Effectivité dans le théorème d'irréductibilité de Hilbert

Yann Walkowiak

Thèse en Cotutelle

franco-italienne
(Tesi in Cotutela)

présentée à

L'UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
et
L'UNIVERSITÀ DEGLI STUDI DI UDINE

pour obtenir

LE TITRE DE DOCTEUR DE L'UNIVERSITÉ

SPÉCIALITÉ : MATHÉMATIQUES PURES

par

Yann WALKOWIAK

Effectivité dans le théorème d'irréductibilité de Hilbert.

Président :	Pr. Michel WALDSCHMIDT	Université de Paris VI.
Directeurs :	Pr. Pierre DÈBES	Université de Lille I.
	Pr. Umberto ZANNIER	Scuola Normale Superiore di Pisa, Italie.
Rapporteurs :	Pr. Roger HEATH-BROWN	University of Oxford, Angleterre.
	Pr. Peter MÜLLER	Universität Würzburg, Allemagne.
Examinateurs :	Pr. Mohamed AYAD	Université du Littoral.
	Pr. Pietro CORVAJA	Università degli Studi di Udine, Italie.

Remerciements

Je tiens à remercier sincèrement mon directeur de thèse, Pierre Dèbes, pour sa disponibilité, sa passion communicative et son ouverture d'esprit. Il a su me guider dans cet apprentissage de la recherche en m'en montrant les plus beaux visages et en m'aidant à surmonter les passages difficiles. Il a fait de ces trois années une période des plus enrichissantes de ma vie, du point de vue mathématique, mais aussi humainement.

Je remercie le professeur Umberto Zannier pour avoir accepté de codiriger cette thèse et pour m'avoir proposé des pistes de recherche fructueuses.

Pietro Corvaja a joué un rôle considérable dans cette thèse. Je lui suis infiniment reconnaissant pour sa disponibilité, ses précieux conseils et les discussions mathématiques que nous avons eues lors de mes séjours en Italie. Je tiens également à le remercier pour son accueil, sa gentillesse et son amitié. Enfin, je ne pourrais terminer sans rendre hommage à ses grands talents de cuisinier.

Je souhaite remercier le Professeur Roger Heath-Brown pour ses suggestions qui m'ont permis d'améliorer certains points, mais aussi pour avoir spontanément accepté d'être rapporteur. Le Professeur Peter Müller a également accepté la lourde tâche de rapporter cette thèse. Je suis très honoré de l'intérêt qu'ils lui ont porté et les en remercie vivement.

Je tiens à exprimer ma très grande reconnaissance aux Professeurs Michel Waldschmidt et Mohamed Ayad qui ont accepté d'examiner cette thèse et de faire partie du jury de soutenance. Mohamed Ayad fait partie des personnes qui m'ont fait découvrir la richesse des polynômes lors de son cours de DEA.

La cotutelle avec l'université de Udine m'a apporté une chose à laquelle je ne m'attendais pas, la rencontre avec Jung-Kyu et Letizia. Ils m'ont accueilli comme si nous étions déjà amis, m'ont hébergé et fait découvrir leur beau pays. Je les remercie pour leur simplicité, leur gentillesse sans égal. J'ai passé avec eux des moments inoubliables (i delfini in croazia !, no fun, l'aglio olio, Roma, e tanti altri momenti !). J'ai également une pensée pour Alfio, Marinella et leur petite Agata qui vient de voir le jour.

J'adresse mes remerciements aux membres de l'équipe d'Arithmétique et plus généralement au personnel du laboratoire de Mathématiques, au sein duquel j'ai préparé ce travail. Je tiens également à remercier le personnel

de la Bibliothèque de Mathématiques, des secrétariats et de la reprographie dont l'aide m'a été précieuse.

Cette thèse m'a également permis de faire la connaissance d'autres doctorants : Pierre-Antoine et Aurélie, que j'ai l'impression de connaitre depuis toujours, Olivier et Sophie qui m'ont accepté dans le bureau de la fac où l'on fait le meilleur café, mais aussi Augustin, Benoit, David, Fred, Véronique, Stéphanie et Virginie. Il y a aussi Salah (quelle gentillesse !) qui se pose comme moi des questions rigolotes sur les polynômes, et plus récemment Stéphane, Séverine, Marco (encore un italien), Romain, Anna et j'en oublie sûrement...

Je n'oublie pas tous mes amis qui n'ont rien à voir avec l'université et qui m'ont permis de conserver un équilibre plus ou moins équilibré. Je pense à Nikho particulièrement et à son gratin de gnocchi à faire pâlir un italien, mais aussi Chkrout avec ses bonnes adresses de resto, et puis tous les autres avec qui j'ai pris du plaisir à discuter de choses et d'autres. Merci David Ivar et André, Jason, les Ex et les prochaines licornes qui ont croisé mes oreilles dans un grand mélange ou ailleurs. Et pour être certain de n'oublier personne, je te remercie aussi, toi qui lis au moins cette page.

Enfin, je remercie profondément ma famille. Mes parents ont su éveiller ma curiosité dès le plus jeune âge et m'ont donné les moyens et les encouragements qui m'ont permis de mener à bien ce travail. Caroline, Eric et Salomé, mais aussi Nadine et Sylvère ont grandement contribué à cette atmosphère de bonheur et de détente qui rend le travail plus facile et plus agréable. Je remercie également mes grands-parents avec une pensée particulière pour ma grand-mère qui était toujours si fière de moi.

Je remercie Ingrid du fond du coeur. Elle m'a aidé bien plus qu'elle ne le croit, par son soutien de chaque instant, mais aussi et simplement car elle me rend heureux.

Résumé

Le théorème d'irréductibilité de Hilbert assure l'existence d'une spécialisation conservant l'irréductibilité d'un polynôme à plusieurs variables et à coefficients rationnels. Des versions effectives ont été données par P. Dèbes (1993) puis par U. Zannier et A. Schinzel (1995). Nous proposons ici diverses tentatives d'améliorer ces résultats effectifs : méthode de Dörge, méthode des congruences inspirée par un article de M. Fried et enfin une utilisation des résultats récents de R. Heath-Brown sur les points entiers d'une courbe algébrique. Cette dernière voie va nous permettre d'améliorer significativement les résultats connus. On finira par une application à la recherche d'un algorithme polynomial pour la factorisation d'un polynôme à deux indéterminées.

Riassunto

Il teorema d'irriducibilità di Hilbert assicura l'esistenza di una specializzazione che conserva l'irriducibilità di un polinomio in più variabili e a coefficienti razionali. Alcune versioni effettive sono state date da P. Dèbes (1993) e da U. Zannier e A. Schinzel (1995). In questa tesi proponiamo diversi tentativi per migliorare questi risultati effettivi : metodo di Dörge, metodo delle congruenze ispirato da un articolo di M. Fried e infine un utilizzo dei recenti risultati di R. Heath-Brown sui punti interi di una curva algebrica. Questo ultimo punto di vista ci permette di migliorare in modo significativo i risultati conosciuti. Termineremo con un'applicazione volta alla ricerca di un algoritmo polinomiale per la fattorizzazione di un polinomio a due indeterminate.

Table des matières

Introduction

Soit $F(T, Y)$ un polynôme à coefficients dans un corps k de degré partiel en Y supérieur ou égal à 1. La question que nous allons étudier est très concrète : on suppose $F(T, Y)$ irréductible sur k et on s'intéresse aux polynômes spécialisés $F(t, Y)$ où $t \in k$; sont-ils irréductibles sur k ? Prenons par exemple le polynôme $F(T, Y) = Y^2 - T$. $F(t, Y)$ est irréductible dans $k[Y]$ si et seulement si t n'est pas un carré dans k. Si $k = \mathbb{C}$, cela n'arrive jamais. Mais pour d'autres corps, comme $k = \mathbb{Q}$, il en existe beaucoup (une infinité). Le théorème d'irréductibilité de Hilbert dit que pour, $k = \mathbb{Q}$, il s'agit d'un phénomène général.

Théorème (Hilbert, 1892). *Étant donné un polynôme $F(T, Y) \in \mathbb{Q}[T, Y]$ irréductible sur $\mathbb{Q}$ et tel que $\deg_Y(F) \geq 1$, il existe une infinité de nombres $t \in \mathbb{Q}$ tels que $F(t, Y)$ est irréductible dans $\mathbb{Q}[Y]$.*

On peut énoncer une version plus générale de ce théorème avec plusieurs variables et plusieurs paramètres qu'on spécialise, mais l'énoncé ci-dessus constitue le cas essentiel du théorème d'irréductibilité de Hilbert.

Le but de cette thèse est de donner une nouvelle version effective de ce théorème améliorant les résultats connus avec comme motivation particulière l'écriture d'un algorithme polynomial pour la factorisation des polynômes à deux variables.

Le premier chapitre va tout d'abord expliciter les différentes motivations de ce travail en donnant quelques unes des nombreuses applications du théorème d'irréductibilité de Hilbert. On insistera sur l'interêt de disposer d'une version effective la meilleure possible pour certaines applications algorithmiques, et on donnera les résultats déjà connus dus à P. Dèbes et à A. Schinzel et U. Zannier. Une seconde partie donnera quelques outils du domaine de l'effectivité : façons de mesurer un polynôme, inégalités entre ces différentes mesures, etc... Enfin, on exposera une réduction classique du théorème de Hilbert qui consiste à transformer le problème d'irréductibilité en un problème de géométrie diophantienne. Cette réduction sera utilisée au

cours des 3 chapitres suivants qui présenteront chacun une méthode qui permet d'obtenir une nouvelle version effective du théorème d'irréductibilité de Hilbert.

Le deuxième chapitre est consacré à rendre effective la preuve originale du théorème de Hilbert comme elle est exposée par Dörge dans [Do] en 1927. Cette méthode se ramène tout d'abord à l'étude de séries de Puiseux solutions d'une équation algébrique. On sera donc amené à démontrer une forme effective du théorème de Puiseux. Elle utilise ensuite des arguments d'interpolation et on sera amené entre autres à estimer le nombre de zéros de la dérivée itérée d'une fonction algébrique. On obtiendra ainsi un nouvel énoncé effectif du théorème de Hilbert ayant la particularité d'être basé uniquement sur des outils simples et déjà connus en 1927. Malheureusement, certaines étapes sont très couteuses et la borne obtenue est moins bonne que les résultats déjà connus.

Le troisième chapitre donne une méthode simple pour trouver une bonne spécialisation inspirée d'une preuve de M. Fried du théorème de Hilbert. Celle-ci utilise le fait que les inégalités de Lang-Weil fournissent de bonnes estimations explicites sur les points entiers sur une courbe algébrique dans le cas des corps finis. L'idée consiste donc à utiliser les congruences puis à utiliser le lemme chinois pour remonter les informations. On obtient ainsi un algorithme très simple pour le théorème de Hilbert. Cependant, on est amené à faire des hypothèses supplémentaires sur l'extension engendrée par F et de plus, la borne trouvée est essentiellement liée à une version effective du théorème d'Ostrowski due à U. Zannier et celle-ci ne fournit pas une borne polynomiale.

Le quatrième chapitre constitue la partie la plus originale de cette thèse. Une première partie présente un résultat récent de R. Heath-Brown sur le nombre de points entiers sur une courbe algébrique. On donnera une version totalement explicite de ce résultat dans le cadre qui nous intéresse. Ceci va nous permettre de donner une borne pour la plus petite spécialisation sans zéro entier puis d'en déduire un nouvel énoncé effectif du théorème d'irréductibilité de Hilbert. Ce nouvel énoncé améliore les résultats connus de manière significative mais ne fournit pas de borne polynomiale, en raison de l'utilisation de la réduction exposée dans le premier chapitre qui est très couteuse. On montrera cependant que, si on se place dans le cadre classique où l'extension définie par F est galoisienne, alors une modification de la réduction nous permet de ramener le problème à une condition de pure théorie des groupes. L'utilisation d'un résultat récent de L. Pyber fournira

alors une réponse positive à notre problème : trouver une borne polynomiale pour le théorème d'irréductibilité de Hilbert.

Enfin, on donnera dans le dernier chapitre le détail de l'algorithme de factorisation d'un polynôme à deux variables par réduction au cas d'une variable.

Chapitre 1

Préliminaires

1.1 Applications - Motivations

La motivation première de Hilbert pour le théorème d'irréductibilité était le problème inverse de Galois mais ce théorème a de nombreuses autres applications. Nous verrons en particulier l'exemple de la factorisation d'un polynôme à deux indéterminées qui nous mènera à nous poser la question de l'effectivité.

1.1.1 Problème inverse de Galois

Le Problème inverse de Galois est l'étude de la conjecture suivante :

Conjecture (Problème Inverse de Galois). *Tout groupe fini G est le groupe de Galois $Gal(E/\mathbb{Q})$ d'une extension $E/\mathbb{Q}$ du corps $\mathbb{Q}$.*

Hilbert cherchait à réaliser S_n comme groupe de Galois sur $\mathbb{Q}$. Il eut alors l'idée de réaliser d'abord S_n sur le corps $\mathbb{Q}(T_1, \ldots, T_n)$ puis de spécialiser les indéterminées $T_1, \ldots, T_n$ en des rationnels $t_1, \ldots, t_n$ tels que l'extension spécialisée reste une réalisation de S_n sur $\mathbb{Q}$. Pour cela, il a besoin de spécialisations qui conservent l'irréductibilité d'un certain polynôme. Il démontre alors le théorème suivant, donnant l'existence d'une infinité de telles spécialisations.

Théorème 1.1.1 (Hilbert, 1892). *Soit $F(T, Y) \in \mathbb{Q}[T, Y]$ un polynôme irréductible sur $\mathbb{Q}$ de degré en Y supérieur ou égal à 1. Il existe une infinité de $t \in \mathbb{Q}$ tels que $F(t, Y)$ reste irréductible sur $\mathbb{Q}$.*

Cet énoncé se généralise au cas de plusieurs indéterminées et plusieurs paramètres qu'on spécialise. Cependant, il constitue le cas essentiel.

1.1.2 Factorisation d'un polynôme à deux variables

Une des motivations de cette thèse est l'étude du problème suivant : écrire un algorithme permettant de factoriser un polynôme à deux indéterminées. Afin de ne pas alourdir le texte, nous allons donner ici une description succinte de cet algorithme. Les détails et l'étude de sa complexité feront l'objet du chapitre 5.

On considère un polynôme $F(T, Y) \in \mathbb{Z}[T, Y]$ dont on cherche la factorisation en irréductibles sur $\mathbb{Q}$

$$F(T, Y) = \prod_{i=1}^{r} F_i(T, Y)^{\alpha_i}.$$

Si on spécialise T en $t \in \mathbb{Z}$, on obtient d'une part

$$F(t, Y) = \prod_{i=1}^{r} F_i(t, Y)^{\alpha_i}$$

et d'autre part, en utilisant un algorithme de factorisation pour les polynômes à une seule variable (celui décrit dans [LeLeLo] par exemple),

$$F(t, Y) = \prod_{i=1}^{s} \Pi_i^t(Y)^{\beta_i},$$

où les $\Pi_i^t(Y) \in \mathbb{Z}[Y]$ sont irréductibles sur $\mathbb{Q}$.

On constate alors qu'en choisissant t de façon à ce que les $F_i(t, Y)$ soient irréductibles, et en le faisant pour un nombre suffisant de spécialisations, on obtient un système d'équations qui nous permet de trouver les polynômes F_i.

Le problème est donc de trouver un certain nombre de spécialisations qui préservent l'irréductibilité des polynômes F_i alors que ces polynômes sont les inconnues. L'existence de ces spécialisations est donnée par le théorème de Hilbert, mais les trouver explicitement est un autre problème. Les détails de la méthode feront l'objet du chapitre 5, signalons simplement ici que cet algorithme est polynomial si on est capable de trouver un nombre polynomial de "bonnes" spécialisations pour le théorème de Hilbert en temps polynomial.

1.1.3 Problème de l'effectivité

De nombreuses preuves différentes du théorème de Hilbert sont connues : Hilbert (1892) [H], Mertens (1911) [Me], Skolem (1921) [Sk], Dörge (1927) [Do], Siegel (1929) [Si], Eichler (1939) [Ei], Inaba (1943) [In], Fried (1974)

[Fr], Roquette (1975) [Ro], Cohen (1981) [Co], Sprindžuk (1981) [Spr], Dèbes (1986) [De2], (1993) [De3], Schinzel et Zannier (1995) [ScZa].

Seuls les deux derniers articles mentionnés se sont intéressés au problème de l'estimation d'une spécialisation vérifiant la conclusion du théorème de Hilbert. Le premier résultat dans ce sens est celui de P. Dèbes. Il donne l'énoncé suivant, $H(F)$ désignant le maximum des valeurs absolues des coefficients de F :

Théorème 1.1.2. *Soient $F_1, \ldots, F_h$ polynômes irréductibles dans $\mathbb{Q}[T, Y]$ tels que $\deg F_i \leq D$ et $H(F_i) \leq H$. Alors il existe un rationnel $t = u/v$ tel que chaque $F_i(t, Y)$ est irréductible sur $\mathbb{Q}$ et*

$$\max(|u|, |v|) \leq \exp(10^{10} D^{100hD^2 \log D} (\log^2 H + 1))$$

Par la suite, A. Schinzel et U. Zannier améliorent cette borne avec ce résultat :

Théorème 1.1.3. *Soient $F_1, \ldots, F_h \in \mathbb{Z}[T, Y]$ polynômes irréductibles sur $\mathbb{Q}$. Alors il existe un entier positif t tel que chaque $F_i(t, Y)$ est irréductible sur $\mathbb{Q}$ et*

$$|t| \leq \max\{\exp(2(6m)^5), \exp(36^6), h^9 \exp(450(\log H)^{5/6} + \\ + 11250m^5 + 45(m+1)^2 n + 45n(\log H)^{2/5})\},$$

où $m = \max\{\deg_T F_i\}$, $n = \max\{\deg_Y F_i\}$ et $H = \max\{20, H(F_i)\}$.

Malheureusement, aucun de ces résultats ne fournit une spécialisation en un temps polynomial. Signalons également l'existence d'algorithmes probabilistes qui permettent de donner, en moyenne, une bonne spécialisation en temps polynomial (voir par exemple [Gao]). Cependant, la complexité au pire de ces algorithmes reste exponentielle. Une des motivations de cette thèse est donc d'étudier différentes preuves du théorème de Hilbert afin de les rendre effectives dans l'espoir d'améliorer les résultats ci-dessus.

1.1.4 Cadre de travail

On considère un polynôme F à coefficients rationnels en 2 variables et on s'intéresse à l'irréductibilité du polynôme obtenu par spécialisation d'une variable. Afin de simplifier les raisonnements, notons qu'on peut toujours se ramener, quitte à multiplier par un rationnel convenable, à l'étude d'un polynôme à coefficients entiers et premiers entre eux (on dira que F est primitif). Ainsi, par exemple, la notion de hauteur absolue définie dans la section suivante coïncide avec le maximum des valeurs absolues des coefficients (voir remarque 1.2.2).

1.2 Outils de l'effectivité

1.2.1 Différentes mesures d'un polynômes

Dans ce paragraphe, nous allons préciser différentes notions de "taille" d'un polynôme P puis nous donnerons quelques outils qui permettent de comparer les différentes grandeurs définies (voir [HiSi] pour un exposé détaillé et pour les preuves des estimations données).

