Laboratoire Paul Painlevé

Université de Lille

CEMPI CENTRE EUROPÉEN POUR LES MATHÉMATIQUES, LA PHYSIQUE ET LEURS INTERACTIONS

École Doctorale des Sciences Pour l'Ingénieur

THÈSE

Spécialité Mathématiques et leurs interactions

pour obtenir le grade de docteur délivré par

l'Université de Lille

présentée et soutenue publiquement par

François MOTTE

le 31 mai 2019

De la géométrie à l'arithmétique en théorie inverse de Galois

---

sous la direction du professeur **Pierre DÈBES**

Jury

M. Lior Bary-Soroker	Professor, Tel Aviv	Rapporteur
M. Arno Fehm	Professor, Dresde	Rapporteur
Mme Sara Checcoli	Maître de Conférences, Grenoble	Examinateur
M. Raf Cluckers	Directeur de Recherches, Lille	Examinateur
M. Danny Neftin	Professor, Haifa	Examinateur
M. Pierre Dèbes	Professeur, Lille	Directeur

Université de Lille
Laboratoire Paul Painlevé
UMR CNRS 8524, 59655 Villeneuve d'Ascq Cedex, France

Remerciements

Je tiens à remercier ici toutes les personnes qui m'ont écouté, soutenu, aidé pendant cette fabuleuse aventure qu'est la thèse.

Merci d'abord à mon directeur de thèse, Pierre Dèbes. C'est un honneur de travailler sous sa direction. Merci pour les conseils, les encouragements, la patience et la disponibilité. Je n'aurais su en arriver là sans son encadrement et sa personne qui font de lui un directeur en or. Je n'oublierai jamais ces discussions mathématiques, marchant dans les rues, en visite lors de conférences étrangères, ces remarques prises sur le ton de l'humour pour pointer une erreur, ces longues heures à travailler l'anglais et ces conseils qui dépassent le cadre mathématiques. Merci !

Merci à Arno et Lior d'avoir accepté de prendre le temps de relire mon travail et pour leurs retours précieux et constructifs. Je remercie également Sara, Danny et Raf d'avoir accepté d'être membre du jury.

*****

Je tiens à exprimer ma gratitude aux membres du laboratoire Paul Painlevé. Merci d'abord à tous les membres de l'équipe AGA que j'ai pu côtoyer ainsi qu'aux invités lors de séminaires. Un grand merci aussi aux responsables des tâches administratives et bibliothécaires sans qui le laboratoire ne pourrait fonctionner.

Merci également aux collègues doctorants. Vous avez fait l'objet de belles rencontres, de soutiens et d'amitiés. D'abord merci à ceux qui m'ont accueilli en première année. Je pense principalement à Adel, Fadil, Loic, Florian. Je vous ai vu en cours de thèse, la terminer et vos conseils autour de discussions en tout genre ont été précieux. Merci à ceux que j'ai pu côtoyer à partir de la deuxième année, Jacques, Robin, Stefana, Clément, Tonie, Sidy, Angelo et bien d'autres. Merci à Alexandre, aussi membre de mon équipe et avec qui j'ai préparé un exposé au séminaire des doctorants. Merci à Meryem, Mohammed et Joanna avec qui j'ai échangé d'innombrables discussions, rires, soutiens moraux et cafés. Enfin, un grand merci à Octave avec qui nous nous sommes soutenus et encouragés mutuellement depuis le Master 2, autant au laboratoire qu'en dehors.

*****

Mes années de thèse ont été aussi des années passées sur des terrains de badminton à frapper à répétition dans des volants sans jamais se lasser. Ceux qui y sont présent le savent bien. J'ai pu trouver dans ce sport une sorte de refuge pour me vider l'esprit lors de périodes compliquées et je tiens à remercier les personnes qui ont été membres du club de Villeneuve d'Ascq avec qui j'ai pu échanger lors de ces années de thèses. En particulier ceux avec qui je passe (ou j'ai passé, pour ceux qui sont partis) le plus clair de mon temps libre. Ils sont trop nombreux pour que je les cite tous ici. Avec leur soutien moral et pour certain(e)s une expérience de la recherche, ils ont tous contribué de près ou de loin, à l'aboutissement de cette thèse. Je ne compte plus le nombre de soirées passées avec eux que ce soit sur les terrains ou en dehors. Merci à vous les amis !

