} = \max\{p', 3\}$ (if $S = \mathcal{M}_K^\infty$, put $\widehat{p} = 3$). By Proposition 4.5.2, there is a fundamental system of S_L-units $\eta_1, \dots, \eta_r$ satisfying (4.18), (4.19) and (4.20) where $r = |S_L| - 1$. Furthermore, since $\mathcal{Z}_1(\alpha) = F(\alpha, \beta)$, it belongs on L and there exists an S_L-units η and $\omega \in L^*$ satisfying (4.22) such that $\mathcal{Z}_1(\alpha)$ splits into $\mathcal{Z}_1(\alpha) = \omega\eta$. Furthermore, there is rational integers $\ell_1, \dots, \ell_r$ such that $\eta = \eta_1^{\ell_1} \cdots \eta_r^{\ell_r}$. Recall that there is $\sigma \in \Gamma$ such that

$$\mathcal{Z}_2(\alpha) = \sigma(\mathcal{Z}_1(\alpha)) = \sigma(\omega)\sigma(\eta_1)^{\ell_1} \cdots \sigma(\eta_r)^{\ell_r}$$

so that

$$b_0^{-1}\mathcal{Z}(\alpha) = \theta_0\theta_1^{\ell_1} \cdots \theta_r^{\ell_r}$$

where $\theta_0 = b_0^{-1}\omega^{\kappa_2}\sigma(\omega)^{-\kappa_1}$ and $\theta_i = \eta_i^{\kappa_2}\sigma(\eta_i)^{-\kappa_1}$, $i = 1, \dots, r$. And recall that $\kappa_i = \mathrm{ord}_0\mathcal{Z}_i \leqslant 2nN^2$ so that

$$h(\theta_0) \leqslant 4nN^2h(\omega) + h(b_0) \leqslant 4nN^2h(\omega) + 55n^4N^5h_{\mathbb{A}}(F) + O(n^3N^6). \tag{4.23}$$

(The height of b_0 is given by (4.12)). In the same way, we get

$$h(\theta_i) \leqslant 4nN^2h(\eta_i), \qquad (i = 1, \dots, r).$$

Then, if $h_i = \max\{h(\theta_i), \log\widehat{p}\}$ and $h_i' = \max\{dn^2h(\theta_i), |\log\theta_i|, 0.16\}$ for every $i \in \{1, \dots, r\}$, we have

$$h_i \leqslant 2h^*(\theta_i)\log\widehat{p} \leqslant 8nN^2h^*(\eta_i)\log\widehat{p}$$

$$h_i' \leqslant dn^2h(\theta_i) + \pi \leqslant 4dn^3N^2h(\eta_i) + \pi$$

and by Proposition 4.5.2 we get

$$\prod_{i=1}^r h_i \leqslant (8nN^2\log\widehat{p})^r \prod_{i=1}^r h^*(\eta_i) \leqslant (10^{20}dn^2N^2r^2\log\widehat{p})^r R(S_L)$$

and

$$\prod_{i=1}^r h_i' \leqslant r(4dn^3N^2\pi)^r \prod_{i=1}^r h^*(\eta_i) \leqslant (10^{20}d^2n^4N^2r^3)^r R(S_L).$$

Then, by Proposition 4.5.1, if v_0 is finite we have

$$|b_0^{-1}\mathcal{Z}(\alpha) - 1|_{v_0} > \exp(-C_2h_0\log\Lambda) \tag{4.24}$$

where $C_2 = (10^{40}d^8n^2N^2r^6\log\widehat{p})^r\widehat{p}^dR(S_L)$ and $\Lambda = \max\{1, |\ell_1|, \dots, |\ell_r|\}$ while if v_0 is infinite, we have

$$|b_0^{-1}\mathcal{Z}(\alpha) - 1|_{v_0} > \exp(-C_3h_0'(\log\Lambda + 1) - 1) \tag{4.25}$$

where $C_3 = (10^{40}d^5n^4N^2r^9)^r R(S_L)$.