Hauteur et mesure de Mahler

La "taille" d'un polynôme peut être appréhendée de différentes manières. Nous allons voir trois grandeurs associées à un polynôme : son degré, sa hauteur et sa mesure de Mahler.

Définition 1.2.1. *Soient K un corps de nombres, M_K l'ensemble des places de K, $I \subset \mathbb{N}^n$ et*

$$P(X_1, \dots, X_n) = \sum_{i=(i_1,\dots,i_n)\in I} a_i X_1^{i_1} \dots X_n^{i_n}$$

un polynôme à coefficients dans K. Soit $v \in M_K$ une place de K, on appelle v-hauteur *du polynôme P la quantité*

$$H_v(P) = \max_{i\in I} |a_i|_v.$$

On note n_v le degré de l'extension K_v sur $\mathbb{Q}_v$, où K_v (respectivement $\mathbb{Q}_v$) est le complété de K (respectivement $\mathbb{Q}$) pour la place v. On définit alors la hauteur absolue *de P par*

$$H(P) = \prod_{v\in M_K} H_v(P)^{n_v/[K:\mathbb{Q}]}.$$

On parlera également de la hauteur logarithmique absolue $h(P) = \log H(P)$.

Remarque 1.2.2. *Pour $K = \mathbb{Q}$, et P à coefficients entiers et primitif (c'est-à-dire dont les coefficients sont premiers entre eux), on a*

$$H(P) = \max_{i\in I} |a_i|,$$

où $|.|$ est la valeur absolue usuelle sur $\mathbb{Q}$.

Définition 1.2.3. *Soit*

$$P(X_1, \dots, X_n) = \sum_{i=(i_1,\dots,i_n)\in I} a_i X_1^{i_1} \dots X_n^{i_n}$$

un polynôme à coefficients dans $\mathbb{C}$. *On appelle* mesure de Mahler *du polynôme* P *la quantité*

$$M(P) = \exp\left(\int_0^1 \dots \int_0^1 \log|P(e^{2i\pi t_1}, \dots, e^{2i\pi t_n})| dt_1 \dots dt_n \right)$$

Remarque 1.2.4. *Pour* $n = 1$, *si on note* $P(X) = a_0 + \dots + a_d X^d = a_d \prod_{i=1}^d (X - \alpha_i)$, *alors on a l'égalité*

$$M(P) = |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\}$$

Inégalité de Liouville

Cette inégalité classique permet de comparer la hauteur d'un polynôme aux valeurs absolues de ses racines.

Proposition 1.2.5. *Soit* K *un corps muni d'une valeur absolue* $|\ |$. *Soit* $P = a_0 + a_1 X + \dots + a_d X^d$ *un polynôme à coefficients dans* K *de degré* $d \geq 0$. *Si* x *est une racine de* P *dans une clôture algébrique* $\overline{K}$ *de* K *et si on note encore* $|\ |$ *un prolongement quelconque de la valeur absolue à* $K(x)$, *alors*

1. – *si la valeur absolue est archimédienne :* $|x| \leq \dfrac{\max_i |a_i| + |a_d|}{|a_d|}$
   – *si* v *est ultramétrique :* $|x| \leq \dfrac{\max_i |a_i|}{|a_d|}$
2. – *si* v *est archimédienne :* $|x| \geq \dfrac{|P(0)|}{\max_i |a_i| + |P(0)|}$
   – *si* v *est ultramétrique :* $|x| \geq \dfrac{|P(0)|}{\max_i |a_i|}$

Comparaison entre hauteur et mesure de Mahler

On a le résultat classique suivant (voir par exemple [HiSi]), qui permet de comparer la hauteur d'un polynôme et sa mesure de Mahler :

Proposition 1.2.6. *Soit*

$$P(X_1,\dots,X_n)=\sum_{i=(i_1,\dots,i_n)\in I} a_i X_1^{i_1}\dots X_n^{i_n}\in\mathbb{C}[X_1,\dots,X_n]$$

On note $d_i=\deg_{X_i}(P)$

$$\forall i\in I,\ |a_i|\leq 2^{d_1+\dots+d_n}M(P)$$

et

$$M(P)\leq[(d_1+1)\dots(d_n+1)]^{1/2}\max_{i\in I}|a_i|.$$

Donnons en corollaire les estimations obtenues pour un polynôme à coefficients entiers et primitif :

Corollaire 1.2.7. *Soit* $P\in\mathbb{Z}[X_1,\dots,X_n]$ *un polynôme primitif de degré total* d*. Alors*

$$(1+d)^{-n/2}M(P)\leq H(P)\leq 2^{nd}M(P)$$

De plus, la mesure de Mahler est multiplicative, ce qui permet d'estimer facilement la hauteur d'un produit en fonction des hauteurs de ses facteurs :

Proposition 1.2.8. *Soient* $P_1,P_2\in\mathbb{Z}[X_1,\dots,X_n]$ *des polynômes primitifs. Alors*

$$h(P_1)\leq h(P_1)+h(P_2)\leq h(P_1P_2)+n\deg(P_1P_2)$$

1.2.2 Inégalités de Cauchy

Rappelons également les inégalités de Cauchy qui serviront plusieurs fois.

Soit $y=\sum_{n\geq 0}a_nz^n$ une série entière de rayon de convergence R. On a le résultat suivant :

Proposition 1.2.9. *Pour tout* $r<R$*, on a*

$$|a_n|\leq\frac{\sup_{|z|=r}|y(z)|}{r^n},\ \forall n\in\mathbb{N}.$$

1.2.3 Majorations des coefficients d'une série formelle algébrique

Dans sa thèse [De1], P. Dèbes donne de telles estimations dans un corps de nombres et pour toute valuation. Nous allons donner ici l'énoncé et la démonstration dans le cas rationnel et pour la valeur absolue usuelle.

Proposition 1.2.10. *Soient $A \in \mathbb{Z}[T,Y]$ un polynôme non nul primitif et $y = \sum_{m\geq 0} y_m T^m$ une série formelle à coefficients y_m dans $\overline{\mathbb{Q}}$ vérifiant $A(T,y) = 0$. On a les majorations suivantes :*

$$|y_m| \leq \gamma_1 \gamma_2^{m+d_1},$$

$$\text{où } \begin{cases} d_1 = \deg_T A, \\ \gamma_1 = 4(1+d_1)H(A), \\ \gamma_2 = 4(1+d_1)H(A)H(R) \quad \textit{avec } R(T) = Res_Y(A, A'_Y). \end{cases}$$

Preuve. On utilisera les notations suivantes :

$$A(T,Y) = A_{d_2}(T)Y^{d_2} + \cdots + A_1(T)Y + A_0(T)$$

où $A_j(T) = \sum_{i=1}^{d_1} a_{i,j}T^i,\ j = 1,\ldots,d_2$ et $d_2 = \deg_Y A$.

Notons r le rayon de convergence de la série formelle y ; on sait, par un raisonnement classique, montrer que

$$r \geq \Delta = \text{Inf}\{|t|;\ t \in \mathbb{C},\ t \neq 0,\ R(t) = 0\}. \tag{1.1}$$

Soit $\tilde{y}$ la fonction analytique induite par y sur le disque ouvert $D(0,r)$ de $\mathbb{C}$; on va obtenir les majorations désirées en utilisant les inégalités de Cauchy :

$$|y_m| \leq \frac{M(r_0)}{r_0^m}$$

où $0 < r_0 < r$ et $M(r_0) = \text{Sup}_{|t|=r_0}|\tilde{y}(t)|$.

Il reste à estimer $M(r_0)$ et bien choisir r_0.

(1) Estimation de $M(r_0)$

Soient ν l'ordre du polynôme A_{d_2} en 0 et $r_1 = \dfrac{1}{2(1+d_1)H(A)}$. On a alors

Lemme 1.2.11. *Pour tout r_0 tel que $0 < r_0 < r$ et $r_0 \leq r_1$, on a*

$$M(r_0) \leq \frac{4(1+d_1)H(A)}{r_0^\nu}.$$

Preuve. Soit t tel que $|t| < r$ et que $A_{d_2}(t) \neq 0$. Alors $\tilde{y}(t)$ est défini et c'est une racine du polynôme $A(t,Y)$. En utilisant l'inégalité de Liouville, on obtient

$$\tilde{y}(t) \leq \frac{2(1+d_1)H(A)\text{Max}(1,|t|)^{d_1}}{|A_{d_2}(t)|}. \tag{1.2}$$

Nous allons maintenant minorer A_{d_2} sur un cercle centré en O. Par définition de ν, on peut écrire :

$$A_{d_2}(T) = T^{\nu} a_{\nu,d_2}(1 + T\mathcal{A}(T))$$

où $a_{\nu,d_2} \neq 0$ et $\mathcal{A}(T) = \sum_{i>\nu} \frac{a_{i,d_2}}{a_{\nu,d_2}} T^{i-\nu-1}$.

Soit t tel que $|t| = r_0$ vérifie $0 < r_0 \leq r_1$ et $r_0 < r$. On a alors

$$|t\mathcal{A}(t)| \leq \frac{r_0 d_1 H(A)}{|a_{\nu,d_2}|} \leq \frac{1}{2}$$

et donc

$$|A_{d_2}(t)| \geq \frac{|a_{\nu,d_2}| r_0^{\nu}}{2} \geq \frac{r_0^{\nu}}{2}$$

ce qui prouve la majoration. □

(2) Minoration de r

Soient μ l'ordre du polynôme R en 0 et $r_2 = \frac{1}{2H(R)}$.

Lemme 1.2.12. *On a :*

$$r > r_2.$$

Preuve. Notons tout d'abord que l'inégalité est triviale si $r = +\infty$ (on déduit facilement de (1.2), en utilisant la formule de Cauchy, que ceci ne peut arriver que si y est un polynôme). Supposons donc $r < +\infty$; dans ce cas, (1.1) s'écrit

$$r \geq \Delta = \mathrm{Min}\{|t|;\ t \neq 0\ R(t) = 0\}.$$

Pour minorer Δ, on utilise encore l'inégalité de Liouville, mais cette fois sous sa forme permettant de minorer les racines d'un polynôme. On l'applique, non pas au polynôme R dont 0 peut être une racine - et en ce cas l'inégalité qu'on obtient est inintéressante - mais au polynôme $\tilde{R} = R/T^{\mu}$.

Comme $H(\tilde{R}) = H(R)$ et que $\tilde{R}(0) = \delta_{\mu}$, on obtient $\Delta \geq \frac{|\delta_{\mu}|}{2H(R)} \geq \frac{1}{2H(R)}$ et donc la minoration annoncée de r. □

Il suffit désormais d'écrire les inégalités de Cauchy pour $r_0 = r_1 r_2$ et d'utiliser les estimations données par les lemmes ci-dessus pour terminer la preuve de la proposition. □

1.2.4 Les inégalités de Lang-Weil

Un résultat effectif important en géométrie diophantienne sera utilisé pour la deuxième méthode. Il s'agit des estimations suivantes dues à S. Lang et A. Weil sur le nombre de points rationnels sur les courbes algébriques sur les corps finis (voir par exemple [FrJa]).

Théorème 1.2.13. *Soient $\mathbb{F}_q$ un corps fini, $p(T,Y) \in \mathbb{F}_q[T,Y]$ un polynôme absolument irréductible de degré d et C_p la courbe affine C_p : $p(t,y) = 0$. On a alors*

$$q + 1 - (d-1)(d-2)\sqrt{q} - d \leq |C_p(\mathbb{F}_q)| \leq q + 1 + (d-1)(d-2)\sqrt{q}.$$

Ces estimations s'étendent à des variétés de dimension supérieure [LaWe]. Elles constituent une partie des *conjectures de Weil* qui ont été démontrées par Deligne.

1.3 Réduction à la recherche de points sur des courbes algébriques

Cette section va rappeler la réduction standard qui permet de réduire le problème à la recherche de points entiers sur une courbe algébrique dans un carré. Nous apporterons quelques précisions à la forme obtenue par A. Schinzel et U. Zannier en estimant le degré et la hauteur des nouveaux polynômes issus de cette réduction.

1.3.1 Réduction classique

Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ de degré d. On notera $m = \deg_T(F)$ et $n = \deg_Y(F)$. On écrit sa décomposition dans $\overline{\mathbb{Q}(T)}[Y]$

$$F(T,Y) = a_0(T) \prod_{i=1}^{n} (Y - y_i)$$

et soit $D(T)$ le discriminant de F par rapport à Y. Pour tout sous-ensemble ω de $\{1,\ldots,n\}$, et pour tout entier positif $j \leq \sharp\omega$, on note $P_{\omega,j}(T,Y)$ le polynôme minimal de $a_0(T)\tau_j(y_i : i \in \omega)$ sur $\mathbb{Q}(T)$, où τ_j est la j-ième fonction symétrique fondamentale. On sait alors que $a_0(T)\tau_j(y_i : i \in \omega)$ est entier sur $\mathbb{Z}[T]$ et donc $P_{\omega,j}$ est un polynôme à coefficients entiers, unitaire en Y (et donc également primitif).

Lemme 1.3.1. *Soit $t \in \mathbb{Z}$ tel que $a_0(t)D(t) \neq 0$ et $F(t,Y)$ est réductible sur $\mathbb{Q}$, alors il existe un sous-ensemble ω de $\{1,\dots,n\}$ et un $j \leq \sharp\omega$ tels que $\deg_Y(P_{\omega,j}) \geq 2$ et $P_{\omega,j}(t,Y)$ a un zéro entier y. On notera P_ω ce polynôme et d_ω son degré en Y.*

Preuve. Soit $t \in \mathbb{Z}$ tel que $a_0(t)D(t) \neq 0$ et $F(t,Y)$ est réductible sur $\mathbb{Q}$. Il existe alors un morphisme de spécialisation

$$\varphi_t \ : \ \mathbb{Q}[T, y_1, \dots, y_n] \to \overline{\mathbb{Q}}$$

qui prolonge la spécialisation $T \to t$ (pour $z \in \mathbb{Q}[T, y_1, \dots, y_n]$, on notera $z(t)$ l'image de z par ce morphisme) et une décomposition du type

$$F(t,Y) = a_0(t) \prod_{i \in \omega} (Y - y_i(t)) \prod_{i \notin \omega} (Y - y_i(t))$$

où $\omega \subset \{1,\dots,n\}$ et $R(Y) = a_0(t) \prod_{i \in \omega} (Y - y_i(t)) \in \mathbb{Z}[Y]$.

Les coefficients de ce $R(Y)$ sont les $a_0(t)\tau_j(y_i(t) : i \in \omega),\ j = 1, \dots, \sharp\omega$. Un d'eux au moins vérifie la condition suivante : $a_0(T)\tau_j(y_i : i \in \omega) \in \overline{\mathbb{Q}(T)} \backslash \mathbb{Q}(T)$ car sinon $F(T,Y)$ serait réductible sur $\mathbb{Q}$. On note θ_ω cet élément et $P_\omega(T,Y)$ son polynôme minimal sur $\mathbb{Q}(T)$. On a alors les propriétés suivantes :

- le polynôme P_ω est à coefficients entiers et est unitaire en Y,
- $d_\omega := \deg_Y(P_\omega) \geq 2$ car sinon $\theta_\omega \in \mathbb{Q}(T)$,
- l'équation $P_\omega(t,Y) = 0$ a une solution dans $\mathbb{Z}$: $\theta_\omega(t)$.

□

1.3.2 Estimation des nouveaux polynômes

On peut préciser les grandeurs associées aux polynômes P_ω :

Lemme 1.3.2. *Les polynômes P_ω définis dans le lemme 1.3.1 ont les propriétés suivantes :*

(i) $2 \leq d_\omega \leq 2^n$,

(ii) $\deg(P_\omega) \leq m d_\omega$,

(iii) $H(P_\omega) \leq (2^{n+1}(m+1)H(F))^{d_\omega}$.

Preuve. Le fait que $d_\omega \geq 2$ provient du lemme précédent. Pour la majoration, on remarque que le polynôme

$$\prod_{\sharp\omega = k} \Big(Y - a_0(T)\tau_j(y_i : i \in \omega) \Big)$$

est à coefficients dans $\mathbb{Q}$ et de degré en Y inférieur à 2^n. Comme P_ω divise ce polynôme, on a $d_\omega \leq 2^n$ ce qui prouve (i).

Pour la même raison, on voit que les zéros de $P_\omega(t, Y)$ sont des fonctions symétriques élémentaires d'un sous-ensemble des racines de $F(t, Y)$ ce qui va nous permettre, *via* les outils décrits dans la section 1.2, de majorer la hauteur de P_ω en fonction des données de F.

D'après les inégalités de Cauchy, on a

$$H(P_\omega) \leq \sup_{|z|\leq 1} ||P_\omega(z, Y)||,$$

où $||P_\omega(z, Y)||$ désigne le maximum des modules des coefficients de $P_\omega(z, Y) \in \mathbb{C}[Y]$. En effet, si $P_\omega = \sum_{i=0}^{d_\omega} p_i(Z)Y^i$ avec $p_i(Z) = \sum_j p_{i,j}Z^j$, on a, pour tout i, j,

$$|p_{i,j}| = |p_i^{(j)}(0)/j!| \leq \sup_{|z|\leq 1} |p_i(z)| \leq \sup_{|z|\leq 1} ||P_\omega(z, Y)||.$$

On rappelle la mesure de Mahler de $P_\omega(z, Y)$:

$$M(P_\omega(z, Y)) = \prod_{i=1}^{d_\omega} \max\{1, |\alpha_i(z)|\},$$

où $d_\omega = \deg_Y P_\omega$ et les $\alpha_i(z)$ sont les zéros de $P_\omega(z, Y)$.