*****

Je remercie enfin ma famille, mes parents, mon frère, mes sœurs, mes cousins, cousines, oncles et tantes... dont le soutien est sans faille et ce tout au long de mes études et de ma vie. Je mets en avant mes parents, Thérèse et Damien Motte, sans qui je ne serai pas celui que je suis aujourd'hui. Ils n'ont pas fait que m'élever, ils sont également devenus un soutien inconditionnel sur lequel je peux m'appuyer tous les jours.

Table des matières

Introduction

Les opérations élémentaires comme l'addition ou la multiplication sont des concepts clés et inévitables dans la compréhension du monde qui nous entoure. Ces notions que l'on apprend dès le plus jeune âge, forgent les débuts de l'algèbre. Du temps de Pythagore, vers l'an -580, la philosophie imposait à l'homme l'idée d'une nature ordonnée et *rationnelle*. Dans leur compréhension géométrique des nombres, les grecs ne concevaient pas que des nombres puissent être autre chose que des quotients de deux nombres entiers, que l'on appelle aujourd'hui *le corps des nombres rationnels*. La compréhension de ce concept de nombre irrationnel n'est pas si simple. Pour preuve, on retrouve cette difficulté dans les salles de classes. Qu'est ce que $\sqrt{2}$? C'est environ 1.41 ? Oui environ, mais ce n'est pas 1.41. Le théorème de Pythagore peut introduire ce nombre et, en leur temps, les grecs admettaient mal que la longueur de l'hypoténuse d'un triangle isocèle rectangle dont deux cotés valent 1 ne soit pas un nombre rationnel. Ce théorème peut nous envoyer directement à la notion de polynôme et aux équations polynômiales. Désignons les longueurs de notre triangle par x, y et z, z étant la longueur de l'hypoténuse. Le théorème nous dit que $x^2 + y^2 = z^2$. Il s'agit d'une équation polynômiale de degré 2. Très vite, les équations polynômiales et la recherche de racines de polynômes allaient devenir un domaine d'étude très prisé des mathématiciens comme en attestent les travaux des algébristes du moyen âge. Pouvons-nous déterminer tous les nombres x solution de l'équation $ax^2 + bx + c = 0$? Que se passe t-il si on augmente le degré ? A la Renaissance, on savait résoudre ce type d'équation aux degrés $1, 2, 3$, et 4 mais le cas du degré 5 resta sans réponse pendant des siècles. Il fallut attendre le XIXe siècle avec Galois pour montrer que ce n'était pas forcément possible pour les degrés plus grands que 5.

La théorie de Galois voit ainsi ses origines dans l'étude d'équations polynômiales et ce que l'on appelle *extensions de corps*. Même si les travaux d'Evariste Galois n'étaient pas considérés par toute la communauté mathématique de son époque, il en résultat finalement une théorie à son nom qui donnera une nouvelle dimension à l'arithmétique : on allait étudier les opérations élémentaires sur d'autres objets que $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. On étudiera par exemple les extension finie de $\mathbb{Q}$, que l'on appelle des *corps de nombres*. Cette théorie établit un lien

puissant entre la *théorie des groupes* et celle des extensions de corps. Ce lien permet de donner des résultats profonds en arithmétique. Certains attribuent même à Galois l'invention de la notion de groupes voire de l'algèbre moderne et on ne remet plus en cause l'utilité de cette théorie en mathématique. Le théorème fondamental de la théorie de Galois montre que l'on peut associer à des extensions de corps, un groupe dit *groupe de Galois* de l'extension. Par exemple, l'extension finie $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ où $\mathbb{Q}(\sqrt{3})$ désigne l'e corps de nombres composé d'éléments du type $a+\sqrt{3}.b$ où a et b sont deux nombres rationnels, a pour groupe de Galois le groupe bien connu à deux éléments : $\mathbb{Z}/2\mathbb{Z}$. Deux extensions ayant même groupe de Galois sont très semblables et la détermination de ce groupe apprend énormément sur la structure de l'extension, elle est cependant souvent délicate. La compréhension des groupes de Galois des corps de nombres est encore très lacunaire, même si des progrès spectaculaires ont été réalisés depuis le début du XXe siècle. Le fait reste qu'à une extension donnée, on peut généralement lui associer un groupe. Il est apparu alors naturel de se poser la question inverse : si on se donne un groupe, disons G, existe t-il une extension de corps dont le groupe de Galois est G ? Et pourquoi pas tenter de réaliser tout groupe fini G comme groupe de Galois d'une extension $E/\mathbb{Q}$? On parle alors de *problème inverse de Galois*. Ce problème, toutefois récent, a suffisamment d'ancienneté et de richesse pour avoir fait naitre une théorie et suscité de nombreuses recherches, des résultats, des conjectures de toute forme. Aujourd'hui encore, on cherche à dénicher les secrets que cette *théorie inverse de Galois* nous cache encore...