4.5.4 A bound for $h(\omega)$

By Proposition 4.5.4, if there is a place $v_1 \in S_L$ such that $|\omega|_{v_1} \leqslant 1$, we have

$$h_{S_L}(\omega) = h_{S_L\setminus\{v_1\}}(\omega) \leqslant \sum_{\substack{v \in S_L \\ v \neq v_1}} \frac{[L_v : \mathbb{Q}_v]}{[L : \mathbb{Q}]} |\log |\omega|_v| \leqslant (r+1)^{2r+1}\zeta(dn)^{r-1}R(S_L).$$

But for any place $v \in \mathcal{M}_L\setminus S_L$, we have $\|\omega\|_v = \|\mathcal{Z}(\alpha)\|_v$. Since α and β are S-integers, for these places, we also have $|\alpha|_v \leqslant 1$ and $|\beta|_v \leqslant 1$ and

$$|\mathcal{Z}_i(\alpha)|_v = |F_i(\alpha,\beta)|_v \leqslant |F|_v.$$

for every $i = 1, \dots, \nu$. Moreover, since $\prod_i \mathcal{Z}_i(\alpha) = A$, we have for every $i = 1, \dots, \nu$

$$|\mathcal{Z}_i(\alpha)|_v \geqslant \frac{|A|_v}{|F|_v^{n-1}}$$

so that

$$\frac{|A|_v^{\kappa_2}}{\|F\|_v^{n\kappa_2}} \leqslant |\mathcal{Z}(\alpha)|_v \leqslant \frac{\|F\|_v^{n\kappa_2}}{|A|_v^{\kappa_1}}. \tag{4.26}$$

Then

$$h_{\mathcal{M}_L\setminus S_L}(\omega) = h_{\mathcal{M}_L\setminus S_L}(\mathcal{Z}(\alpha)) \leqslant n\kappa_2 h_{\mathbb{A}}(F) + \kappa_1 h(A)$$

so that

$$h(\omega) \leqslant 2n^2N^2h_{\mathbb{A}}(F) + 2nN^2h(A) + (2rdn)^{3r}R(S_L).$$

On the other hand, if we have $|\omega|_v > 1$ for every $v \in S_L$, we have $h(\omega) = h(\omega^{-1}) = \sum_{v\notin S_L} h_v(\mathcal{Z}(\alpha)^{-1})$. But by (4.26), we have $|\mathcal{Z}(\alpha)^{-1}|_v \leqslant \|F\|_v^{n\kappa_2}|A|_v^{-\kappa_2}$ for every $v \notin S_L$ so that $h(\omega) \leqslant n\kappa_2 h_{\mathbb{A}}(F) + \kappa_2 h(A)$. Then in any cases, we have

$$h(\omega) \leqslant 2n^2N^2h_{\mathbb{A}}(F) + 2nN^2h(A) + (2rdn)^{3r}R(S_L). \tag{4.27}$$

4.5.5 Last steps

From (4.23) and (4.27) we get

$$h_0 \leqslant h(\theta_0) + \log\widehat{p} \leqslant 63n^4N^5h_{\mathbb{A}}(F) + 8n^2N^4h(A) + (8rdn^2N^2)^{3r}R(S_L) + \log\widehat{p} + O(n^3N^6)$$

and

$$h_0' \leqslant dn^2h(\theta_0) + \pi \leqslant 63dn^6N^5h_{\mathbb{A}}(F) + 8dn^4N^4h(A) + (8rd^2n^4N^2)^{3r}R(S_L) + O(dn^5N^6).$$

Combined with (4.24) and (4.25), we get

$$|\mathcal{Z}(\alpha) - b_0|_{v_0} \geqslant |b_0|_{v_0}\exp(-C_4(\log\Lambda + 1))$$

where

$$\begin{aligned}C_4 =&(10^{20}d^9r^9n^{10}N^7\widehat{p}\log\widehat{p})^r R(S_L)(h_{\mathbb{A}}(F)+h(A))\\ &+O((d^{14}r^{11}n^{16}N^8\widehat{p}(\log\widehat{p})^2)^r R(S_L)(R(S_L)+1)).\end{aligned}$$