On a alors l'inégalité classique (voir le théorème 1.2.6)

$$||P_\omega(z, Y)|| \leq 2^{d_\omega} M(P_\omega(z, Y)).$$

Il reste à estimer $|\alpha_i(z)|$ pour $|z| \leq 1$. On utilise pour cela le fait que $\alpha_i(z)$ est une fonction symétrique élémentaire de zéros de $F(z, Y)$ pour écrire

$$|\alpha_i(z)| \leq 2^l |a_0(z)| \prod_{i=1}^{n} \max\{1, |y_i(z)|\}$$

où $l = \sharp\omega$ et les $y_i(z)$ sont les zéros de $F(z, Y)$, vu comme polynôme en Y. L'autre partie de l'inégalité du théorème 1.2.6 nous donne

$$|a_0(z)| \prod_{i=1}^{n} \max\{1, |y_i(z)|\} = M(F(z, Y)) \leq \sqrt{n+1} \max_i(|a_i(z)|)$$

où les $a_i(z)$ sont les coefficients de $F(z, Y)$ vu comme polynôme en Y. Cela, joint aux majorations

$$|a_i(z)| \leq (m+1)H(F), \quad i = 1, \ldots, n$$

conduit à l'estimation suivante pour $|\alpha_i(z)|$, $|z| \leq 1$:

$$|\alpha_i(z)| \leq 2^l \sqrt{n+1}(m+1)H(F)\max(1,|z|)^m \leq 2^n(m+1)H(F)$$

On obtient donc l'estimation (iii) :

$$H(P_\omega) \leq (2^{n+1}(m+1)H(F))^{d_\omega}.$$

Il nous reste à majorer le degré en T de P_ω. On écrit

$$P_\omega(T,Y) = Y^{d_\omega} + \sum_{i=1}^{d_\omega} P_i(T)Y^{d_\omega - i}.$$

Pour $t \in \mathbb{C}$ fixé, $P_i(t)$ est, au signe près, la i-ème fonction symétrique élémentaire en les zéros de $P_\omega(t,Y)$. Cette observation fournit, pour $|t| \geq 1$, la majoration suivante :

$$|P_i(t)| \leq 2^i 2^{ni}(m+1)^i H(F)^i |t|^{mi} = O(|t|^{mi}),$$

qui prouve que $\deg P_i \leq mi$ et donc

$$\deg P_\omega \leq \max_{0 \leq i \leq d_\omega} (d_\omega - i + \deg P_i) \leq m d_\omega.$$

□

Remarque 1.3.3. *Le nombre de ces nouveaux polynômes P_ω est le nombre de parties de l'ensemble $\{1,\ldots,n\}$ à l éléments. Il est inférieur à 2^n.*

1.3.3 Reformulation du problème

L'idée générale est d'utiliser cette réduction pour compter le nombre de spécialisations qui rendent le polynôme réductible. En effet, si on note

$$S(B) = \sharp\{t \leq B \mid t \in \mathbb{N},\ a_0(t)D(t) \neq 0 \text{ et } F(t,Y) \text{ est réductible sur } \mathbb{Q}\},$$

et

$$S_\omega(B) = \sharp\{t \leq B \mid t \in \mathbb{N},\ a_0(t)D(t) \neq 0 \text{ et } P_\omega(t,Y) \text{ a une racine dans } \mathbb{Z}\},$$

alors on a la majoration

$$S(B) \leq \sum_\omega S_\omega(B).$$

L'intérêt de cette réduction est qu'elle permet de se ramener au problème mieux connu de la recherche de points entiers sur des courbes algébriques. Nous disposons donc désormais de tous les outils de la géométrie diophantienne pour tenter d'estimer $S(B)$.

Cependant, cette réduction est coûteuse puisque les nouveaux polynômes sont de degré, hauteur et en nombre plus grands que le poynôme de départ. Nous verrons par la suite comment essayer d'améliorer cette réduction sous des hypothèses supplémentaires.

Notons qu'une version effective du théorème de Siegel donnerait directement, *via* cette réduction, un énoncé effectif pour le théorème d'irréductibilité de Hilbert.

Chapitre 2

Méthode de Dörge

La première tentative dans la recherche d'une nouvelle forme effective du théorème d'irréductibilité de Hilbert est de reprendre la preuve de Hilbert sous sa forme revue et simplifiée par Dörge [Do] afin de la rendre effective. Celle-ci repose sur l'utilisation du théorème de Puiseux et d'un argument d'interpolation. Les outils employés sont relativement basiques et mènent à un résultat effectif, mais qui n'améliore malheureusement pas les résultats déjà connus. On notera cependant que cette méthode, datant de 1927, pouvait être rendue explicite et cela bien avant les premiers résultats dans ce sens de P. Dèbes et de A. Schinzel et U. Zannier.

2.1 Réduction aux séries de Puiseux

Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ un polynôme à coefficients entiers, primitif et irréductible sur $\mathbb{Q}$. Le but est de trouver une borne pour une spécialisation qui laisse le polynôme irréductible. Pour cela, nous allons compter les spécialisations inférieures à une borne B telles que le polynôme spécialisé $P(t,Y)$ est réductible sur $\mathbb{Q}$.

La méthode de Dörge utilise tout d'abord la réduction classique exposée dans le chapitre précédent, ce qui nous ramène à compter

$$S_\omega(B) = \sharp\{t \leq B \mid t \in \mathbb{N},\ a_0(t)D(t) \neq 0 \text{ et } P_\omega(t,Y) \text{ a une racine dans } \mathbb{Z}\}$$

où $P_\omega(T,Y)$ est un polynôme à coefficients entiers, unitaire en Y, irréductible sur $\mathbb{Q}$ et de degré en Y, noté d_ω, supérieur ou égal à 2.

D'après le théorème de Puiseux dont nous donnerons une version effective dans la section suivante, on peut écrire les solutions dans $\overline{\mathbb{Q}(T)}$ de $P_\omega(T,Y) = 0$ sous la forme de séries de Laurent en $(1/T)^{1/e}$ convergeant pour $t > \tau$; on

les notera $\varphi_1, \ldots, \varphi_{d_\omega}$. On a alors

$$S_\omega(B) \leq \sum_{i=1}^{d_\omega} \sharp V_{\varphi_i}(B) + \tau$$

où

$$V_{\varphi_i}(B) := \{t \leq B \mid t \in \mathbb{N},\ t > \tau \text{ et } \varphi_i(t) \in \mathbb{Z}\}.$$

Nous verrons que la condition $t > \tau$ assurera que $a_0(t)D(t) \neq 0$. Notons également que φ_i ne peut pas être un polynôme (car P_ω est irréductible). La méthode de Dörge se ramène à démontrer l'énoncé suivant :

Théorème 2.1.1 (Lemme de Dörge). *Soient k un entier quelconque, e un entier positif non nul, et*

$$\varphi(T) = T^{k-1} \sum_{l=0}^{\infty} c_l (1/T)^{l/e}$$

une série de Laurent en $(1/T)^{1/e}$ à coefficients complexes convergeant pour tout $t > \tau$. On suppose également que $\varphi(T)$ est racine d'un polynôme $P(T, Y)$ de degré D, unitaire en Y, et n'est pas un polynôme. Alors il existe $\delta > 0$ tel que le nombre d'entiers dans $V_\varphi(B)$ est un $O(B^{1-\delta})$.

2.2 Théorème de Puiseux effectif

Nous allons dans cette section donner une version effective du théorème de Puiseux. L'énoncé général de ce théorème pour les séries formelles nous dit que les extensions finies de $\mathbb{C}((u))$ sont kummériennes, de la forme $\mathbb{C}((u))(u^{1/e})$ $= \mathbb{C}((u^{1/e}))$. Il s'énonce également pour les séries de Laurent convergentes : les extensions finies de $\mathbb{C}\{\{u\}\}$ sont kummériennes, de la forme $\mathbb{C}\{\{u\}\}(u^{1/e}) = \mathbb{C}\{\{u^{1/e}\}\}$. On en déduit l'énoncé suivant :

Théorème 2.2.1. *Soit $P(T, Y) \in \mathbb{Z}[T, Y]$ un polynôme primitif de degrés partiels m en T et n en Y et de hauteur absolue H. Il existe n séries de Puiseux formelles $\varphi_1, \ldots, \varphi_n$, des entiers $e_1, \ldots, e_n$ strictement positifs et un nombre réel $\tau > 0$ tels que*

- *$\forall i \in \{1, \ldots, n\}$, φ_i est une série de Laurent en $(1/T)^{1/e_i}$ convergeant pour $t > \tau$,*
- *pour tout $(t, y) \in \mathbb{R}^2$ tel que $P(t, y) = 0$ et $t > \tau$, il existe $i \in \{1, \ldots, n\}$ tel que $y = \varphi_i(t)$.*

On notera

$$\varphi(T) = T^{k-1} \sum_{l=0}^{\infty} c_l (1/T)^{l/e}$$

(où k est le plus petit entier qui permet cette écriture) une de ces solutions, et on va estimer les quantités k, e, τ ainsi que les coefficients c_l.

2.2.1 Premières estimations

Valuation

On considère le corps $\mathbb{Q}(T)$ muni de la valuation $1/T$-adique. Celle-ci est définie de la façon suivante : $f(T) \in \mathbb{Q}(T)$ s'écrit de manière unique $f(T) = T^n \dfrac{a(1/T)}{b(1/T)}$, avec $a(0) \neq 0$ et $b(0) \neq 0$; on pose $v_{1/T}(f) = -n$.

On applique l'inégalité de Liouville (voir proposition 1.2.5) à la solution φ de l'équation $P(T, Y) = 0$ et au prolongement naturel de la valuation $1/T$-adique à $\overline{\mathbb{Q}}(((1/T)^{1/e}))$, on obtient :

$$k - 1 \leq \deg_T(P)$$

Ramification

Le théorème de Puiseux dans sa forme générale nous dit que $\mathbb{C}((u))(\varphi) = \mathbb{C}((u^{1/e}))$ avec $e = [\mathbb{C}((u))(\varphi) : \mathbb{C}((u))] \leq [\mathbb{C}(u)(\varphi) : \mathbb{C}(u)] = \deg_Y(P)$.

2.2.2 Estimation des coefficients

Pour cette partie, nous utiliserons les estimations des coefficients d'une série formelle solution d'une équation algébrique données dans le premier chapitre (proposition 1.2.10) que nous allons adapter au cas d'une série de Laurent.

L'idée est donc de chercher à quelle équation satisfait la série formelle $\psi(T) = \sum_{l \geq 0} c_l T^l$, où les c_l sont les coefficients de φ. On a :

$$P(T, \varphi(T)) = 0 \Leftrightarrow P\left(\frac{1}{T^e}, \frac{1}{T^{e(k-1)}} \psi(T)\right) = 0$$

ce qui nous permet de dire que si on note $P(T, Y) = P_0(T) + \cdots + P_n(T) Y^n$ avec $P_j(T) = \sum_{i=0}^{m} p_{i,j} T^i$, alors $\psi(T)$ est solution de $A(T, \psi(T)) = 0$ avec $A(T, Y) = A_0(T) + \cdots + A_{n'}(T) Y^{n'}$ et $A_j(T) = T^{e(k-1)(n-j)} \sum_{i=0}^{m} p_{m-1,j} T^{ei}$.

Le polynôme A ainsi construit est clairement à coefficients entiers et primitif. De plus, on a les estimations suivantes :
- $n' := \deg_Y(A) = n$,
- $m' := \deg_T(A) = e(m + n(k-1))$,
- $H(A) = H(P)$.

Afin d'appliquer la proposition 1.2.10, on doit encore estimer la hauteur du discriminant $R(T)$ de $A(T,Y)$ par rapport à Y. Pour cela, il suffit d'utiliser l'écriture de R comme déterminant et d'utiliser les propriétés de la hauteur. On trouve dans [De3] le résultat suivant (proposition 3.5 p.130) :

Proposition 2.2.2. *Soient K un corps de nombre et $A, B \in K[Y_1, \ldots, Y_n]$ deux polynômes tels que $\deg_{Y_1}(A), \deg_{Y_1}(B) > 0$. On pose $R = Res_{Y_1}(A,B)$. Alors*

$$h(R) \leq \deg(A)h(B) + \deg(B)h(A) + n\deg(AB)\log(\deg(AB))$$

En l'appliquant aux polynômes A et A'_Y, on en déduit que

$$H(R) \leq H^{6d^3} d^{90d^3}.$$

On peut donc utiliser les estimations de la proposition 1.2.10 et en déduire les estimations suivantes des c_l :

$$|c_l| \leq \gamma_1 \gamma_2^{l+2d^3}$$

avec $\begin{cases} \gamma_1 = 16d^3H \\ \gamma_2 = 16d^{91d^3} H^{7d^3} \end{cases}$

2.2.3 Estimation de τ

On considère, comme pour l'estimation des coefficients, la série entière $\psi(T) = \sum_{l \geq 0} c_l T^l$ dont on notera r le rayon de convergence. Celui-ci est relié à τ de la façon suivante : $\tau = 1/r^e$. Il suffit donc de minorer r dans le cas où r est fini. Or, on a classiquement

$$r \geq \Delta := \min\{|t| \mid t \in \mathbb{C},\ t \neq 0 \text{ et } R(t) = 0\}.$$

Pour minorer Δ, on utilise l'inégalité de Liouville appliquée au polynôme $\tilde{R}(T) = \dfrac{R(T)}{T^\mu}$ où μ est l'ordre en 0 de R. On obtient alors, en notant δ_μ le coefficient constant de $\tilde{R}$,

$$\Delta \geq \frac{|\delta_\mu|}{2H(R)}$$

ou encore

$$\Delta \geq \frac{1}{2H(R)}$$

et donc

$$\tau \leq (2H(R))^e \leq (2H(R))^d \leq d^{91d^4} H^{6d^4}.$$

2.2.4 Théorème de Puiseux effectif

Nous sommes donc en mesure désormais d'énoncer une version effective du théorème de Puiseux :

Théorème 2.2.3. *Soit $P(T,Y) \in \mathbb{Z}[T,Y]$ un polynôme primitif de degré partiel m en T et n en Y et de hauteur absolue H. Il existe n séries de Puiseux formelles $\varphi_1, \ldots, \varphi_n$, des entiers $e_1, \ldots, e_n$ strictement positifs et un nombre réel $\tau > 0$ tels que*

- *$\forall i \in \{1, \ldots, n\}$, φ_i est une série de Laurent en $(1/T)^{1/e_i}$ convergeant pour $t > \tau$,*
- *pour tout $(t,y) \in \mathbb{R}^2$ tel que $P(t,y) = 0$ et $t > \tau$, il existe $i \in \{1, \ldots, n\}$ tel que $y = \varphi_i(t)$.*

De plus, on a les estimations suivantes :

- *$e_i \leq n$, $\forall i = 1, \ldots, n$*
- *$-v_{1/T}(\varphi) \leq m$*
- *$\tau \leq d^{91d^4} H^{6d^4}$*
- *en notant c_l le coefficient du terme T^{l/e_i}, on a $|c_l| \leq \gamma_1 \gamma_2^{l+2d^3}$ avec $\begin{cases} \gamma_1 = 16d^3H \\ \gamma_2 = 16d^{91d^3} H^{7d^3} \end{cases}$*

Remarque 2.2.4. *Il existe une méthode constructive pour trouver les coefficients des séries de Puiseux solution d'une équation algébrique. Cette méthode est basée sur l'utilisation du polygône de Newton (voir [Ay]).*

2.3 Lemme de Dörge effectif

Dans cette section, nous allons donner une version effective du théorème 2.1.1 (lemme de Dörge). Soit donc

$$\varphi(T) = T^{k-1} \sum_{l=0}^{\infty} c_l (1/T)^{l/e}$$

une série de Puiseux solution de $P(T,Y) = 0$. Il s'agit d'estimer le nombre de spécialisations $t < B$ telles que $\varphi(t)$ prenne des valeurs entières. Pour cela, nous allons d'abord montrer que de telles spécialisations ne peuvent être trop proches.

2.3.1 Écartement des points de $V_\varphi(B)$

On considère $k+1$ points de $V_\varphi(B)$, $t_0, \ldots, t_k$, pris entre deux solutions consécutives de $\varphi^{(k)}(T) = 0$. Nous allons montrer que

$$\exists\ c > 0 \text{ et } \alpha > 0 \text{ tels que } t_k - t_0 \geq c t_0^\alpha.$$

On pose $x_i = \varphi(t_i)$ pour $i = 0, \ldots, k$ et on considère le polynôme d'interpolation $I(T) \in \mathbb{R}[T]$ de degré k vérifiant $I(t_i) = x_i,$ pour $i = 0, \ldots, k$

$$I(T) = \sum_{i=0}^{k} x_i \prod_{j \neq i} \frac{T - t_j}{t_i - t_j}$$

Alors la fonction $\varphi - I$ s'annule en $t_0, \ldots, t_k$. D'après le théorème de Rolle (appliqué k fois), on sait qu'il existe $\xi \in [t_0, t_k]$ tel que $\varphi^{(k)}(\xi) = I^{(k)}(\xi)$, c'est-à-dire

$$\varphi^{(k)}(\xi) = k! \sum_{i=0}^{k} \frac{x_i}{\prod_{j \neq i}(t_i - t_j)}$$

Ce nombre est un nombre rationnel, dont un dénominateur est

$$\prod_{0 \leq i < j \leq k} |t_i - t_j| < (t_k - t_0)^{\frac{k(k+1)}{2}}$$

et donc

$$|\varphi^{(k)}(\xi)|(t_k - t_0)^{\frac{k(k+1)}{2}} \geq 1$$

car on s'est placé sur un intervalle sur lequel on est assuré que $\varphi^{(k)}(\xi) \neq 0$.

D'autre part, notons le fait que le développement de $\varphi^{(k)}(T)$ ne comporte que des puissances négatives de T. On a donc $|\varphi^{(k)}(t)| \sim \gamma t^{-\mu}$ avec $\gamma > 0$ et $\mu > 0$. Afin de rendre le lemme effectif, nous devrons préciser μ et γ.

On peut ensuite trouver un γ' tel que, pour t assez grand, $|\varphi^{(k)}(t)| \leq \gamma' t^{-\mu}$. Ceci nous donne

$$1 \leq |\varphi^{(k)}(\xi)|(t_k - t_0)^{k(k+1)/2} \leq \gamma' t_0^{-\mu}(t_k - t_0)^{k(k+1)/2}.$$

En posant $\alpha = \dfrac{2\mu}{k(k+1)}$ et $c = (1/\gamma')^{2/k(k+1)}$, cela conduit à

$$t_k - t_0 \geq c t_0^\alpha.$$

2.3.2 Première conclusion : preuve non effective

Notons $(I_i)_{i\in I}$ les intervalles entre deux solutions successives de $\varphi^{(k)}(T) = 0$. On vient de montrer que, pour t assez grand, chacun des intervalles $I_i \cap [t, t + ct^\alpha]$ contient au plus $k + 1$ points dans V_φ. Dans la section suivante, nous montrerons que le nombre de racines de $\varphi^{(k)}$ peut être majoré par une constante $N(k, d)$ ne dépendant que de k et d.

On peut donc conclure que chaque intervalle $[t, t + ct^\alpha]$ contient au plus $(k + 1)N(k, d)$ points dans V_φ.

Pour obtenir l'estimation annoncée, on procède de la façon suivante. Soit $\kappa \in]0, 1[$ et B assez grand. On coupe l'intervalle $[0, B]$ en $[0, B^\kappa]$ et $[B^\kappa, B]$, puis $[B^\kappa, B]$ en intervalles égaux de longueur inférieure à $cB^{\kappa\alpha}$. D'après ce qui précède, chacun des sous-intervalles de $[B^\kappa, B]$ contient au plus $N(k, d)(k+1)$ éléments de V_φ. Donc l'intervalle $[0, B]$ contient au plus

$$B^\kappa + N(k, d)(k + 1)\frac{B}{cB^{\kappa\alpha}} \tag{2.1}$$

éléments de V_φ. Si on prend $\kappa = 1/(1 + \alpha)$, alors $0 < \kappa < 1$ et le nombre considéré ci-dessus est un $O(B^\kappa)$. Pour rendre ce résultat effectif, il suffira de donner une majoration de κ et une minoration de c, ce que nous ferons à la section 2.3.4 .

2.3.3 Nombre de zéros de $\varphi^{(k)}$

Notations On note C le modèle projectif lisse de la courbe définie par l'équation $P(t, y) = 0$. On considère φ comme une fonction rationnelle sur C, et on note (φ) le diviseur de φ

$$(\varphi) = \sum_{i=1}^{\alpha_i} n_i P_i - \sum_{j=1}^{\beta_j} m_j Q_j$$

où les P_i et les $Q_j \in C$ sont respectivement les zéros et pôles de φ, et les n_i et m_j leurs multiplicités.