CHAPITRE 1

Préliminaires

1.1 Motivations

1.1.1 Le problème inverse de Galois

De manière classique, la théorie de Galois associe à toute extension finie galoisienne $F/\mathbb{Q}$ un groupe fini appelé groupe de Galois de $E/\mathbb{Q}$ et noté $\mathrm{Gal}(E/\mathbb{Q})$. Cette théorie, née dans le XIXe siècle et approfondie par la suite, fait maintenant partie du cursus Licence-Master pour la plupart des étudiants s'intéressant à l'algèbre. Ceci pour de bonne raisons, à tel point que certains mathématiciens attribuent à Galois une renouveau en algèbre et arithmétique. Parmi les grandes applications de la théorie de Galois, on peut citer la construction à la règle et au compas et la résolution d'équation

La réciproque de cette association

$$\text{théorie des corps} \longrightarrow \text{théorie des groupes}$$

est la question centrale de la théorie inverse de Galois : est ce que tout groupe fini peut être réalisé comme groupe de Galois d'une extension $E/\mathbb{Q}$? La question peut se poser sur n'importe quel corps K, donnant l'énoncé suivant :

Problème Inverse de Galois sur K (IGP $/K$). *Tout groupe fini est-il le groupe de Galois d'une certaine extension galoisienne de K ?*

Cette question, bien que simple à énoncer, n'a toujours pas de réponse générale sur $\mathbb{Q}$ aujourd'hui et a soulevé de nombreuses recherches. La réponse n'étant pas évidente à trouver, les recherches sur le sujet se sont diversifiées et ont amené à formuler diverses conjectures et présenter des résultats variés en lien avec différents domaines des mathématiques. On parle désormais d'un domaine de recherche à part entière appelé *théorie inverse de Galois*. Les

notions présentées dans les parties §1.1.2, §1.1.3 et §1.1.4 font partie de cette théorie et il y a bien entendu, d'autres thèmes de la théorie inverse de Galois non abordés dans cette thèse. Présentons un bref aperçu des résultats obtenu sur le problème (IGP $/K$).

Sur le corps des rationnels $\mathbb{Q}$, on sait réaliser
— les groupes abéliens,
— les groupes résolubles,
— certains groupes simples non abéliens.

La preuve dans le cas abélien est relativement simple (voir par exemple [Dè09, théorème 2.1.3]). Le cas des groupes résolubles est plus difficile et a été démontré par Shafarevich en 1954 (voir par exemple [NSW08]).

L'approche pour les groupes simples non-abéliens est différente. Etant donné un groupe fini G, plutôt que de tenter de construire une extension galoisienne $E/\mathbb{Q}$ de groupe G, on construit une extension galoisienne $F/\mathbb{Q}(T)$ où T est une indéterminée que l'on spécialise ensuite en un nombre rationnel t bien choisi.

$$\begin{array}{ccc} F & & E \\ | & T \to t & | \\ & \rightsquigarrow & \\ \mathbb{Q}(T) & & \mathbb{Q} \end{array}$$

Le précurseur de cette méthode est le mathématicien Hilbert, qui a pu notamment montrer que les groupes S_n sont des groupes de Galois sur $\mathbb{Q}$. La méthode repose sur son théorème d'irréductibilité présenté en §1.1.4 et permet de dire qu'une réponse positive à l'énoncé (IGP$/\mathbb{Q}(T)$) implique une réponse positive à l'énoncé (IGP$/\mathbb{Q}$). On peut étendre cette implication à tout corps K dit *hilbertien*.