Finally, from (4.12) we get

$$|b_0|_{v_0}\geqslant \exp(-dn^2h(b_0))\geqslant \exp(-55dn^6N^5h_{\mathbb{A}}(F)+O(dn^5N^6))$$

and combined with (4.13) and (4.14), we get

$$\begin{aligned}h(\alpha)&\leqslant \frac{e|S|d_{v_0}}{d}\left(\log C_1+C_4(\log\Lambda+1)+55dn^6N^5h_{\mathbb{A}}(F)+O(dn^5N^6)\right)\\ &\leqslant C_4'\log\Lambda+C_5\end{aligned}\tag{4.28}$$

where

$$\begin{aligned}C_4' =&(10^{20}d^9r^{10}n^{11}N^8\widehat{p}\log\widehat{p})^r R(S_L)(h_{\mathbb{A}}(F)+h(A))\\ &+O((d^{14}r^{13}n^{17}N^9\widehat{p}(\log\widehat{p})^2)^r R(S_L)(R(S_L)+1))\end{aligned}$$

and

$$\begin{aligned}C_5 =&(10^{20}d^9r^{10}n^{11}N^8\widehat{p}\log\widehat{p})^r (R(S_L)+1)(h_{\mathbb{A}}(F)+h(A))\\ &+O((d^{14}r^{13}n^{17}N^9\widehat{p}(\log\widehat{p})^2)^r (R(S_L)+1)^2).\end{aligned}$$

On the other hand, recall that $\mathscr{Z}_1(\alpha)=\omega\eta=\omega\eta_1^{\ell_1}\cdots\eta_r^{\ell_r}$. Then if we put $\Lambda^*=\max\{|\ell_1|,\ldots,|\ell_r|\}$, by Corollary 4.5.3, we have

$$\Lambda^*\leqslant (r+1)^{2r+2}\zeta(dn)h(\eta)\leqslant (16dnr^4)^r h(\eta)$$

and by (4.27) we get

$$\begin{aligned}h(\eta)&\leqslant h(\omega)+h(\mathscr{Z}_1(\alpha))\\ &\leqslant 2nN^2h(\alpha)+4n^2N^2h_{\mathbb{A}}(F)+2nN^2h(A)+(2rdn)^{3r}R(S_L)+O(nN^2).\end{aligned}\tag{4.29}$$

(The estimation of $h(\mathscr{Z}_1(\alpha))$ comes from Proposition 2.1.7). Then

$$\Lambda\leqslant\Lambda^*+1\leqslant C_6h(\alpha)+C_7\tag{4.30}$$

where

$$C_6=(32dr^4n^2N^2)^r$$

and

$$C_7=(64dr^4n^2N^2)^r(h_{\mathbb{A}}(F)+h(A))+O((d^4r^4n^4N^2)^r(R(S_L)+1)).$$

Combined with (4.28), we get

$$h(\alpha) \leqslant C_4' \log h(\alpha) + C_5' \tag{4.31}$$

where

$$C_5' = C_4' \log((64dr^4n^2N^2)^r(h_{\mathbb{A}}(F) + h(A)) + O((d^4r^4n^4N^2)^r(R(S_L) + 1))) + C_5.$$

Finally, the following lemma will end the proof.

Lemma 4.5.5 *Let A and B be non-negative constants ($B \geqslant 1$). Then for any $x > 1$ such that $x \leqslant A \log x + B$ we have*

$$x \leqslant 2A \log(2A) + 2B. \tag{4.32}$$

Proof If $x \leqslant 2B$, this is done. Otherwise, we have $x \leqslant 2A \log x \leqslant 2A\sqrt{x}$ so that $x \leqslant 4A^2$ and by hypothesis, we get (4.32). □

Applied to (4.31), we get that

$$h(\alpha) \leqslant 2C_4' \log(2C_4') + 2C_5'$$

and from Proposition 2.1.7, we get

$$\begin{aligned} h(\beta) &\leqslant h_{\mathbb{P}}(G) + \mu h(\alpha) + \nu + \log(\mu + 1) \\ &\leqslant nh_{\mathbb{A}}(F) + 5nN + 2nNC_4' \log(2C_4') + C_5' \end{aligned}$$

□

Remark 4.5.6 A tiresome but routine calculation, using the fact that $dn \leqslant 2r + 2$, implies that for a large constant C, we have

$$\max\{h(\alpha), h(\beta)\} \leqslant (Cnr\widehat{p} \log \widehat{p})^{30r} R(S_L)\Omega \log \Omega$$

where $\Omega = h_{\mathbb{A}}(F) + h(A) + R(S_L)$. Also, the regulator $R(S_L)$ can be explicitly estimated in terms of the degrees d and n, the discriminant of L and the prime $\widehat{p}$ (see for instance [2, Section 1.4, Corollary 10]).

Bibliographie

[1] A. Baker, *Transcendental Number Theory*, Cambridge University Press (1975).