Soient

$$\deg^+((\varphi)) = \sum_{i=1}^{\alpha_i} n_i \qquad \text{qui représente le nombre de zéros de } \varphi$$

$$\deg^-((\varphi)) = \sum_{j=1}^{\beta_j} m_j \qquad \text{qui représente le nombre de pôles de } \varphi$$

On sait que ces degrés sont égaux et qu'ils valent également $[\bar{\mathbb{Q}}(C) : \bar{\mathbb{Q}}(\varphi)]$. On définit alors le degré de φ de la façon suivante :

$$\deg(\varphi) = \deg^+((\varphi)) = \deg^-((\varphi)) = [\bar{\mathbb{Q}}(C) : \bar{\mathbb{Q}}(\varphi)] = \deg_T P$$

On notera également g_φ le genre de la courbe C et en un point Q de C, $e_\varphi(Q)$ l'indice de ramification de φ en Q.

On peut désormais énoncer le lemme suivant :

Lemme 2.3.1. *Soit $P(T, Y) \in \mathbb{Q}[T, Y]$ un polynôme irréductible de degré d. Soit $\varphi(T) \in \mathbb{C}((1/T))$ une solution de $P(T, \varphi(T)) = 0$ convergeant pour $t > \tau$.*

Alors pour tout entier positif k, le nombre de zéros de $\varphi^{(k)}(T)$ dans $]\tau, +\infty[$ est inférieur à $2^{k+2}d^2$.

Preuve. Résolvons tout d'abord le cas $k = 1$. On cherche à estimer le nombre de racines de $\varphi'(T)$ dans $]\tau; +\infty[$. Ce nombre est inférieur au nombre de zéros distincts de la fonction algébrique $\dfrac{\mathrm{d}\varphi}{\mathrm{d}T}$ qui n'est rien d'autre que

$$\deg^+\left((\frac{\mathrm{d}\varphi}{\mathrm{d}T})\right) \leq \deg^+((\mathrm{d}\varphi)) + \deg^-((\mathrm{d}T))$$

On estime $\deg^+((\mathrm{d}\varphi))$:

$$\begin{array}{rcl} \deg^+((\mathrm{d}\varphi)) & = & \sum_{a\neq\infty} \sum_{Q\in\varphi^{-1}(a)} (e_\varphi(Q) - 1) \\ & \leq & \sum_{Q\in\mathcal{C}} (e_\varphi(Q) - 1) \\ & \leq & 2g_\varphi - 2 + 2[\bar{\mathbb{Q}}(T, \varphi) : \bar{\mathbb{Q}}(\varphi)] \end{array}$$

par la formule de Riemann-Hurwitz. Puis $\deg^-((\mathrm{d}T))$:

$$\begin{array}{rcl} \deg^-((\mathrm{d}T)) & = & \sum_{Q\in T^{-1}(\infty)} |\mathrm{ord}_Q(1/T)| + 1 \\ & \leq & 2[\bar{\mathbb{Q}}(T, \varphi) : \bar{\mathbb{Q}}(T)] \end{array}$$

On obtient donc que si φ est algébrique sur $\bar{\mathbb{Q}}(T)$, alors le nombre de racines de $\varphi'(T)$ dans $]\tau; +\infty[$ est inférieur à

$$2g_\varphi - 2 + 2[\bar{\mathbb{Q}}(T, \varphi) : \bar{\mathbb{Q}}(T)] + 2[\bar{\mathbb{Q}}(T, \varphi) : \bar{\mathbb{Q}}(\varphi)]$$

On applique ensuite ce résultat à $\varphi^{(k-1)}$ et on majore ainsi le nombre de racines de $\varphi^{(k)}(T)$ dans $]\tau; +\infty[$ par

$$2g_{\varphi^{(k-1)}} - 2 + 2[\bar{\mathbb{Q}}(t, \varphi^{(k-1)}) : \bar{\mathbb{Q}}(T)] + 2[\bar{\mathbb{Q}}(T, \varphi^{(k-1)}) : \bar{\mathbb{Q}}(\varphi^{(k-1)})]$$

Comme $\varphi^{(k-1)}$ est dans $\bar{\mathbb{Q}}(T,\varphi)$, on a

$$[\bar{\mathbb{Q}}(T,\varphi^{(k-1)}) : \bar{\mathbb{Q}}(T)] \leq [\bar{\mathbb{Q}}(T,\varphi) : \bar{\mathbb{Q}}(T)] \leq \deg_Y(P)$$

et

$$2g_{\varphi^{k-1}} \leq 2g_\varphi \leq (d-1)(d-2)$$

Pour majorer $[\bar{\mathbb{Q}}(T,\varphi^{(k-1)}) : \bar{\mathbb{Q}}(\varphi^{(k-1)})]$, on va chercher à construire un polynôme $F(T,Y,Z) \in \mathbb{Q}[T,Y,Z]$ vérifiant $F(T,\varphi,\varphi^{(k-1)}) = 0$. Le résultant $R(T,Z)$ de F et P par rapport à Y vérifiera alors : $R(T,\varphi^{(k-1)}) = 0$ puisque $P(T,Y)$ et $F(T,Y,\varphi^{(k-1)})$ ont la racine commune φ. On pourra donc conclure que R est un multiple du polynôme minimal de T sur $\mathbb{Q}(\varphi^{(k-1)})$ et donc $[\bar{\mathbb{Q}}(T,\varphi^{(k-1)}) : \bar{\mathbb{Q}}(\varphi^{(k-1)})] \leq \deg(R) \leq 2\deg(F)\deg(P)$.

Par dérivations successives de l'égalité $P(T,\varphi) = 0$, on obtient des polynômes P_i et Q_i tels que

$$P_i(T,\varphi) + \varphi^{(i)}Q_i(T,\varphi) = 0.$$

On montre qu'ils vérifient les relations de récurrence suivantes :

$$P_{i+1} = P'_T Q_i P'_{iT} - P'_Y Q_i P'_{iY} - P'_T P_i Q'_{iT} + P'_Y P_i Q'_{iY}$$

$$Q_{i+1} = P'_T Q_i^2$$

On pose alors $F(T,Y,Z) = P_{k-1}(T,Y) + ZQ_{k-1}(T,Y)$, et les relations ci-dessus nous permettent d'estimer le degré de F. On obtient alors après calculs :

$$[\bar{\mathbb{Q}}(T,\varphi^{(k-1)}) : \bar{\mathbb{Q}}(\varphi^{(k-1)})] \leq 2^k d^2$$

Finalement, le nombre de racines de $\varphi^{(k)}$ est majoré par $2^{k+2}d^2$. □

2.3.4 Estimations

Évaluation de μ

On considère désormais T comme une variable et on cherche un équivalent de $|\varphi^{(k)}(T)|$ sous la forme $\gamma T^{-\mu}$.

Pour cela, on introduit la fonction

$$\psi(T) = \varphi(T) - \{c_0 T^{k-1} + c_e T^{k-2} + \cdots + c_{e(k-1)}\}.$$

(on enlève la partie polynomiale de φ car sa dérivée $k-$ième est nulle)

$\psi(T)$ est racine du polynôme $Q(T,Y) = P(T, Y + c_0 T^{k-1} + c_e T^{k-2} + \cdots + c_{e(k-1)})$. On peut donc, grâce aux résultats de la section 2.2 sur les

développements de Puiseux, évaluer la valuation de $\psi(T)$. En dérivant ce terme k fois, on obtient un équivalent à l'infini de $\psi^{(k)}(T)$ de la forme $\gamma T^{-\mu}$. En utilisant ensuite le fait que $\varphi^{(k)}(T) = \psi^{(k)}(T)$, on obtient le résultat souhaité.

D'après la partie sur les développements de Puiseux, on sait que, si $\psi(T)$ est une solution de $Q(T, Y) = 0$, alors la valuation μ_0 de $\psi(T)$ est majorée par $\deg_T(Q)$. On a donc

$$\mu_0 \leq \deg_T(Q) \leq \deg_T(P) + \deg_Y(P)(k-1) \leq 2d^2$$

En dérivant $\psi(T)$ k fois, on a donc

$$\mu \leq \mu_0 + k \leq 3d^2.$$

Afin d'obtenir une minoration de μ, il suffit de voir que μ est une puissance positive de T et fractionnaire de dénominateur e. On a donc

$$\mu \geq 1/e \geq 1/d.$$

Évaluation de l'exposant κ apparaissant dans (2.1)

On a $\alpha = \dfrac{2\mu}{k(k+1)}$. De plus, on sait que $k \leq \deg_T(P) \leq d$ et que $\mu \geq 1/d$. Donc

$$\alpha \geq 1/d^3,$$

ce qui nous permet de majorer $\kappa = \dfrac{1}{1+\alpha}$:

$$\kappa \leq \frac{d^3}{d^3+1}.$$

D'autre part, on a trivialement

$$\alpha = \frac{2\mu}{k(k+1)} \leq \mu \leq 3d^2,$$

et donc

$$1/\kappa \leq 1 + 3d^2.$$

Minoration de c

On écrit

$$\varphi(T) = \sum_{l \geq 0} c_l T^{n-1-l/e}.$$

On dérive k fois (rappelons que les coefficients jusqu'à $l = e(\mu - 1)$ sont nuls) :

$$\varphi^{(k)}(T) = T^{-\mu} \sum_{l \geq 0} c_l (k - 1 - l/e)(k - 2 - l/e) \dots (-l/e) T^{-1-l/e+\mu}$$

Soit $\tilde{t}$ fixé, dont on discutera la valeur plus tard. Pour tout $t > \tilde{t}$, on a

$$|\varphi^{(k)}(t)| \leq t^{-\mu} \gamma'(\tilde{t})$$

avec

$$\gamma'(\tilde{t}) = \sum_{l \geq 0} |c_l| |k - 1 - l/e| \dots | - l/e| \left(\frac{1}{\tilde{t}^{1/e}} \right)^l \tilde{t}^{\mu - 1}$$

On coupe alors cette somme en deux autour de $e(k-1)$ et on majore, pour $l \leq e(k-1)$, chaque terme $k - i - l/e$ pour $i \in \{1, \dots, k\}$ par $k - 1$, pour $l \geq e(k-1)$, chaque terme $k - i - l/e$ par l/e puis par $\exp(l/e)$ et $|c_l|$ par $\tilde{\gamma_1} \gamma_2^l$ avec $\tilde{\gamma_1} = \gamma_1 \gamma_2^{2d^3}$:

$$\gamma'(\tilde{t}) \leq \underbrace{(k-1)^k \tilde{\gamma_1} \tilde{t}^{\mu-1} \sum_{l=0}^{e(k-1)-1} \left(\frac{\gamma_2}{\tilde{t}^{1/e}} \right)^l}_{A(\tilde{t})} + \underbrace{\tilde{\gamma_1} \tilde{t}^{\mu-1} \sum_{l=0}^{+\infty} \left(\frac{\gamma_2 \exp(k/e)}{\tilde{t}} \right)^l}_{B(\tilde{t})}$$

On choisit désormais $\tilde{t}$ tel que la raison de la série géométrique qui apparaît dans $B(\tilde{t})$ soit $1/2$, c'est-à-dire $\tilde{t} = (2\gamma_2)^e \exp(k)$. On a alors

$$A(\tilde{t}) \leq k^k \tilde{\gamma_1} \tilde{t}^{\mu-1} e(k-1)$$

et

$$B(\tilde{t}) \leq 2 \tilde{\gamma_1} \tilde{t}^{\mu-1}$$

En utilisant les majorations trouvées pour μ, k et les valeurs de γ_1 et $\tilde{t}$, on trouve

$$\gamma' \leq (16)^{12d^3} d^{458d^6} H^{43d^6}$$

et

$$c = (1/\gamma')^{2/k(k+1)} \geq 1/\gamma' \geq (16)^{-12d^3} d^{-458d^6} H^{-43d^6}$$

2.3.5 Conclusion : version effective du lemme de Dörge

On a montré le résultat suivant, qui correspond à une version effective de la conclusion (2.1) :

L'intervalle $[0, B]$ contient au plus

$$(16)^{13d^3} d^{459d^6} H^{43d^6} B^{\frac{d^3}{d^3+1}}$$

éléments de $V_\varphi(B)$ dès que $B > \tau$ et $B^\kappa > \tilde{t}$. Il nous reste à expliciter la deuxième condition sur B en fonction de d et H.

On a $\tilde{t} = (2\gamma_2)^e \exp(k)$, donc avec les majorations de γ_2, e et k, on obtient

$$\tilde{t} \leq d^{92d^4} H^{7d^4}$$

ce qui nous permet de remplacer la condition $B^\kappa > \tilde{t}$ par

$$B > d^{368d^6} H^{28d^6}.$$

On peut désormais énoncer une version effective du lemme de Dörge.

Théorème 2.3.2 (Lemme de Dörge effectif). *Soient e et k deux entiers positifs et*

$$\varphi(T) = T^{k-1} \sum_{l=0}^{\infty} c_l (1/T)^{\frac{l}{e}}$$

une série en $(1/T)^{1/e}$ à coefficients $c_l \in \mathbb{R}$ convergeant pour tout $t \in \mathbb{R}$ supérieur à un nombre réel τ. On suppose également que $\varphi(t)$ est racine d'un polynôme $P(t, Y)$ unitaire en Y et de degré d. Soit

$$V_\varphi(B) = \{t \in \mathbb{Z} \mid B > t > \tau \text{ et } \varphi(t) \in \mathbb{Z}\}$$

Alors le nombre d'entiers dans $V_\varphi(B)$ est inférieur à

$$d^{462d^6} H^{36d^6} B^{\frac{d^3}{d^3+1}}$$

dès que $B > d^{368d^6} H^{28d^6}$.

2.4 Théorème d'irréductibilité de Hilbert effectif

Soit $F(T, Y) \in \mathbb{Z}[T, Y]$ un polynôme irréductible sur $\mathbb{Q}$ de degré en Y supérieur à 1. On note d son degré total et m et n ses degrés partiels en T et Y respectivement. La réduction classique (voir section 1.3) nous donne un nombre N de polynômes notés P_ω, vérifiant :

$$S(B) \leq \sum_{\omega} S_\omega(B),$$

où $S(B)$ et $S_\omega(B)$ sont définis de la façon suivante :

$$S(B) = \sharp\{t \leq B \mid t \in \mathbb{N},\ a_0(t)D(t) \neq 0 \text{ et } F(t,Y) \text{ est réductible sur } \mathbb{Q}\},$$

et

$$S_\omega(B) = \sharp\{t \leq B \mid t \in \mathbb{N},\ a_0(t)D(t) \neq 0 \text{ et } P_\omega(t,Y) \text{ a une racine dans } \mathbb{Z}\}.$$

La version effective du lemme de Dörge, appliquée aux d_ω solutions de $P_\omega(T,Y) = 0$, nous donne une estimation de $S_\omega(B)$:

$$S_\omega(B) \leq D_\omega^{463D_\omega^6} H(P_\omega)^{36D_\omega^6} B^{\frac{D_\omega^3}{D_\omega^3+1}} + D_\omega^{91D_\omega^4} H(P_\omega)^{6D_\omega^4}$$

où D_ω est le degré total de P_ω.

En utilisant les estimations de D_ω et $H(P_\omega)$ fournies par le lemme 1.3.2, on a

$$S_\omega(B) \leq 2^{2^{15d}} H^{2^{14d}} B^{1-1/2^{5d}}$$

ce qui nous donne, en considérant que le nombre de polynômes P_ω sur lesquels se fait la somme est inférieur à 2^n, et en prenant en compte le nombre de solutions de $a_0(T)D(T) = 0$, que le nombre d'entiers positifs t inférieurs à B tels que la spécialisation $F(t,Y)$ est réductible sur $\mathbb{Q}$ est plus petit que

$$2^{2^{16d}} H^{2^{14d}} B^{1-1/2^{5d}}$$

dès que $B \geq 2^{2^{15d}} H^{2^{14d}}$.

Si on choisit B assez grand pour que cette majoration soit valable et tel que cette quantité soit inférieure à B, alors on est assuré de trouver une spécialisation $t \leq B$ qui est une bonne spécialisation pour le théorème de Hilbert. Ceci est possible si on prend

$$B = (2^{2^{18d}} H^{2^{7d}})^{2^{5d}}.$$

On peut donc énoncer une version effective du théorème d'irréductibilité de Hilbert.

Théorème 2.4.1. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, de degré en Y supérieur ou égal à 1. Notons H sa hauteur et d son degré. Il existe un entier positif t inférieur à*

$$2^{2^{20d}} H^{2^{19d}}$$

tel que $F(t,Y)$ est irréductible sur $\mathbb{Q}$.

Cette méthode a l'avantage de n'utiliser que des outils simples mais en contrepartie, les estimations provenant des coefficients des séries de Puiseux donnent une borne très mauvaise comparée aux résultats connus.

Chapitre 3

Méthode de Fried

Nous allons donner ici une méthode plus algorithmique dans le sens où nous allons décrire une façon de trouver des bonnes spécialisations sous la forme d'une progression arithmétique. L'idée principale est de travailler sur les corps finis pour lesquels on dispose des résultats effectifs de Lang-Weil sur le nombre de points entiers d'une courbe algébrique. On devra se restreindre aux extensions galoisiennes régulières, qui reste cependant le cadre habituel du Problème Inverse de Galois. Le résultat final sera fortement lié à une version effective du théorème d'Ostrowski.

3.1 Réduction dans le cas galoisien-régulier

Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ un polynôme irréductible sur $\mathbb{Q}$. La réduction classique du théorème d'irréductibilité de Hilbert (voir section 1.3) fournit N polynômes que nous noterons ici $Q_1, \ldots, Q_N \in \mathbb{Z}[T,Y]$ irréductibles sur $\mathbb{Q}$ et unitaires en Y.

On suppose de plus dans ce chapitre que l'extension définie par le polynôme F est galoisienne régulière. On se place ainsi dans le cadre usuel du problème inverse et de Galois, et on dispose alors des avantages suivants :

- le degré des polynômes de la réduction n'est pas trop grand,
- les polynômes irréductibles sur $\mathbb{Q}$ correspondant à des extensions intermédiaires de l'extension définie par F sont absolument irréductibles.

3.2 Spécialisations sans zéro entier

Théorème 3.2.1. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ un polynôme absolument irréductible de degré total d, unitaire en Y, et définissant une extension galoisienne N de $\mathbb{Q}(T)$. On notera $y \in N$ une solution de $F(T,Y) = 0$. Considérons un*

polynôme $Q(T,X) \in \mathbb{Z}[T,X]$ irréductible et unitaire en X, définissant une extension intermédiaire E entre $\mathbb{Q}(T)$ et N telle que $E \neq \mathbb{Q}(T)$. Supposons que les racines de $Q(T,X)$ vu comme polynôme en X, qui sont a priori dans $\mathbb{Q}(T,y)$, sont dans $\mathbb{Q}[T,y]$. Soit également un premier p supérieur à $(2d)^{10}$ tel que les réductions $\overline{F}$ et $\overline{Q}$ de F et Q modulo p restent absolument irréductibles sur $\mathbb{F}_p$. Alors il existe une spécialisation $t < p$ telle que, pour tout entier m, l'équation $Q(t+mp,X) = 0$ n'a pas de solution dans $\mathbb{Z}$.