Noether présenterait les choses différemment. Etant donné un corps K et groupe fini G plongé dans S_n, le groupe G agit sur le corps $E = K(T_1, \cdots, T_n)$. Le corps des invariants E^G est une extension de K et l'extension E/E^G est galoisienne de groupe G.

$$\begin{array}{c} E = K(T_1, \cdots, T_n) \circlearrowleft G \\ | \\ | G \\ | \\ K(T_1, \cdots, T_n)^G \end{array}$$

Si E^G est une extension transcendante pure (c'est le cas si $G = S_n$), disons $K(Y_1, \cdots, Y_n)$, la méthode de Hilbert peut s'appliquer et on peut spécialiser les indéterminées $Y_1, \cdots, Y_n$ dans K pour obtenir une extension galoisienne de K à partir de l'extension galoisienne E/E^G. Mais comme l'ont montré Swan [Swa69], Voskresenskiĭ [Vos70], puis Lenstra [Len74] et Saltman [Sal82], le corps E^G n'est pas en général une extension transcendante pure. L'idée de Noether, bien qu'ingénieuse, n'aboutit donc pas, en général, à la conclusion voulue.

Dans l'approche récente pour résoudre le problème inverse de Galois sur $\mathbb{Q}$, on demande de plus que l'extension $F/\mathbb{Q}(T)$ soit *régulière* sur $\mathbb{Q}$, c'est à dire qu'elle vérifie $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$. Cette propriété de régularité permet un angle d'attaque géométrique : l'extension $F/\mathbb{Q}(T)$ correspond, via le foncteur corps de fonctions, à un revêtement galoisien $f : X \to \mathbb{P}^1$ de groupe d'automorphisme G, défini sur $\mathbb{Q}$ ainsi que ses automorphismes.

$$\begin{array}{ccc} f : X & & K(X) \\ \downarrow & \rightsquigarrow & | \\ \mathbb{P}^1(\mathbb{Q}) & & \mathbb{Q}(T) \end{array}$$

Cette approche convient aussi si l'on remplace le corps $\mathbb{Q}$ par un corps de nombre K. Elle a permi de construire certains groupes simples comme des $PSL_n(\mathbb{F}_q)$, le Monstre, comme groupe de Galois sur $\mathbb{Q}$ (pour plus de détails, on renvoie au livre [MM99]). L'approche par l'étude des revêtements a aussi permis de réaliser tout groupe G comme groupe de Galois régulier sur $\overline{\mathbb{Q}}$. La question de réaliser les groupes finis comme groupe de Galois d'une extension régulière $F/K(T)$ est désormais connue comme *problème inverse de Galois régulier sur* K (RIGP $/K$).

1.1.2 La conjecture de Malle

Au-delà de chercher à résoudre le problème inverse de Galois, on peut se demander si, non pas une, mais plusieurs extensions galoisiennes d'un corps de nombres fixé, ont pour groupe de Galois un même groupe (à isomorphisme près). A partir de la fin du XXe siècle, des études ont été menées sur le sujet, par exemple, par Wright [Wri89], puis Malle [Mal02], [Mal04] et les résultats obtenus ont amené à former des conjectures.

Fixons nous un corps de nombres K et un groupe fini G. Afin de quantifier le problème, on impose une contrainte de discriminant sur les extensions étudiées. Il est bien connu que le nombre d'extensions de K (dans une clôture algébrique de K fixée) dont la norme du discriminant est bornée par un certain nombre y est un nombre fini. Il s'agit du théorème d'Hermite.

Fixons nous alors un nombre positif y. On définit un nombre $N(K, G, y)$ comme étant le nombre d'extensions galoisiennes E/K, de groupe de Galois G et de discriminant $d_{E/K}$ de norme $N_K(d_{E/K})$ plus petite que y.

On peut aussi définir ce nombre $N(K, G, y)$ pour des extensions non galoisiennes, en comptant le nombre d'extensions dont la clôture galoisienne a pour groupe de Galois, le groupe G. Plus précisément, soit S_n le groupe des permutations d'un ensemble à n éléments. Soit $G \subset S_n$ un groupe fini agissant sur l'ensemble $\{1, ..., n\}$ de manière transitive et soit y un nombre réel strictement positif. Pour un corps de nombres K, on note par $\overline{K}$ la clôture algébrique de K. Pour une extension E/K de degré n, on note par $\hat{E}/K$ sa clôture galoisienne.