[2] Yu. Bilu, *Effective analysis of Integral Points on Algebraic Curves*, Thesis, Beer Sheva (1993), available on `http://www.ufr-mi.u-bordeaux.fr/ yuri/publ/`.

[3] Yu. Bilu, G. Hanrot, P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. reine angew. Math. **539** (2001), 75-122.

[4] Yu. Bilu, D. Masser, *A quick proof of Sprindzhuk's decomposition theorem*, Finite and Infinite Mathematics, to appear.

[5] Yu. Bilu, *Quantitative Siegel's theorem for Galois coverings*, Compositio Mathematica **106** (1997), 125-158.

[6] Y. Bugeaud, K. Győry, *Bounds for the solutions of units equations*, Acta Arithm. **74** (1996), n°1, 67-80 .

[7] Y. Bugeaud, K. Győry, *Bounds for the solutions of Thue-Mahler equations and norm form equations*, Acta Arithm. **74** (1996), n°3, 273-292.

[8] P.D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$. Ann. Math. (2) **15** (1913), 30-70.

[9] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arithm. **34** (1994), 421-443.

[10] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. **9** (1959) 437-41.

[11] B. M. Dwork, A. J. Van der Poorten, *The Eisenstein Constant*, Duke Math. J. **65** (1992), 23-43 ; corrections : **76** (1994), 669-672.

[12] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Pure and Applied Math. **23**, Academic Press (1966).

[13] P. Habegger, *Intersecting a variety with algebraic subgroups of multiplicative groups*, in preparation.

[14] S. Lang, *Algebra*, GTM **221**, Springer, Revised Third Edition (2002).

[15] S. Lang, *Diophantine Geometry*, Tracts in Mathematics number **11** (1962).

[16] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930) 419-48.

[17] E. Lucas, *Sur les rapports qui existent entre la théorie des nombres et le calcul intérgal*, C. R. Acad. Sci. Paris, **82** (1876) 1303-5.

[18] E. Lucas, *Théorie des fonctions numériques simplement pèriodiques*, Amer. J. Math. **1** (1878) 184-240, 289-321.

[19] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II*, Izv. Math. **64** (2000), nř 6. 1217-1269.

[20] D. Roy, J.L. Thunder, *An absolute Siegel's Lemma*, J. reine angew. Math. **476** (1996), 1-26.

[21] A. Schinzel, *The intrinsic divisors of Lehmer numbers I*, Acta Arith. **8** (1963) 213-23.

[22] C. L. Siegel, *Uber einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), 41-69. Reprinted as pp. 209-266 of his Gesammelte Abhandlungen I, Springer, Berlin (1966).

[23] M. Hindry, J. Silverman, *Diophantine Geometry, an introduction*, GTM **201**, Springer. (2000).

[24] T. Skolem, *Diophantische Gleichungen*, J. Springer, Berlin (1938), reprinted by Chelsea, New York (1950).

[25] T. Skolem, *Lösung gewisser Gleichungssysteme in ganzen Zahlen oder ganzzahligen Polynomen mit beschränktem gemeinschaftlichen Teiler*, Oslo Vid. Akar. Skr. I, n°**12** (1929).

[26] V. G. Sprindžuk, *Arithmetic specializations in polynomials*, J. Reine Angew. Math. **340** (1983), 26–52.

[27] V. G. Sprindžuk, *Classical Diophantine equations*, Translated from the 1982 Russian original. Lecture Notes in Mathematics **1559**. Springer-Verlag (1993).

[28] C. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1997), 425-447.

[29] D. Poulakis, *Integer points on rational curves with fixed gcd*, Publ. Math. Debrecen **64/3-4** (2004), 369-379.

[30] P.M. Voutier, *Primitive divisors of Lucas ans Lehmer sequences*, Math. Comp **64** (1995), 869-888.

[31] P. G. Walsh, *A quantitative version of Runge's theorem on diophantine equations*, Acta Arithm. **LXII.2** (1992), 157-172.

[32] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) **62** (1955) 230-36.

[33] K. Yu, *p-adic logarithmic forms and group varieties II*, Acta Arithm. **LXXXIX.4** (1999), 337-378.

[34] K. Zsigmondy, *Zur Theorie der Potenzreste*, Moantsh. Math. **3** (1892), 265-284.