Remarque 3.2.2. *Ce théorème peut s'appliquer par exemple pour $Q = F$. La forme donnée permet de considérer des extensions intermédiaires et sera appliquée aux polynômes de la réduction afin d'obtenir une version effective du théorème de Hilbert.*

Preuve. On note :
- $\deg_T(F) = m$, $\deg_Y(F) = n$ et $\deg(F) = d$,
- $\deg_T(Q) = d_1$, $\deg_X(Q) = d_2$ et $\deg(Q) = D$,

D'après les hypothèses, on peut écrire les racines de Q sous la forme $P_i(T,y)$ avec $P_i(T,Y) \in \mathbb{Z}[T,Y]$, $i = 1, \ldots, d_2$. On a donc

$$Q(T,X) = \prod_{i=1}^{d_2} \Big(X - P_i(T,y) \Big)$$

ce qu'on peut écrire

$$Q(T,X) = \prod_{i=1}^{d_2} \Big(X - P_i(T,X) \Big) \quad [mod\ F(T,Y)]$$

dans $\mathbb{Q}(T)[X,Y]$. Ou encore, en tirant parti du fait que $F(T,Y) \in \mathbb{Z}[T,Y]$ et est unitaire en Y,

$$Q(T,X) = \prod_{i=1}^{d_2} (X - P_i(T,Y)) \quad [mod\ F(T,Y)] \tag{3.1}$$

dans $\mathbb{Z}[T,X,Y]$.

Soit p un nombre premier tel que les réductions $\overline{F}(T,Y)$ et $\overline{Q}(T,X)$ de F et Q modulo p sont absolument irréductibles sur $\mathbb{F}_p$. L'existence d'une infinité de tels p est assurée par le théorème d'Ostrowski (voir par exemple [Za], où il suffit de prendre p assez grand) car F et Q sont absolument irréductibles. On note $\Delta(T)$ le discriminant par rapport à X de Q et $\overline{\Delta}(T)$ sa réduction *modulo* p. On considère l'ensemble

$$\mathcal{T} = \left\{ \bar{t} \in \mathbb{F}_p \;\middle|\; \begin{array}{l} \exists\ \overline{y} \in \mathbb{F}_p \text{ tel que } \overline{F}(\bar{t},\overline{y}) = 0 \\ \overline{\Delta}(\bar{t}) \neq 0 \end{array} \right\}$$

Si pour chaque $\bar{t}$ dans $\mathbb{F}_p$, il existe $\overline{x} \in \mathbb{F}_p$ tel que $\overline{Q}(\bar{t}, \overline{x}) = 0$, alors on peut minorer le nombre $\mathcal{N}$ de points à coordonnées dans $\mathbb{F}_p$ vérifiant $\overline{Q}(\bar{t}, \overline{x}) = 0$ de la façon suivante

$$\mathcal{N} \geq p + (d_2 - 1)\mathrm{Card}(\mathcal{T}),$$

car pour $\bar{t} \in \mathcal{T}$, il découle de 3.1 et de la définition de $\mathcal{T}$ que $\overline{Q}(\bar{t}, X)$ a d_2 zéros distincts dans $\mathbb{F}_p$. Ceci, couplé avec la majoration de $\mathcal{N}$ donnée par les inégalités de Lang-Weil (voir section 1.2.4), donne une majoration de $\mathrm{Card}(\mathcal{T})$:

$$\mathrm{Card}(\mathcal{T}) \leq \frac{1 + (D-1)(D-2)\sqrt{p}}{d_2 - 1}.$$

D'autre part, les inégalités de Lang-Weil, appliquées cette fois-ci au polynôme F, fournissent une minoration de $\mathrm{Card}(\mathcal{T})$:

$$\mathrm{Card}(\mathcal{T}) \geq \frac{p + 1 - d - (d-1)(d-2)\sqrt{p}}{n} - \deg(\Delta).$$

Ceci entraîne que p est borné par une constante p_0 ne dépendant que de d. Il suffit donc de choisir un premier p supérieur à ce p_0 et satisfaisant le théorème d'Ostrowski (une borne a par exemple été donnée par A. Zannier dans [Za] à partir de laquelle tous les premiers conviennent) pour arriver à la conclusion du théorème.

Il nous reste à expliciter cette borne p_0 en fonction du degré de F.

Sous les hypothèses précédentes, on a

$$\frac{p + 1 - d - (d-1)(d-2)\sqrt{p}}{n} \leq \frac{1 + (D-1)(D-2)\sqrt{p}}{d_2 - 1} + 2d^3$$

Mais on a les inégalités suivantes :
- $d_2 \geq 2$,
- $n \leq d$,
- $D \leq d_1 + d_2 \leq 2d^2$,

On obtient, après calculs, la condition suivante pour p :

$$p \leq (2d)^{10}.$$

□

Remarque 3.2.3. *Sans l'hypothèse que l'extension définie par F est régulière, on doit travailler avec un facteur absolument irréductible F_1 de F. Ceci nous oblige à travailler dans un corps L contenant les coefficients de F_1. Afin d'appliquer le théorème de Bertini, nous avons besoin d'un idéal premier qui se décompose totalement dans l'anneau d'entiers de L. Ceci est possible grâce au théorème de Cebotarev, mais ne peut malheureusement pas être rendu effectif car le corps L n'est pas bien connu.*

3.3 Algorithme pour trouver une bonne spécialisation

La réduction classique du théorème de Hilbert, exposée dans le paragraphe 1.3, nous fournit N polynômes que nous noterons ici $Q_1, \ldots, Q_N$, pour lesquels on est ramené à chercher une spécialisation t telle que les polynômes spécialisés $Q_i(t, Y)$ n'aient pas de racine dans $\mathbb{Z}$. Or, le résultat précédent nous permet de trouver, pour chaque polynôme Q_i, une progression arithmétique $(t_i+mp_i)_{m\in\mathbb{Z}}$ telle que le polynôme spécialisé $Q_i(t_i+mp_i, Y)$ n'ait pas de racine dans $\mathbb{Z}$. Le lemme Chinois nous donne alors la possibilité de trouver une progression arithmétique sous la forme $(t + mp_1 \ldots p_N)_{m\in\mathbb{Z}}$ telle qu'aucun des polynômes spécialisés $Q_i(t + mp_0 \ldots p_N, Y)$ n'ait de racine dans $\mathbb{Z}$. Si, de plus, on évite l'ensemble des zéros de $a_0(T)D(T)$, alors la réduction nous permet de conclure que ce sont de bonnes spécialisations pour le théorème de Hilbert.

Nous allons donner un algorithme qui synthétise les différentes étapes afin d'obtenir une bonne spécialisation pour le théorème d'irréductibilité de Hilbert dans le cas où l'extension définie par le polynôme F définit une extension galoisienne régulière.

3.3.1 Étape 1

Trouver N nombres premiers $p_1, \ldots, p_N$ supérieurs à $(2d)^{10}$ tels que les réductions $\overline{F}$ et $\overline{Q_i}$ soient absolument irréductibles *modulo* p_i, $i = 1, \ldots, N$.

On aimerait ne pas avoir à calculer les Q_i, ce qui complique la recherche des p_i. Une première idée est d'utiliser la version effective du théorème d'Ostrowski donnée par U. Zannier dans [Za]. Celle-ci fournit une borne à partir de laquelle tous les nombres premiers ont bonne réduction. Mais auparavant, nous avons besoin d'introduire quelques notations.

Soit k un corps de caractéristique 0 et v une valuation discrète sur k dont le corps résiduel, noté k_0 est de caractéristique $p > 0$. Soit $\mathcal{R}$ l'anneau de valuation de k et (π) un générateur de l'idéal maximal $\mathcal{M}$ de $\mathcal{R}$. On surlignera la réduction *modulo* $\mathcal{M}$. Soit $f \in \mathcal{R}[T, Y]$ un polynôme absolument irréductible de degrés $m, n > 0$ en T et Y respectivement. Soient $a_0(T)$ et $D(T)$ respectivement le coefficient dominant de f et son discriminant par rapport à Y et soient $\rho_1, \ldots, \rho_h$ les racines distinctes du produit $a_0(T)D(T)$. On peut alors énoncer le théorème :

Théorème 3.3.1. *Supposons que $a_0(T)D(T) \notin \mathcal{M}[T]$ et $p > n$. Supposons également que les racines ρ_i sont dans $\mathcal{R}$ pour tout i et qu'elles ont réduction*

distinctes modulo $\mathcal{M}$. Alors $\overline{f} \in k_0[T,Y]$ est de la forme $f_1(T)f_2(T,Y)$ avec $f_1(T) \in k_0[T]$ et $f_2(T,Y) \in k_0[T,Y]$ absolument irréductible.

On note $R(T) = a_0(T)D(T)$, $R^*(T)$ un polynôme sans facteur multiple, à coefficients entiers et ayant exactement les mêmes racines que R et $\delta = \mathrm{Disc}(R^*)$. Alors, en prenant pour k le corps engendré sur $\mathbb{Q}$ par les racines de R, l'énoncé suivant donne des conditions pour des p qui conviennent :

Corollaire 3.3.2. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ absolument irréductible sur $\mathbb{Q}$. Si p est un nombre premier vérifiant les conditions*

(i) $p \nmid \delta$

(ii) $p \nmid R(T)$

(iii) $\overline{a_0}(T), \ldots, \overline{a_n}(T)$ *sans facteurs communs*

alors $\overline{F}(T,Y)$ est absolument irréductible sur $\mathbb{F}_p$.

On peut également fournir une borne explicite (voir [Za]) :

Corollaire 3.3.3. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ absolument irréductible sur $\mathbb{Q}$ de degrés m,n respectivement en T et Y et de hauteur H. Si p est un nombre premier supérieur à*

$$e^{12n^2m^2}(4n^2m)^{8n^2m}H^{2(2n-1)^2m}$$

alors la réduction de $\overline{F}(T,Y)$ est absolument irréductible sur $\mathbb{F}_p$.

Afin de s'assurer que les réductions des Q_i restent absolument irréductibles, et en utilisant les estimations des degrés et hauteur des Q_i, il suffit de choisir chaque p_i supérieur à

$$e^{36n^5m^2}(4n^3m)^{9n^4m}H^{8n^4m}$$

On peut donc par exemple prendre pour $p_1, \ldots, p_N$ les N premiers nombres premiers supérieurs à cette borne. On remarque que les nombres ainsi obtenus sont d'une taille trop importante pour espérer obtenir une bonne version effective du théorème de Hilbert. Cependant, la description de la méthode est très simple.

Une autre méthode pour trouver des p_i qui conviennent consiste à utiliser une autre version effective du théorème d'Ostrowski. En effet, la version utilisée ci-dessus donne un résultat bien plus fort que ce dont on a besoin : elle nous assure que tous les p après une certaine borne satisfont à la propriété demandée, alors qu'on a besoin d'un seul tel p. Il est possible de donner une borne en-dessous de laquelle on est assuré de trouver un premier qui convient. Cependant, afin de le déterminer effectivement, on doit tester tous les nombres premiers inférieurs à cette borne, ce qui est également très coûteux.

3.3.2 Étape 2

Les premiers p_i étant fixés, le théorème 3.2.1 appliqué pour chaque $i \in \{1, \ldots, N\}$ à F et Q_i avec le premier p_i prouve l'existence d'un entier positif $t_i \leq p_i$ tel que, pour tout entier k, l'équation $Q_i(t_i + kp_i, Y) = 0$ n'a pas de solution entière. L'application du lemme chinois nous permet d'en déduire l'existence d'un entier positif t inférieur au produit $p_1 \ldots p_N$ tel que, pour tout entier k, les équations $Q_i(t + kp_1 \ldots p_N, Y) = 0$, $i = 1, \ldots, N$, n'ont pas de solution entière.

Afin de trouver explicitement une bonne spécialisation pour le théorème d'irréductibilité de Hilbert, il suffit donc de trouver un point de cette progression arithmétique qui n'annule pas le polynôme $a_0(T)D(T)$. Le degré de ce polynôme étant inférieur à $(2n-1)m$, on est assuré de trouver une bonne spécialisation t inférieure à $2nmp_1 \ldots p_N$.

3.4 Conclusion

À ce stade, il est clair qu'afin d'avoir une bonne majoration, on a besoin de limiter la taille des p_i et le nombre de polynômes issus de la réduction N. Ce dernier peut être rendu polynomial sous l'hypothèse que l'extension définie par F soit galoisienne (voir l'amélioration de la réduction dans ce cas dans le chapitre suivant, section 4.4). Pour ce qui est de la taille des p_i, nous ne voyons pour l'instant pas de meilleure solution que l'utilisation de versions effectives du théorème d'Ostrowski.

Chapitre 4

Utilisation des résultats de Heath-Brown

Ce chapitre va présenter une nouvelle méthode qui permet d'améliorer de façon significative les résultats connus à ce jour. Dans un premier temps, nous donnerons une version explicite du résultat récent de Heath-Brown sur l'étude de la quantité

$$N(F;B) = \sharp\{(t,y) \in \mathbb{Z}^2 \ : \ F(t,y) = 0, \ \max(|t|,|y|) \leq B\}$$

où B est un entier supérieur ou égal à 2.

Théorème 4.0.1. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$ de degré total $d \geq 1$. On a*

$$N(F,B) \leq 2^{48} d^8 \log^5(B) B^{d^{-1}}.$$

Un des intérêts de cette version effective est que la dépendance en d est polynomiale, ce qui améliore les résultats de Bombieri et Pila [BP] et de Schinzel et Zannier [ScZa]. De plus, le résultat est indépendant de la hauteur de F.

Nous appliquerons ensuite ce résultat afin d'estimer le nombre de spécialisations entières $t \leq B$, telles que le polynôme $F(t,Y)$ ait un zéro entier. Ceci nous permettra en premier lieu de donner une borne pour les spécialisations telles que $F(t,Y)$ n'ait pas de zéro entier :

Théorème 4.0.2. *Soient $s \in \mathbb{N}^*$ et $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, primitif, de degré d et tel que $\deg_Y(F) \geq 2$. Notons $H = \max H(F), e^e$. Il existe s entiers positifs $t_1, \ldots, t_s$ inférieurs à*

$$(s + 2^{88} d^{45} \log^{19}(H))^4$$

tels que les équations $F(t_i, Y) = 0, \ i = 1, \ldots, s$ n'ont pas de solution entière.

Cela nous permettra également, via une réduction classique du théorème de Hilbert, de donner une nouvelle forme effective qui améliore de façon significative les résultats existants.

Théorème 4.0.3. *Soient $s \in \mathbb{N}^*$ et $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, primitif et tel que $\deg_Y(F) \geq 1$. Notons m et n les degr{es partiels de F en T et Y respectivement, et $H = \max\{H(F), e^e\}$. Il existe s entiers positifs $t_1, \ldots, t_s$ inférieurs à*

$$(s + 2^{108} 2^{76n} m^{64} \log^{19}(H))^4$$

tels que les polynômes $F(t_i, Y),\ i = 1, \ldots, s$ sont irréductibles sur $\mathbb{Q}$.

Enfin, nous verrons que dans le cas où l'extension définie par F est galoisienne, il est possible de modifier la réduction usuelle afin de donner, via un résultat récent de L. Pyber de théorie des groupes, une borne polynomiale pour la plus petite spécialisation qui conserve l'irréductibilité d'un polynôme. Le résultat de L. Pyber fait intervenir une constante absolue qui sera notée c.

Théorème 4.0.4. *Soient $s \in \mathbb{N}^*$ et $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, primitif, tel que $\deg_Y(F) \geq 1$ et définissant une extension galoisienne sur $\mathbb{Q}(T)$. Notons m et n les degrés partiels de F en T et Y respectivement, et $H = \max\{H(F), e^e\}$. Il existe s entiers positifs $t_1, \ldots, t_s$ inférieurs à*

$$(s + 2^{165} m^{64} n^{147+c} \log^{19}(H))^4$$

tels que les polynômes $F(t_i, Y),\ i = 1, \ldots, s$ sont irréductibles sur $\mathbb{Q}$.

4.1 Théorème de Heath-Brown explicite

Dans cette section, nous allons nous intéresser à la quantité

$$N(F,B) = \sharp\{(x_1, x_2) \in \mathbb{Z}^2 \ :\ F(x_1, x_2) = 0,\ \max(|x_1|, |x_2|) \leq B\}$$

où F est un polynôme irréductible de degré d et B est un entier strictement positif. Un théorème de Bombieri et Pila [BP] donne une majoration de $N(F;B)$ en $B^{1/d}$. Afin d'améliorer la borne pour la plus petite spécialisation qui laisse un polynôme irréductible, A. Schinzel et U. Zannier [ScZa] ont modifié la preuve de Bombieri et Pila et ont supprimé une condition contraignante sur la taille de B. Le résultat récent de Heath-Brown [HB] donne une nouvelle méthode plus générale (pour une boîte quelconque et dans l'espace projectif) que nous allons donner en explicitant les constantes et dans

le cas qui nous intéresse, c'est-à-dire pour deux variables et dans l'espace affine. Le résultat principal de Heath-Brown pour les courbes algébriques est le suivant :

Théorème H-B. *Soit $F(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ un polynôme irréductible sur $\mathbb{Q}$ de degré d, et soient $\varepsilon > 0$ et $B \geq 1$ donnés. Alors on peut trouver D ne dépendant que de d et ε et un entier k satisfaisant la condition*

$$k \ll_{d,\varepsilon} B^{d^{-1}+\varepsilon}(\log H(F))^3$$

tels qu'on ait la propriété suivante : il existe k polynômes $F_1, \ldots, F_k \in \mathbb{Z}[X_1, X_2]$, premiers avec $F(X_1, X_2)$ et de degré au plus D tels que chaque point compté par $N(F; B)$ est le zéro d'un des polynômes $F_j(X_1, X_2)$.

Remarque. On peut supposer que F est absolument irréductible. En effet, dans le cas contraire, on a une borne directement pour $N(F, B)$, qui plus est indépendante de B, de la façon suivante :

$F(x_1, x_2) = 0$ implique que $\varphi(x_1, x_2) = 0$ pour un facteur $\varphi \notin \mathbb{Q}[X_1, X_2]$ de F irréductible sur $\mathbb{C}$ unitaire en x_2, et donc $\psi(x_1, x_2) = 0$ pour un conjugué de φ sur $\mathbb{Q}$ qui est un autre facteur de F. Comme $\mathrm{Res}_{x_2}(\varphi, \psi)^2 \mid \mathrm{disc}_{x_2} F$, alors le nombre de x_1 entiers tels que $\varphi(x_1, x_2) = \psi(x_1, x_2) = 0$ pour un x_2 entier est inférieur à $\dfrac{1}{2}\deg(\mathrm{disc}_{x_2} F) \leq d(d-1)$. Le même raisonnement s'applique pour x_2, et on obtient alors que le nombre total de points entiers est majoré par d^4.

Pour estimer $N(F, B)$, il suffira alors de compter le nombre d'intersections de F avec les F_j en appliquant le théorème de Bézout.

Nous allons désormais donner la preuve de ce théorème en explicitant la dépendance en d et ε.

4.1.1 Points singuliers

Commençons par considérer les points singuliers. Tout point singulier de la courbe $F(\underline{X}) = 0$ satisfait

$$\frac{\partial F}{\partial X_i}(\underline{x}) = 0, \ (i = 1, 2).$$

Comme F n'est pas constant, au moins un des polynômes $\partial F/\partial X_i$ n'est pas identiquement nul. Un tel polynôme ne peut pas être un multiple de F car son degré est $d-1$. On inclut donc les deux dérivées partielles de F parmi les polynômes F_i décrits dans le théorème H-B ci-dessus. On peut alors majorer

le nombre k' de polynômes associés aux points singuliers par 2.