Le groupe de Galois $\mathrm{Gal}(\hat{E}/K)$ agit transitivement sur les n plongements $E \hookrightarrow \overline{K}$. Soit $G(1) \subset G$ le sous-groupe stabilisateur de l'élément neutre 1. On dira qu'une extension finie E/K a *pour groupe de Galois* $G \subset S_n$ si $\hat{E}/K$ a pour groupe de Galois G et que E est le sous-corps de $\hat{E}$ fixé par $G(1)$. Enfin, on défini le nombre $N(K, G, y)$ par :

$$N(K, G, y) = \#\{E/K \text{ galoisienne } : \mathrm{Gal}(E/K) = G, N_{K/\mathbb{Q}}(d_{E/K}) \leq y\}.$$

Le comportement asymptotique du nombre $N(K, G, y)$ a été sujet à de nombreuses recherches et spéculations. Une conjecture a été donnée et démontrée dans le cas où le groupe G est abélien en utilisant la *théorie du corps de classes* [Wri89]. On la donne dans le cas galoisien sous cette forme :

Conjecture 1.1. *Il existe des constantes $a(G) > 0$, $b(k, G) > 0$ et $c(k, G) > 0$, telles que*

$$N(K, G, y) \sim c(K, G) x^{a(G)} (\log x)^{b(K,G)-1}.$$

De plus, les constantes $a(G)$ et $b(K, G)$ peuvent être données explicitement.

Ici, pour des fonctions f, $g : \mathbb{R} \to \mathbb{R}$, on écrit $f \sim g$ si

$$\lim_{x \to +\infty} \frac{f(x)}{g(x)} = 1.$$

Malle s'est aussi intéressé à cette conjecture, dans le cas où G n'est pas forcément abélien mais demeure résoluble [Mal02], [Mal04]. Il a démontré, avec Klüners, la conjecture 1.2 ci dessous, qui est une version plus faible de la conjecture 1.1 lorsque G est un groupe nilpotent (une classe de groupes contenue dans la classe des groupes résolubles) en utilisant le résultat de Shafarevich sur l'existence d'au moins une extension E/K de groupe G [KM04] :

Conjecture 1.2. *Il existe une constante $a(G) > 0$, ne dépendant que de G, telle que pour chaque $\varepsilon > 0$, on a*

$$c_1 y^{a(G)} \leq N(K, G, y) < c_2 y^{a(G)+\varepsilon} \text{ pour tout } y \geq y_0$$

pour des constantes positives c_1 (dépendant de G, K) et c_2, y_0 (dépendant de G, K, ε).

Nous nommerons cette dernière conjecture *la conjecture de Malle*. Toujours dans le cas galoisien, Malle a aussi donné la valeur de la constante $a(G)$: $(|G|(1 - 1/l))^{-1}$ où l est le plus petit diviseur premier du cardinal du groupe G.

Klüners a prouvé la partie minoration de la conjecture 1.2 pour les groupes diédraux d'ordre $2p$, où p est un nombre premier impair [Klü06]. A l'heure actuelle, en dehors des groupes résolubles, nous ne savons que peu de choses sur le comportement asymptotique du nombre $N(K, G, y)$. La thèse contribue à ce problème.

On peut s'intéresser à cette conjecture à travers l'étude des extensions de $K(T)$. En effet, si l'on sait réaliser un groupe fini G comme groupe de Galois d'une extension $F/K(T)$, alors la méthode introduite par Hilbert qui est présentée en §1.1.1 et précisée plus en détails en §1.1.4 permettent d'obtenir une ou plusieurs extensions E/K de groupe G. Nos résultats portant sur la conjecture de Malle regroupent plusieurs recherches et sont présentés dans le chapitre 4.

1.1.3 Le problème de Grunwald

Ce problème, devenu célèbre en théorie inverse de Galois, porte de nom du mathématicien Grunwald. La question ici, est de savoir si l'on peut imposer des conditions locales en certains idéaux premiers de K, sur une extension E/K que l'on veut de plus galoisienne de groupe donné G.

Pour être plus précis dans la présentation du problème, nous aurons besoin de quelques notations.

— Pour un idéal premier $\mathfrak{p}$ de K, la complétion de K en $\mathfrak{p}$ est notés $K_\mathfrak{p}$. Dans le cas $K = \mathbb{Q}$, il s'agit de $\mathbb{Q}_p$ pour un nombre premier p.

— Pour une extension galoisienne E/K et un idéal premier $\mathfrak{p}$ de K et $\mathcal{P}$ un idéal au dessus de $\mathfrak{p}$, la complétion de E en $\mathcal{P}$ de dépend pas de l'idéal $\mathcal{P}$ choisi (car l'extension est galoisienne) et c'est aussi le compositum $EK_\mathfrak{p}$. On l'appelera la complétion de E en $\mathfrak{p}$.

Le *problème de Grunwald* pose alors la question de la véracité de cette affirmation :

Etant donné un ensemble fini S d'idéaux premiers de K et une liste d'extensions galoisiennes finies $(L^\mathfrak{p}/K_\mathfrak{p})_{\mathfrak{p}\in S}$ de groupe de Galois s'injectant dans G, il existe une extension galoisienne E/K de groupe G dont la complétion $EK_\mathfrak{p}/K_\mathfrak{p}$ en $\mathfrak{p}$ est $K_\mathfrak{p}$-isomorphe à $L^\mathfrak{p}/K_\mathfrak{p}$ en chaque $\mathfrak{p} \in S$.

Une telle extension E/K obtenue sera appelée une *solution* au *problème de Grunwald* $\left(G, (L^\mathfrak{p}/K_\mathfrak{p})_{\mathfrak{p}\in S}\right)$.

Le cas des groupes abéliens, ou plus généralement, des groupes résolubles, a été étudié par Grunwald, Wang et Neukirch [Wan48] [Neu79] : en particulier, la réponse est positive si G est d'ordre impair. Mais en général, il y a des problèmes de Grunwald sans solution. Par exemple, Wang a démontré que si G est cyclique d'ordre 8 et si S contient un premier de K au dessus de 2, alors on peut trouver des problèmes de Grunwald sans solution [Wan48].

Pour contourner ce contre exemple, on essaye aujourd'hui de déterminer s'il n'existe pas d'ensemble fini d'idéaux premiers exceptionels S_{exc} tels que l'affirmation précédente reste valide pour les ensembles S de premiers qui sont disjoints de S_{exc}. De nombreux travaux ont été voués à cette forme faible [Har07], [DG12], [DLAN17] et elle a été démontrée vraie pour les groupes super-résolubles (par exemple résolubles ou nilpotents) et sur tout corps de nombres [HW18].

Pour les groupes non résolubles, un résultat de Dèbes et Ghazi [DG12] montre que tout problème de Grunwald $(L^\mathfrak{p}/K_\mathfrak{p})_{\mathfrak{p}\in S}$ (avec $S \cap S_{exc} = \emptyset$), également supposé non ramifié (les extensions $L^\mathfrak{p}/K_\mathfrak{p}$ sont non ramifiées), a toujours une solution si G est un *groupe de Galois régulier*[1] sur K.

Des conditions locales peuvent être incorporées au travail sur la conjecture de Malle. Ceci permet de donner un résultat par rapport au problème de Grunwald qui sera lui aussi exposé dans le chapitre 4.

1. Pour la définition plus précise de groupe de Galois régulier, voir chapitre 4

1.1.4 Le théorème d'irréductibilité de Hilbert (effectif)

L'histoire du théorème d'irréductibilité de Hilbert est très riche et l'on compte bon nombre de motivations et applications à ce théorème.

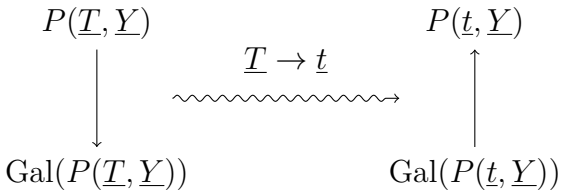
Sans surprise, ce théorème est dû à Hilbert [Hil92]. Sous une forme simple, ce théorème s'énonce comme suit :

Theorème (Hilbert)**.** *Soit K un corps de nombres et soit $P(T,Y) \in K[T,Y]$ un polynôme irréductible dans $K[T,Y]$ avec $\deg_Y(P(T,Y)) \geq 1$. Alors on peut spécialiser l'indéterminée T en une infinité $t \in K$ de sorte que le polynôme spécialisé $P(t,Y)$ soit irréductible dans $K[Y]$.*

Considérons par exemple le polynôme $Y^2 - T$. Si t n'est pas un carré dans $\mathbb{Q}$ alors le polynôme spécialisé $Y^2 - t$ reste irréductible sur $\mathbb{Q}$. Le théorème énoncé ci-dessus peut s'étendre à un ou plusieurs polynômes du type $P(\underline{T},\underline{Y}) = P(T_1,\cdots,T_n,Y_1,\cdots,Y_k)$ où l'on spécialise les indéterminées $T_1,\cdots,T_n$.