En ce qui concerne les points non singuliers, nous utiliserons le résultat suivant qui nous permet de regarder les points non singuliers modulo un premier p qu'on peut choisir assez grand.

4.1.2 Réduction modulo p pour les points non singuliers

Soient

$$S(F;B,p)=\left\{\underline{x}\in\mathbb{Z}^2\ :\ F(\underline{x})=0,\ |x_i|\leq B\ (1\leq i\leq 2),\ \exists j;\ p\nmid\frac{\partial F}{\partial X_j}(\underline{x})\right\}$$

et

$$S(F;B)=\left\{\underline{x}\in\mathbb{Z}^2\ :\ F(\underline{x})=0,\ |x_i|\leq B\ (1\leq i\leq 2),\ \exists j;\ \frac{\partial F}{\partial X_j}(\underline{x})\neq 0\right\}$$

Lemme 4.1.1. *Soient P un entier, $P\geq 2$, et $r=[\log_2(2d^3H(F)B^{d-1})]+1$. Alors il existe r nombres premiers distincts $p_1,\ldots,p_r$ dans l'intervalle*

$$P\leq p_i\leq 8r^2P\log P$$

tels que

$$S(F;B)=\bigcup_{i=1}^{r}S(F;B,p_i).$$

Preuve. Soient $p_1,\ldots,p_r$ les r premiers nombres premiers supérieurs à P.

Soit $\underline{x}\in S(F;B)$, alors $\dfrac{\partial F}{\partial X_j}(\underline{x})\neq 0$ pour un certain j. On a la majoration suivante

$$\left|\frac{\partial F}{\partial X_j}(\underline{x})\right|\leq 2d^3H(F)B^{d-1}$$

qui nous donne

$$\sharp\left\{p\text{ premier}\ :\ p\mid\left|\frac{\partial F}{\partial X_j}(\underline{x})\right|\right\}\leq\log_2\left|\frac{\partial F}{\partial X_j}(\underline{x})\right|\leq\log_2(2d^3H(F)B^{d-1}).$$

Cette quantité étant par hypothèse strictement inférieure à r, un des p_i ne divise pas $\dfrac{\partial F}{\partial X_j}(\underline{x})$.

Pour majorer les p_i, il suffit de majorer p_r. Pour cela, on peut le majorer par le $(P+r)$-ième premier, soit

$$p_i\leq 2(r+P)\log(r+P)\leq 8r^2P\log P\leq 72\log^2(2d^3H(F)B^{d-1})P\log P.$$

□

Remarque. Nous avons modifié le résultat de Heath-Brown afin d'obtenir une dépendance polynomiale en d par la suite, quitte à perdre un peu puisqu'il obtient une majoration des p_i de l'ordre de P.

Ce résultat nous permet de considérer les points non singuliers modulo un premier p convenable pour un coût dans l'estimation finale du nombre de polynômes F_j d'un facteur $r = [\log_2(2d^3H(F)B^{d-1})] + 1$.

Soit k'' le nombre de points $\underline{t} \in \mathbb{F}_p^2$ non singuliers de $F(\underline{t}) = 0$. Nous allons étudier les k'' ensembles

$$S(\underline{t}) = \{\underline{x} \in S(F; B, p) \ : \ \underline{x} \equiv \underline{t} \pmod{p}\}.$$

Nous allons montrer que, si on choisit P assez grand, alors on peut associer à chaque ensemble $S(\underline{t})$ un polynôme F_j tel que $\forall \underline{x} \in S(\underline{t}),\ F_j(\underline{x}) = 0$.

On a alors, en utilisant les inégalités de Lang-Weil (voir section 1.2.4), une estimation du nombre de polynômes associés aux points non singuliers :

$$k'' \leq d(p+1+(d-1)(d-2)\sqrt{p}) \leq 2d^3p \leq 144d^3\log^2(2d^3H(F)B^{d-1})P\log P.$$

On obtient finalement que le nombre de polynômes k décrits dans le théorème H-B est

$$k \leq k' + k''r \leq 433d^3\log^3(2d^3H(F)B^{d-1})P\log P$$

pour un P assez grand à préciser.

4.1.3 Construction d'un polynôme F_j pour un ensemble $S(t_1, t_2)$ donné

Soit $\underline{t} = (t_1, t_2) \in \mathbb{F}_p^2$ un point non singulier de $F(\underline{t}) = 0$. Une des dérivées partielles au moins ne s'annule pas en $\underline{t}$, on peut supposer

$$\frac{\partial F}{\partial X_1}(\underline{t}) \neq 0.$$

Soit $D \geq d$, on définit une collection de monômes de degré inférieur à D par un ensemble d'exposants :

$$\mathcal{E} \subset \{(e_1, e_2) \in \mathbb{Z}^2 \ : \ e_i \geq 0 \ (i = 1, 2),\ e_1 + e_2 \leq D\}$$

On écrira $\underline{x}^{\underline{e}} = x_1^{e_1}x_2^{e_2}$, et on notera $E = \sharp\mathcal{E}$ et $K = \sharp S(\underline{t})$.

Soient $\underline{x}_{(1)}, \ldots, \underline{x}_{(K)}$ K éléments distincts de $S(\underline{t})$. Notons M_2 la matrice de taille $K \times E$ suivante

$$M_2 = \left(\underline{x}_{(i)}^{\underline{e}}\right)_{\substack{1 \leq i \leq K \\ \underline{e} \in \mathcal{E}}}$$

Nous allons montrer que, pour p bien choisi, le rang de M_2 est strictement inférieur à E, ce qui permet de trouver une solution non triviale $C \in \mathbb{Z}^E$ à l'équation $M_2 C = 0$. Les éléments de C fourniront alors les coefficients du polynôme F_j recherché.

- Si $K \leq E-1$, alors $\mathrm{rg}(M_2) \leq E-1$
- Si $K \geq E$, on regarde les mineurs d'ordre E : soient E éléments de $S(\underline{t})$, qu'on notera $\underline{x}_{(1)}, \ldots, \underline{x}_{(E)}$, quitte à renuméroter, et

$$\Delta = \det\left[\left(\underline{x}_{(i)}^{\underline{e}}\right)_{\substack{1 \leq i \leq E \\ \underline{e} \in \mathcal{E}}}\right].$$

Nous allons montrer que, si p est suffisamment grand, alors $\Delta = 0$.

Valuation en p de Δ

$$\Delta = \begin{vmatrix} \underline{x}_{(1)}^{\underline{e}} & \underline{x}_{(1)}^{\underline{e}'} & \cdots \\ \underline{x}_{(2)}^{\underline{e}} & \underline{x}_{(2)}^{\underline{e}'} & \cdots \\ \vdots & & \\ \underline{x}_{(E)}^{\underline{e}} & & \end{vmatrix}$$

On utilise le lemme suivant, qui est une version polynomiale du théorème des fonctions implicites :

Lemme 4.1.2. *Soit $F(\underline{X}) \in \mathbb{Z}_p[\underline{X}]$ un polynôme à 2 variables et soit $\underline{u} \in \mathbb{Z}_p^2$ tel que $F(\underline{u}) = 0$ et $p \nmid \dfrac{\partial F}{\partial X_1}(\underline{u})$. Alors pout tout $m \geq 1$, il existe $f_m(Y) \in \mathbb{Z}_p[Y]$ tel que si $F(\underline{x}) = 0$ pour un $\underline{x} \in \mathbb{Z}_p^2$ tel que $\underline{x} \equiv \underline{u}$ (mod p), alors*

$$x_1 \equiv f_m(x_2) \ (mod\ p^m).$$

Démonstration. Nous allons faire la preuve par récurrence sur m. On note

$$\frac{\partial F}{\partial X_1}(u_1, u_2) = \mu.$$

On définit f_m par $f_1(Y) = u_1$ et

$$f_{m+1}(Y) = f_m(Y) - \mu^{-1} F(f_m(Y), Y)$$

pour $m \geq 1$. Le cas $m = 1$ est immédiat. Pour le cas général, l'hypothèse de récurrence $x_1 \equiv f_m(x_2)$ (mod p^m) permet d'écrire

$$x_1 = f_m(x_2) + \lambda p^m$$

avec $\lambda \in \mathbb{Z}_p$. La formule de Taylor, tronquée modulo p^{m+1}, donne alors

$$0 = F(\underline{x}) \equiv F(f_m(x_2), x_2) + \lambda p^m \frac{\partial F}{\partial X_1}(f_m(x_2), x_2) \pmod{p^{m+1}}.$$

De plus, comme $f_m(x_2) \equiv x_1 \equiv u_1 \pmod{p}$ (car $(x_1, x_2) \equiv (u_1, u_2) \pmod{p}$), on a

$$\frac{\partial F}{\partial X_1}(f_m(x_2), x_2) \equiv \mu \pmod{p}.$$

On peut donc en conclure que

$$\lambda p^m \equiv -\mu^{-1} F(f_m(x_2), x_2) \pmod{p^{m+1}}$$

d'où

$$x_1 \equiv f_{m+1}(x_2) \pmod{p^{m+1}},$$

ce qui termine la récurrence. □

Ce lemme va nous permettre d'écrire le déterminant Δ en fonction d'une seule variable. En effet, on obtient que, quelque soit m,

$$\Delta \equiv \Delta_0 \pmod{p^m},$$

où

$$\Delta_0 = \det(M_0), \ M_0 = (\underline{w}_{(i)}^{\underline{e}})_{1 \le i \le E, \ \underline{e} \in \mathcal{E}}$$

avec

$$\underline{w}_{(i)} = (w_{(i),1}, w_{(i),2}) = (f_m(x_{(i),2}), x_{(i),2}).$$

En écrivant le développement $p-$adique de $x_{(i),2}$ comme $u_2 + y_{(i),2}$ avec $u_2 \in \mathbb{Z}_p$ indépendant de i (par définition de $S(\underline{t})$) et $y_{(i),2} \in p\mathbb{Z}_p$, on a

$$\underline{w}_{(i)}^{\underline{e}} = f_m(u_2 + y_{(i),2})^{e_1} (u_2 + y_{(i),2})^{e_2} = g_{\underline{e}}(y_{(i),2})$$

où $g_{\underline{e}}(Y) \in \mathbb{Z}_p[Y]$.

Chaque colonne correspond à un polynôme $g_{\underline{e}}(Y)$. On ordonne les colonnes par degré du monôme de plus bas degré croissant. Notons a le degré du monôme de plus bas degré de la première colonne. On supprime des colonnes 2 à E le monôme de degré a, s'il existe. On itère ensuite ce procédé de façon à classer les colonnes par degré du monôme de plus bas degré *strictement* croissant. Ceci est toujours possible si les colonnes sont linéairement indépendantes, et dans le cas contraire, la conclusion $\Delta = 0$ est trivialement vérifiée. Ce procédé n'utilisant que des opérations élémentaires ne change pas le déterminant au signe près.

Il est alors clair que la k-ième colonne est divisible par p^{k-1} car constituée de polynômes dont le premier terme est de degré supérieur à $k-1$ et p divise $y_{(i),2}$. Donc Δ_0 est divisible par $p^{E(E-1)/2}$. Finalement, on a montré que, si on pose $\nu := E(E-1)/2$, alors la valuation en p de Δ est supérieure à ν.

Taille de Δ

On peut estimer la taille de Δ :

$$|\Delta| \leq E^E \prod_{\underline{e} \in \mathcal{E}} B^{e_1+e_2} \leq E^E B^{E'}$$

où $E' = \sum_{\underline{e} \in \mathcal{E}} e_1 + e_2$. On obtient donc la conclusion suivante

$$\text{Si } p^\nu > E^E B^{E'}, \text{ alors } \Delta = 0.$$

Première conclusion

On a montré que sous la condition

$$p^\nu > E^E B^{E'}, \tag{4.1}$$

le rang de la matrice (M_2) est inférieur à $E-1$ (car tous les mineurs $E \times E$ sont nuls). On en déduit qu'il existe $C = (c_{\underline{e}}) \in \mathbb{Z}^E$, $C \neq 0$, tel que $M_2 C = 0$. Si on pose

$$F_j(\underline{X}) = \sum_{\underline{e} \in \mathcal{E}} c_{\underline{e}} \underline{X}^{\underline{e}},$$

alors F_j est un polynôme non nul de degré inférieur ou égal à D tel que $F_j(\underline{x}) = 0$ pour tout $\underline{x}$ de $S(\underline{t})$.

Choix de $\mathcal{E}$

Il reste à choisir l'ensemble d'exposants $\mathcal{E}$ afin de s'assurer que $F \nmid F_j$. On écrit

$$F(X_1, X_2) = \sum_{\underline{f}} a_{\underline{f}} X_1^{f_1} X_2^{f_2}$$

et on considère le polygône de Newton $\mathcal{P}(F)$ de F, qui est l'enveloppe convexe des points $(f_1, f_2) \in \mathbb{Z}^2$ tels que $a_{\underline{f}} \neq 0$.

On choisit un point (m_1, m_2) de $\mathcal{P}$ tel que $m_1 + m_2 = d (= \deg F)$.

Il suffit alors de choisir l'ensemble $\mathcal{E}$ de la façon suivante

$$\mathcal{E} = \{(e_1, e_2) \in \mathbb{Z}^2 \ : \ e_i \geq 0 \, (i = 1, 2), \ e_1 + e_2 \leq D, e_i < m_i \text{ pour un certain } i\}$$

avec $D > d$. En effet, s'il existe un G tel que $F_j = FG$, alors les propriétés des polygônes de Newton nous disent que $\mathcal{P}(F_j)$ est égal à $\mathcal{P}(F) + \mathcal{P}(G)$ (Ostrowski [Ost]) et contient donc un point du type $(m_1, m_2) + (g_1, g_2)$. Or ceci est impossible car ce point ne peut appartenir à $\mathcal{E}$.

Etude de la condition (4.1) : $p^\nu > E^E B^{E'}$

On a $E = \sharp\mathcal{E}_1 - \sharp\mathcal{E}_2$ avec

$$\mathcal{E}_1 = \{(e_1, e_2) \in \mathbb{Z}^2 \ : \ e_i \geq 0 \ (i = 1, 2), \ e_1 + e_2 \leq D\}$$

et

$$\mathcal{E}_2 = \{(e_1, e_2) \in \mathbb{Z}^2 \ : \ e_i \geq 0 \ (i = 1, 2), \ e_1 + e_2 \leq D, \ e_i \geq m_i \ (i = 1, 2)\}$$

donc

$$E = \begin{pmatrix} D+2 \\ 2 \end{pmatrix} - \begin{pmatrix} D-d+2 \\ 2 \end{pmatrix} = dD + 1 - \frac{(d-1)(d-2)}{2}.$$

Joint à la définition $\nu = E(E-1)/2$, cela donne

$$\frac{E}{\nu} = \frac{2}{E-1} \leq \frac{2}{dD - d^2/2} \leq \frac{2}{dD} + \frac{2}{D^2}.$$

De la même manière, on peut estimer $E' = E'_1 + E'_2$ où

$$E'_i = \sum_{\underline{e} \in \mathcal{E}} e_i = \sum_{\underline{e} \in \mathcal{E}_1} e_i - \sum_{\underline{e} \in \mathcal{E}_2} e_i.$$

En effet, les égalités

$$\begin{cases} \sum_{\underline{e} \in \mathcal{E}_1} e_i = \dfrac{D}{3} \begin{pmatrix} D+2 \\ 2 \end{pmatrix} \\ \sum_{\underline{e} \in \mathcal{E}_2} e_i = \left(m_i + \dfrac{D-d}{3} \right) \begin{pmatrix} D-d+2 \\ 2 \end{pmatrix} \end{cases}$$

donnent l'estimation

$$E' \leq \frac{dD^2}{2} + \frac{dD}{2}.$$

On obtient ainsi, après calculs, la majoration suivante de E'/ν, valable pour $D > d$

$$\frac{E'}{\nu} \leq \frac{1}{d} + \frac{6}{D}.$$

Il suffit donc de s'assurer que

$$p > (2dD)^{2(dD)^{-1} + 2D^{-2}} B^{d^{-1} + 6D^{-1}}.$$

En remarquant de plus que $(2dD)^{2(dD)^{-1} + 2D^{-2}} \leq e^8$ pour $D > d$, on choisit

$$P = 1 + [e^8 B^{d^{-1} + 6D^{-1}}].$$

On obtient donc, pour cette valeur de P, que le nombre k des polynômes du théorème H-B est majoré par

$$k \leq 2^{27} d^3 \log^3(2d^3 H(F) B^{d-1}) B^{d^{-1}+6D^{-1}} \log(B)$$

dès que $D > d$.

Ceci nous fournit donc une borne explicite pour le théorème H-B. Il suffit désormais d'appliquer le théorème de Bezout pour compter les intersections de F avec chaque F_j, ce qui donne une estimation totalement explicite de $N(F, B)$.

$$N(F, B) \leq 2^{27} d^4 D \log^3(2d^3 H(F) B^{d-1}) \log(B) B^{d^{-1}+6D^{-1}}$$

dès que $D > d$.

Cette estimation est optimale pour $D = \log B$. Afin de satisfaire la condition $D > d$, et de simplifier les calculs, on choisit la valeur $D = [d \log B] + 1$, ce qui donne la borne

$$N(F, B) \leq 2^{27} d^5 \log^3(2d^3 H(F) B^{d-1}) \log^2(B) B^{d^{-1}+6(d \log B)^{-1}}$$

ou encore, en majorant $B^{6(d \log B)^{-1}}$ par 2^9,

$$N(F, B) \leq 2^{36} d^5 \log^3(2d^3 H(F) B^{d-1}) \log^2(B) B^{d^{-1}}.$$

4.1.4 Borne indépendante de $H(F)$

Nous allons maintenant montrer le résultat suivant qui permet de donner une borne indépendante de la hauteur de F.

Proposition 4.1.3. *Soit $F(T, Y) \in \mathbb{Z}[T, Y]$ un polynôme de degré d dont les coefficients sont sans facteur commun. Alors $N(F, B) \leq d^2 + 3$ ou $H(F) \leq 625 d^8 B^{4d}$.*

Preuve. Posons $N = d^2 + 4$ et $M = (d+1)(d+2)/2$. Si $F(X_1, X_2) = 0$ a au moins $N = d^2+4$ solutions $\underline{x}^{(1)}, \ldots, \underline{x}^{(N)}$ telles que $|x_j^{(i)}| \leq B$ $(1 \leq i \leq N,\ j = 1, 2)$, on considère la matrice $C = (c_{i,j})_{i,j}$ de taille $N \times M$ dont la i-ème ligne est formée des M monômes possibles de degré d en les variables $x_1^{(i)}, x_2^{(i)}$. On note $f \in \mathbb{Z}^M$ le vecteur dont les composantes sont les coefficients de F de sorte que $Cf = 0$. D'après le lemme de Siegel (voir par exemple [Sch]), comme $N > M$, ce système admet une solution $g \in \mathbb{Z}^M$ non nulle vérifiant la majoration :

$$\max_{k=1,\ldots,M} |g_k| \leq (NA)^{\dfrac{M}{N-M}}$$

où A est choisi supérieur aux $|c_{i,j}|$. On prend $A = B^d$ et on construit un polynôme G dont les coefficients sont les éléments de g (en gardant l'ordre des monômes choisi pour F) ; G est alors un polynôme non nul à coefficients entiers, de degré inférieur à d, s'annulant en les N points $\underline{x}^{(1)}, \ldots, \underline{x}^{(N)}$ et vérifiant

$$\max_{k=1,\ldots,M} |g_k| \leq (NB^d)^{\frac{M}{N-M}}.$$

Par construction, $G(\underline{X})$ et $F(\underline{X})$ ont d^2+4 zéros communs et sont de degré inférieur à d. Ceci contredit le théorème de Bezout, à moins que F et G soient proportionnels. Mais comme F est irréductible et que ses coefficients n'ont pas de facteur commun, alors $G = aF$ avec $a \in \mathbb{Z}$ et on a

$$H(F) = \max_{k=1,\ldots,M} |f_k| \leq \max_{k=1,\ldots,M} |g_k| \leq (NB^d)^{\frac{M}{N-M}}.$$

Après calculs, on obtient la majoration suivante de $H(F)$ en fonction de d et B :

$$H(F) \leq 625 d^8 B^{4d}.$$

□

Le lemme précédent nous permet de donner une borne totalement explicite et indépendante de H pour $N(F,B)$:

$$N(F,B) \leq 2^{36} d^5 \log^3(1250 d^{11} B^{5d-1}) \log^2(B) B^{d^{-1}}.$$

qui peut être présentée sous la forme moins précise mais plus compacte donnée dans le théorème 4.0.1.