L'étude de cette propriété fait l'objet d'un domaine à part entière et cela a amené à introduire les notions d'ensembles hilbertiens, de corps hilbertiens... Sans entrer dans les détails, on peut appliquer le théorème de Hilbert dans notre cas en disant que *les corps de nombres sont des corps hilbertiens.*

Le théorème est utilisé dans certaines démonstrations en arithmétique des corps, ou pour créer des courbes elliptiques de rang élevé sur un corps K et il peut être appliqué à la factorisation des polynômes en deux variables. La motivation initiale de Hilbert fut en théorie inverse de Galois. Il souhaitait réaliser le groupe S_n des permutations comme groupe de Galois d'une extension de $\mathbb{Q}$. Sa méthode expliquée dans [Hil92] montre que le polynôme générique $P = Y^n + T_1Y^{n-1} + ... + T_n$ dont les coefficients $T_1, ..., T_n$ sont des indéterminées a pour groupe de Galois S_n sur $\mathbb{Q}(T_1, ..., T_n)$ et en utilisant le fait que $\mathbb{Q}$ est hilbertien, on peut spécialiser le polynôme $P(T_1, ..., T_n, Y)$ en un polynôme $P(t_1, ..., t_n, Y)$ irréductible dans $\mathbb{Q}[Y]$ et ayant S_n comme groupe de Galois.



L'aspect effectif du théorème consiste à borner le plus petit entier positif t tel que le polynôme spécialisé reste irréductible. Un des buts étant de savoir si l'on peut le trouver en un temps convenable.

Enfin, tout comme le théorème d'irréductibilité de Hilbert classique peut se lier avec la théorie inverse de Galois, la partie effective peut se lier à compter des extensions galoisiennes (voir par exemple [Coh81]) et nous amène directement à la conjecture de Malle enoncée précédemment.

1.1.5 La recherche de points entiers sur une courbe

Le domaine d'étude portant sur la recherche de points rationnels sur une courbe est très vaste et les recherches portant sur le sujet permettent de répondre à des questions comme "comment trouver les nombres rationnels solutions de l'équation $x_1^4 + x_2^4 = 17$ ".

On peut définir les courbes planes comme l'ensemble des zéros d'un polynôme à deux variables à coefficients dans un corps K (comme par exemple le polynôme $X_1^4 + X_2^4 - 17$), et, de manière plus moderne, généraliser la notion aux courbes algébriques sur K, qui sont des variétés algébriques dont les composantes irréductibles sont de dimension 1, dont la notion est également liée aux polynômes. On s'intéressera plus particulièrement au cas de la recherche de zéros rationnels d'un polynôme à deux variables, et ce, de manière effective.

Nous étudierons l'effectivité de la manière suivante : soit $F(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ et $B > 1$. Le nombre de points (x_1, x_2) à coordonnées entières compris dans la *boite* définie par

$$|x_1| \leq B \text{ et } |x_2| \leq B$$

est clairement un nombre fini. On en déduit qu'il y a un ensemble fini de points entiers dans cette boite et sur la courbe définie par $F(X_1, X_2) = 0$; il s'agit alors d'estimer leur nombre en fonction de B lorsque l'on fait grandir B.

Un théorème de Bombieri et Pila [BP89] donne une majoration en $B^{1/d}$ où d est le degré de $F(X_1, X_2)$ et on a cherché à améliorer cette borne [SZ95a], [HB02]. L'étude de ce problème fait partie de cette thèse.

Enfin, le problème peut être étendu dans un cas plus général où l'on remplace le corps de base (ici $\mathbb{Q}$) par un corps de nombres K et $\mathbb{Z}$ par l'anneaux des entiers O_K. Dans ce cas, on ne parlera pas de valeur absolue de x bornée par le nombre B, mais de "hauteur", qui généralise la valeur absolue sur $\mathbb{Z}$. Pour un polynôme $F(X_1, X_2) \in \mathcal{O}_K[1, X_2]$ et $B > 1$, l'étude des points $\mathcal{O}_K$-rationnels qui sont racines de F devient plus complexe et non moins intéressante que le cas $K = \mathbb{Q}$. On sait également que le nombre de $(x_1, x_2) \in \mathcal{O}_K^2$ vérifiant

$$H(x_1) \leq B \text{ et } H(x_2) \leq B$$

est un nombre fini (ici H est une hauteur que l'on défini sur $\mathcal{O}_K$, on la définit en détail dans §1.3.1). La base de travail vérifiée sur $\mathbb{Q}$ pour la hauteur usuelle $|.|$ est ainsi aussi vérifiée sur $\mathcal{O}_K$.