4.2 Borne pour la plus petite spécialisation sans zéro entier

Le résultat précédent va nous permettre d'estimer le nombre de spécialisations $t \in \mathbb{N}$, $t \leq B$, telles que, étant donné un polynôme $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, le polynôme spécialisé $F(t,Y)$ a un zéro entier. On en déduira d'une part une borne pour trouver s spécialisations telles que le polynôme $P(t,Y)$ n'a pas de zéro entier (théorème 4.0.2) et d'autre part une nouvelle version effective du théorème d'irréductibilité de Hilbert (section 4.3).

On notera toujours m et n les degrés partiels de F en T et Y respectivement. On supposera $m > 0$, le résultat étant trivial sinon.

4.2.1 Estimation des solutions entières de $F(t, Y) = 0$

On écrit F sous la forme

$$F(T, Y) = a_0(T)Y^n + \cdots + a_n(T).$$

L'inégalité de Liouville nous permet de majorer une telle solution y de $F(t, Y) = 0$ pour un entier positif t tel que $a_0(t) \neq 0$ et $t \leq B$:

$$|y| \leq 2 \max_{i=0\ldots n} |a_i(t)| \leq 2(m+1)H(F)B^m \leq 2(m+1)HB^m$$

où $H = \max\{H(F), e^e\}$. On peut donc se ramener à compter les points entiers sur la courbe algébrique définie par F dans le carré de côté $2B'$ avec $B' = 2(m+1)HB^m$. Afin d'obtenir une borne strictement inférieure à B, nous allons distinguer deux cas. On notera pour plus de lisibilité $L_1 = \log H$ et $L_2 = \log\log H$. Notons que $H \geq e^e$ et donc $L_2 \geq 1$.

4.2.2 Cas 1 : $d \geq 2mL_1/L_2$

On applique la version effective du résultat de Heath-Brown donnée par le théorème 4.0.1 au polynôme F avec $B' = 2(m+1)HB^m$. L'hypothèse sur d nous permet de majorer efficacement les termes en H et B provenant de $B'^{1/d}$. En effet, pour H, la majoration $1/d \leq L_2/L_1$ donne

$$H^{1/d} \leq H^{L_2/L_1} = \log(H)$$

et pour B, la majoration $1/d \leq 1/2m$ donne

$$B^{m/d} \leq B^{1/2}.$$

On obtient, après calculs, que le nombre d'entiers positifs t inférieurs à B tels que $a_0(t) \neq 0$ et que $F(t, Y) = 0$ a une solution entière est majoré par

$$2^{58}d^{18}\log^6(H)B^{1/2}\log^5 B.$$

4.2.3 Cas 2 : $d < 2mL_1/L_2$

On applique cette fois-ci le théorème de la section précédente au polynôme

$$G(T, Y) = F(T, T^E + Y)$$

où $E = [2mL_1/L_2] + 1 \leq 4mL_1$ (ce polynôme est alors de degré d' compris entre nE et $nE + m$). Tout zéro entier (t, y) de G correspond à un zéro de la forme $(t, t^E + y)$ de F.

On sait alors que pour tout zéro (t, y) de G tel que $|t| \leq B$, on a

$$|y| \leq B^E + 2(m+1)HB^m \leq 2(m+1)HB^E.$$

On peut alors appliquer le théorème 1 au polynôme G avec $B' = 2(m+1)HB^E$. Notons également que la hauteur $H(G)$ est majorée par $2^n H(F)$. Le même type de calculs que pour le cas 1 nous donne une majoration en B de l'ordre de $B^{1/n}$ qui est bien strictement inférieur à B puisqu'on a supposé $n \geq 2$. Le nombre d'entiers positifs t inférieurs à B tels que $a_0(t) \neq 0$ et que $F(t, Y) = 0$ a une solution entière est majoré par

$$2^{87} d^{45} \log^{19}(H) B^{1/2} \log^5 B.$$

4.2.4 Conclusion

On en déduit que dans tous les cas, en tenant compte du nombre de solutions de $a_0(t) = 0$, le nombre de spécialisations $t \geq 0$ inférieures à B telles que $F(t, Y) = 0$ a une solution entière est plus petit que

$$2^{88} d^{45} \log^{19}(H) B^{1/2} \log^5 B. \tag{4.2}$$

Pour trouver s valeurs de $t \geq 0$ inférieures à B telles que $F(t, Y) = 0$ n'a pas de solution entière, il suffit que cette quantité soit inférieure à $B - s$, ce qui est le cas si

$$B > (s + 2^{88} d^{45} \log^{19}(H))^4.$$

Notons qu'ainsi B est assez grand pour que la majoration $\log^5 B \leq B^{1/4}$ soit valable. Un tel choix de B nous fournit alors la borne donnée par le théorème 4.0.2.

4.3 Théorème de Hilbert effectif - cas général

Rappelons rapidement la reformulation du problème décrite à la fin du premier chapitre.

On a introduit les polynômes P_ω qui sont les polynômes minimaux de fonctions symétriques élémentaires d'un sous-ensemble de racines de F (indexé par $\omega \subset \{1, \ldots, n\}$). On note $S(B)$ le nombre d'entiers positifs $t \leq B$ tels que $a_0(t)D(t) \neq 0$ et $F(t, Y)$ est réductible sur $\mathbb{Q}$, et $S_\omega(B)$ le nombre d'entiers positifs $t \leq B$ tels que $a_0(t)D(t) \neq 0$ et $P_\omega(t, Y)$ a un zéro entier. On a alors l'inégalité

$$S(B) \leq \sum_\omega S_\omega(B)$$

Pour estimer $S(B)$, il suffit donc d'estimer chaque $S_\omega(B)$ en utilisant l'estimation (4.2) de la section précédente.

4.3.1 Estimation de $S_\omega(B)$

Connaissant le degré et la hauteur des polynômes P_ω (voir lemme 1.3.2), on applique l'estimation (4.2) de la section 4.2.4, ce qui donne

$$S_\omega(B) \leq 2^{107} 2^{75n} m^{65} \log^{19}(H) B^{1/2} \log^5 B.$$

D'autre part, la somme sur ω fait intervenir au plus 2^n termes. On a donc

$$S(B) \leq 2^{107} 2^{76n} m^{64} \log^{19}(H) B^{1/2} \log^5 B.$$

En prenant en compte le nombre de solutions de $a_0(T)D(T) = 0$, ce qui ne change que la constante, on en déduit que le nombre d'entiers positifs t inférieurs à B tels que la spécialisation $F(t, Y)$ est réductible sur $\mathbb{Q}$ est plus petit que

$$2^{108} 2^{76n} m^{64} \log^{19}(H) B^{1/2} \log^5 B.$$

Pour trouver s spécialisations t qui ne satisfont pas à cette condition, il suffit alors de rendre cette quantité strictement inférieure à $B - s$, ce qui est le cas si on choisit

$$B \geq (s + 2^{108} 2^{76n} m^{64} \log^{19}(H))^4.$$

On obtient donc la nouvelle version effective du théorème d'irréductibilité de Hilbert donnée par le théorème 4.0.3.

Remarques. *(a)* Ce résultat améliore les dépendances en le degré et en la hauteur de F par rapport à la borne donnée par Schinzel et Zannier. On n'obtient toujours pas de borne polynomiale en le degré, ceci en raison du nombre et du degré des polynômes issus de la réduction. Il semble qu'il soit difficile d'améliorer ce résultat dans le cas général sans éviter cette réduction. Cependant, nous allons voir dans la section suivante que dans le cas où l'extension définie par le polynôme F est galoisienne, alors une modification de cette réduction va nous permettre d'obtenir une borne polynomiale.

(b) Le résultat de la section précédente nous permet également de donner directement une borne polynomiale pour les polynômes unitaires en Y et dont le degré en Y vaut 2 ou 3. En effet, dans ce cas, il y a équivalence pour un polynôme à une variable entre être irréductible sur $\mathbb{Q}$ et ne pas avoir de racine dans $\mathbb{Z}$.

4.4 Théorème de Hilbert effectif - cas galoisien

Si on analyse la provenance des termes exponentiels dans la borne fournie par le théorème 4.0.3, on voit deux origines : le degré des polynômes issus de la réduction et leur nombre. Sous l'hypothèse que F définit une extension galoisienne de $\mathbb{Q}(T)$, nous allons voir qu'il est facile de baisser le degré de ces polynômes. D'autre part, une modification de la réduction va nous permettre, *via* un résultat récent de théorie des groupes, de contrôler également le nombre de polynômes à considérer et donner ainsi une borne polynomiale pour le théorème d'irréductibilité de Hilbert (théorème 4.0.4). Nous terminerons par une remarque sur la possibilité de généraliser cette méthode sous des conditions plus faibles sur l'extension définie par F.

4.4.1 Nouvelle réduction

Nous allons modifier la réduction habituelle afin de ne considérer que des polynômes définissant des extensions minimales parmi les extensions intermédiaires entre $\mathbb{Q}(T)$ et la clôture galoisienne de F. Nous verrons que les degrés et hauteurs restent d'un ordre de grandeur convenable.

On note N la clôture galoisienne de F. Comme pour la réduction classique, on note P_ω le polynôme minimal d'un élément $\theta_\omega = a_0(T)\tau_j\{y_i \ : \ i \in \omega\}$ appartenant à $N \setminus \mathbb{Q}(T)$. Soit maintenant un corps k_ω minimal satisfaisant $\mathbb{Q}(T) \subsetneq k_\omega \subseteq \mathbb{Q}(T, \theta_\omega)$, et $p_\omega(Y) \in k_\omega[Y]$ le polynôme minimal de θ_ω sur k_ω. Un des coefficients de p_ω est dans $k_\omega \setminus \mathbb{Q}(T)$ car sinon $p_\omega = P_\omega$ et k_ω serait $\mathbb{Q}(T)$. On note η_ω ce coefficient. Il s'écrit comme fonction symétrique élémentaire des racines de p_ω, donc de conjugués de θ_ω. On a alors par minimalité $k_\omega = \mathbb{Q}(T, \eta_\omega)$. Soit alors $R_\omega(T, Y)$ le polynôme minimal de η_ω sur $\mathbb{Q}(T)$. On sait que η_ω est entier sur $\mathbb{Z}[T]$, et donc R_ω est dans $\mathbb{Z}[T, Y]$, et est unitaire en Y.

Soit désormais $t \in \mathbb{Z}$ tel que $F(t, Y)$ est réductible sur $\mathbb{Q}$ et vérifiant $a_0(t)D(t) \neq 0$. Dans ces conditions, on peut définir un morphisme de spécialisation $\mathbb{Q}[T, y_1, \ldots, y_n] \to \overline{\mathbb{Q}}$ qui prolonge la spécialisation $T \to t$. Pour $z \in \mathbb{Q}[T, y_1, \ldots, y_n]$, on notera $z(t)$ l'image de z par ce morphisme, *i.e.* la "valeur de z en t". Il existe un sous-ensemble ω de $\{1, \ldots, n\}$ tel que $\theta_\omega(t)$ est un zéro entier de $P_\omega(t, Y)$ (il s'agit de la réduction classique), et $\eta_\omega(t)$ est alors un zéro entier de $R_\omega(t, Y)$. On peut donc énoncer un analogue du lemme 1.3.2 en remplaçant les P_ω par ces polynômes R_ω, lesquels sont en nombre inférieur ou égal au nombre d'extensions minimales entre $\mathbb{Q}(T)$ et

N.

Lemme 4.4.1. *Pour tout $t \in \mathbb{Z}$, si $a_0(t)D(t) \neq 0$ et $F(t, Y)$ est réductible sur $\mathbb{Q}$, alors un des polynômes $R_\omega(t, Y)$ a un zéro entier.*

Supposons désormais que l'extension définie par F est galoisienne. Ceci va nous permettre de majorer de façon efficace le degré et le nombre des extensions k_ω construites ci-dessus. On discutera ensuite dans une remarque des conditions plus générales que doit vérifier l'extension définie par F pour que cette méthode donne une borne polynomiale.

4.4.2 Estimation du degré et de la hauteur de R_ω

Par construction, l'extension k_ω est une sous-extension de l'extension galoisienne $\mathbb{Q}(T, y_1) = N$. Donc le degré en Y de R_ω, qui est égal au degré $[k_\omega : \mathbb{Q}(T)]$, est majoré par le degré en Y de F. C'est-à-dire $\deg_Y R_\omega \leq n$.

Afin d'estimer le degré en T, il suffit d'estimer le degré en T de chaque coefficient de R_ω vu comme polynôme en Y

$$R_\omega(T, Y) = Y^k + \sum_{i=1}^{k} R_i(T) Y^{k-i}.$$

Pour chaque $t \in \mathbb{C}$ fixé, $R_i(t)$ est, au signe près, la i-ème fonction symétrique élémentaire en les zéros de $R_\omega(t, Y)$. Ceux-ci sont les conjugués de $\eta_\omega(t)$, qui est lui-même fonction symétrique élémentaire de conjugués de $\theta_\omega(t)$. Or, on a l'estimation suivante, due au fait que $\theta_\omega(t)$ est encore fonction symétrique élémentaire d'un ensemble de zéros de F et obtenue à l'aide de comparaisons classiques entre mesure de Mahler et hauteur usuelle :

$$|\theta_\omega(t)| \leq 2^n (m+1) H \max(1, |t|^m).$$

On obtient donc, pour $|t| \geq 1$,

$$|R_i(t)| \leq 2^i (2^{2n^2} (m+1)^n H^n |t|^{mn})^i = O(|t|^{mni})$$

et donc $\deg(R_i) \leq mni$ et $\deg_T(R_\omega) \leq mn^2$.

On peut également donner une majoration du degré total $\deg(R_\omega) \leq 2mn^2$.

Pour estimer la hauteur, on utilise la même méthode que pour la hauteur de P_ω.

L'inégalité de Cauchy nous permet d'écrire

$$H(R_\omega) \leq \sup_{|z| \leq 1} ||R_\omega(z, Y)||$$

où $||R_\omega(z,Y)||$ est le maximum des modules des coefficients de $R_\omega(z,Y) \in \mathbb{C}[Y]$. Puis $||R_\omega(z,Y)||$ est majoré en utilisant la mesure de Mahler, ce qui nous donne, pour $|z| \leq 1$,

$$||R_\omega(z,Y)|| \leq 2^n(2^{2n^2}(m+1)^n H^n)^n$$

soit

$$H(R_\omega) \leq 2^{3n^3}(m+1)^{n^2} H^{n^2}.$$

4.4.3 Estimation de $S_\omega(B)$

Nous allons refaire les estimations de $S_\omega(B)$ dans le cas galoisien. Connaissant le degré et la hauteur des polynômes R_ω, il suffit d'appliquer une nouvelle fois l'estimation (4.2) de la section 2.4, ce qui donne

$$S_\omega(B) \leq 2^{164} m^{64} n^{147} \log^{19}(H) B^{1/2} \log^5 B$$

D'autre part, la somme sur ω correspond au nombre d'extensions minimales non triviales entre $\mathbb{Q}(T)$ et $\mathbb{Q}(T, y_1)$, qui est, par la théorie de Galois, égal au nombre de sous-groupes maximaux d'un groupe fini d'ordre n. Or, on trouve une telle estimation dans [LuSe] (Th.11.3.4 de L.Pyber) :

Théorème (L. Pyber). *Il existe une constante absolue c telle que pour tout groupe fini G, le nombre de sous-groupes maximaux de G est au plus $(\sharp G)^c$.*

En prenant en compte également le nombre de solutions de $a_0(T)D(T) = 0$, on en déduit que le nombre d'entiers positifs t inférieurs à B tels que la spécialisation $F(t,Y)$ est réductible sur $\mathbb{Q}$ est plus petit que

$$2^{165} m^{64} n^{147+c} \log^{19}(H) B^{1/2} \log^5 B.$$

Pour trouver s spécialisations t qui ne satisfont pas à cette condition, il suffit alors de rendre cette quantité strictement inférieure à $B - s$, ce qui est le cas si on choisit

$$B \geq (s + 2^{165} m^{64} n^{147+c} \log^{19}(H))^4.$$

On obtient ainsi la nouvelle version effective du théorème d'irréductibilité de Hilbert sous l'hypothèse que l'extension définie par le polynôme F soit galoisienne donnée par le théorème 4.0.4.

Remarques *(a)* De façon générale (c'est-à-dire sans condition sur l'extension définie par F), l'inégalité $\deg_Y R_\omega \leq n$ peut être remplacée par $\deg_Y R_\omega = [G : M]$, où $G = \mathrm{Gal}(N/\mathbb{Q}(T))$ et M est un sous-groupe maximal de G. En notant $\Gamma = \mathrm{Gal}(N/\mathbb{Q}(T, y_1))$, qui est d'indice n dans G, la condition suivante est suffisante pour obtenir une borne polynomiale :

(*) Il existe une constante A telle que

$$\sum_{\substack{M<G \\ M \text{ maximal}}} [G : M] \leq [G : \Gamma]^A.$$

On voit ainsi que si N est de degré une puissance de n sur $\mathbb{Q}(T)$ d'exposant borné par une constante absolue, cette condition est vérifiée grâce au théorème de Pyber et la borne obtenue par la méthode reste donc polynomiale.

(b) On peut également énoncer une condition de pure théorie des groupes qui, si elle était vraie, donnerait une borne polynomiale pour le cas général :

(**) Il existe une constante a absolue telle que pour tout groupe G fini,

$$\sum_{\substack{M<G \\ M \text{ maximal}}} [G : M] \leq \left(\min_{\substack{\Gamma<G,\ \Gamma\neq G \\ \cap_{g\in G}\Gamma^g=\{1\}}} [G : \Gamma] \right)^a$$

où la condition sur les $\Gamma^g = g\Gamma g^{-1}$ assure que N est la cloture galoisienne de $\mathbb{Q}(T, y_1)$.

Cette condition revient à dire que l'action $G \to S_n$ (où $n = [G : \Gamma]$) par translation sur les classes de G modulo Γ est fidèle. Le membre de droite est donc égal à une puissance du plus petit degré $n > 1$ d'une représentation transitive et fidèle $G \to S_n$. On peut alors citer deux types de contre-exemples :

- Il peut exister un sous-groupe maximal d'indice trop élevé : c'est le cas si G est représenté naturellement par A_n. Il existe alors (voir [DiMo]) des sous-groupes maximaux d'indice supérieur à toute puissance de n.
- Il peut y avoir trop de sous-groupes maximaux. C'est le cas par exemple si G est un 2-groupe transitif qui ne peut être engendré par moins de $\dfrac{n}{\sqrt{\log n}}$ éléments (l'existence de tels groupes est prouvée dans [KoNew]). Le groupe G possède alors $2^{n/\sqrt{\log n}}$ sous-groupes maximaux d'indice 2, ce qui rend impossible la condition (**).

Chapitre 5

Algorithme de factorisation d'un polynôme à deux variables

Soit $F(T,Y) \in \mathbb{Z}[T,Y]$, qu'on peut supposer de contenu égal à 1. On notera m et n les degrés respectivement en T et Y de F et d le degré total. On cherche à trouver sa factorisation dans $\mathbb{Z}[T,Y]$:

$$F(T,Y) = \prod_{i=1}^{r} F_i(T,Y)^{\alpha_i}$$

où pour tout $i = 1,\ldots,r$, $F_i(T,Y) \in \mathbb{Z}[T,Y]$ est irréductible sur $\mathbb{Q}$ et de contenu égal à 1, et $F_i \neq F_j$ pour $i \neq j$.

Notons $F_i(T,Y) = \sum_{j=0}^{m} F_{i,j}(T)Y^j$. Les inconnues sont donc les coefficients de chaque $F_{i,j}(T)$.

5.1 Spécialisation et factorisation

Supposons qu'on puisse trouver un nombre t_1 tel que tous les polynômes spécialisés $F_i(t_1,Y)$ soient irréductibles sur $\mathbb{Q}$. La factorisation

$$F(t_1,Y) = \prod_{i=1}^{r} F_i(t_1,Y)^{\alpha_i}$$

est alors la décomposition de $F(t_1,Y)$ en irréductibles de $\mathbb{Q}[Y]$. Or, celle-ci peut-être déterminée à partir de $F(t_1,Y)$ en utilisant par exemple l'algorithme de Lenstra-Lenstra-Lovàsz (voir [LeLeLo]) et est donc donnée indépendamment par :

$$F(t_1,Y) = \prod_{i=1}^{s} \pi_i^{t_1}(Y)^{\beta_i}$$

avec $\pi_i^{t_1}(Y) \in \mathbb{Z}[Y]$ irréductibles sur $\mathbb{Q}$ et $\pi_i^{t_1} \neq \pi_j^t$ pour $i \neq j$.

Supposons de plus que t_1 peut être choisi de façon à ce que $F_i(t_1, Y) \neq F_j(t_1, Y)$ pour $i \neq j$. On obtient alors par unicité de la factorisation que $r = s$ et les degrés en Y des différents facteurs qu'on notera $d_i = \deg_Y(F_i)$. On pourra donc chercher les facteurs F_i sous la forme

$$F_i(T, Y) = \sum_{j=0}^{d_i} F_{i,j}(T) Y^j, \quad i = 1, \ldots, r$$

où les $F_{i,j}(T)$ sont de degré inférieur à m et vérifient

$$F_{i,j}(t_1) = \pi_{i,j}^{t_1} \quad i = 1, \ldots, r \text{ et } j = 0, \ldots, d_i$$

si on note $\pi_i^{t_1}(Y) = \sum_{j=0}^{d_i} \pi_{i,j}^{t_1} Y^j$ pour $i = 1, \ldots, r$.

Si on fait la même chose pour une autre spécialisation, disons t_2, on va identifier de nouveau les facteurs de même degré de $F(t_2, Y)$ et $\pi(Y)$. Il faut alors faire attention au phénomène suivant : si $F(T, Y)$ a plusieurs facteurs de même degré en Y, il faut savoir à quel facteur se rapporte chaque facteur $\pi_i^{t_2}(Y)$ ayant ce degré. Voyons ceci sur un exemple :

Exemple 5.1.1. *Soit* $F(T, Y) = Y^4 - TY^3 + (T+1)Y^2 + (T^2 - T)Y - 2T^2 + 2T$. *Supposons que l'on sache que les spécialisations* $T = 3, 4$ *et* 6 *conviennent, on a*

$$F(3, Y) = (Y^2 - 2)(Y^2 - 3Y + 6)$$
$$F(4, Y) = (Y^2 - 3)(Y^2 - 4Y + 8)$$
$$F(6, Y) = (Y^2 - 5)(Y^2 - 6Y + 12)$$

On pose alors $F(T, Y) = F_1(T, Y)F_2(T, Y)$ et il faut déterminer pour chaque spécialisation t quel facteur est $F_1(t, Y)$ et quel facteur est $F_2(t, Y)$. Pour cela, une idée est de choisir la première spécialisation t_1 comme ci-dessus, puis de chercher les autres spécialisations sous la forme $t_1 + mp$, où p est un premier tel que des facteurs distincts de F restent distincts *modulo* p. Ainsi, on reconnaît chaque facteur en regardant sa réduction *modulo* p.

On peut donc effectuer ce raisonnement pour trouver un nombre N de spécialisations de cette forme. Le problème est alors ramené à résoudre $\sum_{i=1}^{r} d_i$ systèmes linéaires de N équations à $m + 1$ inconnues. En choisissant $N = m + 1$, ces systèmes sont de Cramer et ont une solution unique, ce qui nous donne les coefficients recherchés.

Conclusion : le problème est de pouvoir déteminer effectivement suffisamment d'entiers tels que les spécialisations des polynômes F_i en ces entiers

soient irréductibles et tels que deux F_i distincts ne deviennent pas égaux quand on spécialise.

Pour cela, nous allons d'abord décrire comment trouver effectivement le premier t, puis nous donnerons la démarche pour en trouver d'autres.

5.2 Étape 1

La première étape consiste à trouver une spécialisation $t \in \mathbb{Z}$ vérifiant les conditions suivantes :
(1) Pour $i = 1, \ldots, r$, $F_i(t, Y)$ irréductible sur $\mathbb{Q}$.
(2) Pour tout $i \neq j$, on doit avoir $F_i(t, Y) \neq F_j(t, Y)$.

Propriété (1) Les différentes versions effectives du théorème de Hilbert mènent à une borne sous laquelle on est assuré de trouver autant de bonnes spécialisations que l'on veut, borne qui dépend du degré, de la hauteur, du nombre de poynômes et du nombre de spécialisations voulues. Il nous faut donc commencer par borner le degré et la hauteur des polynômes F_i.

Lemme 5.2.1. *Les polynômes F_i vérifient les propriétés suivantes :*

1. $\deg_t(F_i) \leq m$
2. $\deg_Y(F_i) \leq n$
3. $\deg(F_i) \leq 2d$
4. $H(F_i) \leq e^{2d} H(F)$

Preuve. Par construction, on obtient que les degrés partiels des F_i sont majorés par les degrés partiels respectifs de F. Donc $\deg(F_i) \leq 2\deg(F)$. En ce qui concerne la hauteur, l'idée est d'utiliser les résultats de la section 1.2.1 qui permettent de relier la hauteur à la mesure de Mahler qui est multiplicative. En effet, on obtient ainsi que

$$H(F_i) \leq \prod_{j=1}^{r} H(F_j) \leq 2^{2d} \prod_{j=1}^{r} M(F_j) \leq 2^{2d}(1+d)H(F) \leq e^{2d} H(F)$$

□

On obtient donc, en appliquant par exemple le théorème 4.0.4 de la section 4.4, l'existence d'un nombre k de spécialisations vérifiant (1) et inférieures

à une borne $C(k, 2d, e^{2d}H)$. Pour trouver explicitement ces spécialisations, il suffit de factoriser toutes les spécialisations $F(t, Y)$ pour t allant de 0 à $C(k, 2d, e^{2d}H)$. Les spécialisations qui conviennent sont celles pour lesquelles le nombre de facteurs comptés avec multiplicité est minimal. En effet, en cas de réductibilité, un facteur au moins se transforme en plusieurs facteurs. Notons que l'application du théorème donne l'assurance qu'en testant toutes les spécialisations jusqu'à cette borne, il y en a au moins k qui ne changent pas le nombre de facteurs.

Propriété (2) On va estimer le nombre de spécialisations pour lesquelles la condition (2) n'est pas vérifiée. En effet, F contient au plus d facteurs irréductibles, il suffit donc d'empecher qu'un couple de facteurs aient la même spécialisation. Il y a strictement moins de d^2 couples et pour chaque couple, il y a au plus $\deg_T(F)$ spécialisations à éviter (en effet, $F_i(T, Y) \neq F_j(T, Y)$ donc il existe k tel que $F_{i,k}(T) \neq F_{j,k}(T)$, mais alors $F_{i,k}(t)$ ne peut être égal à $F_{j,k}(t)$ que pour au plus $\deg_T(F)$ spécialisations t). On peut donc dire que la condition (2) n'est pas vérifiée pour strictement moins de d^3 spécialisations.

Si on applique le théorème de Hilbert effectif avec $k = d^3$, alors on est assuré de l'existence d'au moins une spécialisation t_1 vérifiant les conditions (1) et (2) et inférieure à $C(d^3, 2d, He^{2d})$. Pour la trouver, on regarde les factorisations de toutes les spécialisations $F(t, Y)$ pour t de 0 à $C(d^3, 2d, He^{2d})$ et on procède en deux temps :
- on garde toutes les spécialisations telles que le nombre de facteurs, comptés avec multiplicité, est minimal (ainsi, t vérifie (1)),
- puis parmi celles-ci, on en prend une telle que le nombre de facteurs distincts est maximal (ainsi, t vérifie (2)).

A la fin de cette étape, on a trouvé de manière totalement explicite une spécialisation t_1 telle que

$$(*) \quad F(t_1, Y) = \prod_{i=1}^{r} F_i(t_1, Y)^{\alpha_i}$$

est la factorisation en irréductibles de $F(t_1, Y)$.

5.3 Étape 2

Nous allons désormais chercher d'autres spécialisations t_i satisfaisant les mêmes conditions (1) et (2) (i.e. donnant le même nombre de facteurs distincts et les mêmes exposants que $(*)$) et nous allons les chercher de sorte

qu'il soit facile de reconnître le facteur de provenance de chaque facteur irréductible de $F(t_i, Y)$ (voir l'exemple 5.1.1).

Pour cela, il suffit de chercher $t_2, \ldots, t_{m+1}$ dans la partie hilbertienne associée aux polynômes $Q_i(T, Y) = F_i(t_1 + pT, Y)$, $i = 1, \ldots, r$, avec p tel que les réductions de $F_i(t_1, Y)$ et $F_j(t_1, Y)$ sont distinctes si $i \neq j$. On peut par exemple choisir un p qui ne divise pas le discriminant du polynôme $\tilde{F}(t_1, Y) = \prod_{i=1}^{r} F_i(t_1, Y)$.

On applique alors l'étape 1 aux polynômes Q_i afin de trouver cette fois-ci m spécialisations vérifiant (1) et (2). Il suffit de tester les spécialisations jusqu'à la borne $C(d'^3+m, d', H')$, où d' et H' sont respectivement des majorants des degré et hauteur des Q_i. On choisit pour $t_2, \ldots, t_{m+1}$ les spécialisations pour lesquelles la factorisation donne le même nombre de facteurs comptés avec multiplicité et le même nombre de facteurs distincts que $F(t_1, Y)$.

Afin d'estimer cet algorithme, on a besoin d'estimer d', H' et p. Le lemme suivant donne les deux premières estimations.

Lemme 5.3.1. *Les polynômes $Q_i(T, Y)$ ont les propriétés suivantes :*

1. $d' \leq 2d$
2. $H' \leq p^d e^d H C(d^3, 2d, e^d H)$

Preuve. On a

$$d' = \deg(Q_i) \leq \deg F_i \leq 2d$$

et

$$H' = H(Q_i(t_1 + pT, Y)) \leq e^{2d} |t_1|^d p^d H \leq e^{2d} C(d^3, 2d, e^d H)^d p^d H$$

□

Lemme 5.3.2. *On note Δ le discriminant du polynôme $\tilde{F}(t_1, Y)$.Le nombre de premiers qui divisent Δ est inférieur à $2d \log(e^{2d}|t_1|H)$.*

Preuve. On a

$$\sharp\{p \text{ premier; } p \mid \Delta\} \leq \frac{\log(\Delta)}{\log 2}$$

or l'expression avec le déterminant donne

$$|\Delta| \leq (2 \deg(\tilde{F}))^{2 \deg(\tilde{F})} H(\tilde{F})^{2 \deg(\tilde{F})}$$

et on peut estimer les degré et hauteur de $\tilde{F}(t_1, Y)$:

$$\begin{cases} \deg(\tilde{F}) \leq d \\ H(\tilde{F}(t_1, Y)) \leq e^{\deg(F(t_1, Y))} H(F(t_1, Y)) \leq e^{2d} |t_1|^d H \end{cases}$$

On a donc :

$$\sharp\{p \text{ premier; } p \mid \Delta\} \ < \ 2d \log(e^{2d}|t_1|H)$$

□

On est alors assuré de trouver un p qui ne divise pas Δ si on en teste $[2d\log(e^{2d}|t_1|H)] + 1$.

5.4 Étude de la complexité

D'après les estimations données dans les sections précédentes, on peut dire que cet algorithme est polynomial à condition qu'il soit possible de trouver une bonne spécialisation pour le théorème de Hilbert en temps polynomial en d et en $\log(H)$.

Bibliographie

[Ay] M. Ayad, *Irréductibilité des polynômes à plusieurs variables*, Cours de DEA, Université de Lille I, (2000/2001).

[BP] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J., **59** (1989), 337–357.

[Co] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc., (3) **43** (1981), 227–250.

[De1] P. Dèbes, *Valeurs algébriques de fonctions algébriques et théorème d'irréductibilité de Hilbert*, Thèse 3ème cycle, Univ. P. et M. Curie (Paris VI), (1984).

[De2] P. Dèbes, *Parties hilbertiennes et progressions géométriques*, C. R. Acad. Sci. Paris Sér. I, **302** (1986), 87–90.

[De3] P. Dèbes, *Hilbert subsets and s-integral points*, Manuscripta Math., **89** (1996), 107–137.

[DiMo] J.D. Dixon and B. Mortimer, *Permutation groups*, Springer, 1996.

[Do] K. Dörge, *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*, Math. Ann., **96** (1927), 176–182.

[Ei] M. Eichler, *Zum Hilbertschen Irreduzibilitätssatz*, ibid., **116** (1939), 742–748.

[Fr] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory, **6** (1974), 211–231.

[FrJa] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, (1986).

[Gao] S. Gao, *Factoring multiariate polynomials via partial diferential equations*, Math. Comp., **72** (2003), 801–822.

[HB] D. R. Heath-Brown, *The Density of Rational Points on Curves and Surfaces*, Annals of Math., **155** (2002), 553–595.

[H] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math., **110** (1892), 104–129 = Gesammelte Abhandlungen, Bd. II, Springer, 1970, 264–286.

[HiSi] M. Hindry and J. H. Silverman, *Diophantine Geometry : An Introduction*, Springer, 2000.

[In] E. Inaba, *Über den Hilbertschen Irreducibilitätssatz*, Japan. J. Math., **19** (1944), 1–25.

[KoNew] L.G. Kovàcs and M.F. Newman, *Generating transitive permutation groups*, Quart. J. Math. Oxford Ser., **39** (1988), 361–372.

[Ld] E. Landau, *Sur quelques théorèmes de M. Petrovich relatifs aux zéros des fonctions analytiques*, Bull. Soc. Math. France, **33** (1905), 1–11.

[LaWe] S. Lang and A. Weil, *Number of points on varieties in finite fields*, Amer. J. Math., **76** (1954), 819–827.

[LeLeLo] A. K. Lenstra and H. W. Lenstra and L. Lovàsz, *Factoring polynomials with rational coefficients*, Math. Ann., **261** (1982), 515–534.

[LuSe] A. Lubotzky and D. Segal, *Subgroup growth*, Progress in Mathematics 212, Birkhäuser Verlag, Basel, 2003.

[Me] F. Mertens, *Über die Zerfällung einer ganzen Funktion einer Veränderlichen in zwei Faktoren*, Sitzungsberg. K. Akad. Wiss. Wien, **120** (1911), Math. Naturwiss. Cl., 1485–1502.

[Ro] P. Roquette, *Nonstandard aspects of Hilbert's irreducibility theorem*, in : Model Theorey and Algebra (A memorial tribute to Abraham Robinson), Lecture Notes in Math. 498, Springer, 1966, 209–266.

[Ost] A.M. Ostrowski, *Über die Bedeutung der Theorie der konvexen Polyheder für formale Algebra*, Jahresber. Deutsche Math.-Verein., **30** (1921),98–99.

[ScZa] A. Schinzel and U. Zannier, *The least admissible value of the parameter in Hilbert's Irreducibility Theorem*, Acta Arith.,**69.3** (1995), 293–302.

[Sch] W. M. Schmidt, *Diophantine approximations and diophantine equations*, Lecture Notes in Mathematics,**1467**.

[Si] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Phys. Math. Klasse, **1** (1929) = Gesammelte Abhandlungen, Bd. I, Springer, 1966, 209–266.

[Sk] T. Skolem, *Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen*, Kristiania Vid. Selskab. Skrifter I, **17** (1921).

[Spr] V. G. Sprindžuk, *Diophantine equations involving unknown primes*, Trudy Mat. Inst. Steklov., **158** (1981), 180–196 (in Russian).

[Za] U. Zannier, *On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$*, Arch. Math., **68** (1997), 129–138.

Résumé

Le théorème d'irréductibilité de Hilbert assure l'existence d'une spécialisation conservant l'irréductibilité d'un polynôme à plusieurs variables et à coefficients rationnels. Des versions effectives ont été données par P. Dèbes (1993) puis par U. Zannier et A. Schinzel (1995). Nous proposons ici diverses tentatives d'améliorer ces résultats effectifs : méthode de Dörge, méthode des congruences inspirée par un article de M. Fried et enfin une utilisation des résultats récents de R. Heath-Brown sur les points entiers d'une courbe algébrique. Cette dernière voie va nous permettre d'améliorer significativement les résultats connus. On finira par une application à la recherche d'un algorithme polynomial pour la factorisation d'un polynôme à deux indéterminées.

Mots-clés. Théorème d'irréductibilité de Hilbert, Polynômes, Géométrie diophantienne, Courbes algébriques, Factorisation, Algorithme polynomial.

Abstract

Hilbert's irreducibility theorem gives the existence of a specialization preserving the irreducibility of a multivariate polynomial with rational coefficients. Effective versions have been given by P. Dèbes (1993) and by A. Schinzel and U. Zannier (1995). We discuss some attempts to improve these effective results : Dörge's method, congruence method inspired by an article of M. Fried and finally the use of a recent result of R. Heath-Brown about rational points on curves. This last attempt leads to a significant improvement of known results. We also give an application to the research of an algorithm for the factorization of bivariate polynomials.

Keywords. Hilbert's irreducibility theorem, Polynomials, Diophantine Geometry, Algebraic Curves, Factorisation, Polynomial Algorithm.