1.2 Présentation de la thèse

La fin du chapitre 1 présente divers outils de travail dont on se servira à divers moments dans la thèse. Ces outils sont, pour la plupart, des résultats classique que nous avons choisi d'utiliser pour effectuer nos calculs.

Dans cette fin de chapitre, on présente essentiellement la hauteur H que nous définissons sur $\mathcal{O}_K$, ainsi que diverses propriétés, que nous utiliserons tout au long de la thèse. Il est

évident que les utilisations que nous ferons de la hauteur seront cruciales pour les résultats obtenus.

Le **chapitre 2** traite de la recherche de points entiers sur une courbe algébrique. On travaillera ici sur les notions abordées en §1.1.5. Dans ce chapitre, on reprend, entre autre, un résultat donné par Heath-Brown en 2002 et une application effective donnée par Walkowiak en 2006. On obtient une extension de ces résultats qui n'ont actuellement été prouvés que dans le cas $K = \mathbb{Q}$.

Le point central de ce second chapitre est l'étude du nombre $N(F, B)$ défini ainsi. Soit K un corps de nombre fixé, $\mathcal{O}_K$ l'anneau des entiers de K, et $F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$ un polynôme à deux variables. A partir d'une hauteur sur K que l'on définira dans §1.3, on définit $N(F, B)$, pour un nombre positif B, comme le nombre de couples (x_1, x_2) qui sont des zéros de $F(X_1, X_2)$ dont la hauteur des composantes est bornée par B. C'est à dire

$$N(F, B) = \#\{(x_1, x_2) \in \mathcal{O}_K^2 \mid F(x_1, x_2) = 0,\ H(x_1) \leq B,\ H(x_2) \leq B\}.$$

Autrement dit, $N(F, B)$ compte le nombre de points entiers sur la courbe définie par $F(X_1, X_2) = 0$ et dans la "boîte" délimitée par B.

Les résultats obtenus ont un intérêt en soi, et sont aussi primordiaux pour les chapitres suivants. On en retiendra ce théorème principal [2] :

Theorème. *Soient $F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$ irréductible sur K, unitaire en X_2 et de degré total $d \geq 1$. Pour B suffisamment grand, dépendant de K, on a*

$$N(F, B) \leq cd^{14}(\log B)^4 B^{[K:\mathbb{Q}]/d}$$

où c est une constante dépendant uniquement de K.

Dans le **chapitre 3**, on travaille sur les notions abordées en §1.1.4. On donne une version effective du théorème d'irréductibilité de Hilbert, et ce, lorsque le polynôme étudié est à coefficients dans un corps de nombres fixé.

Dans ce chapitre, on reprend également le cheminement de Walkowiak qui a démontré une version effective du théorème d'irréductibilité de Hilbert dans le cas où le polynôme $P(T, Y)$ est à coefficients dans $\mathbb{Q}$. De la même manière que dans le chapitre 2, on généralise le résultat et on se sert de la majoration de $N(F, B)$ obtenue dans le chapitre 2. La première partie de ce troisième chapitre est aussi un point important dans la suite de la thèse. On travaille sur le nombre $N_T(F, B)$ défini, à partir d'un polynôme $F(T, Y) \in \mathcal{O}_K[T, Y]$ irréductible et d'un nombre réel $B > 1$, comme le nombre de $t \in \mathcal{O}_K$ de hauteur bornée par B et tels que le polynôme spécialisé $F(t, Y)$ ait une racine dans $\mathcal{O}_K$. autrement dit

$$N_T(F, B) = \#\{t \in \mathcal{O}_K \mid H(t) \leq B,\ F(t, Y) \text{ a une racine dans } \mathcal{O}_K\}.$$

Le nombre $N_T(F, B)$ est directement relié au théorème d'irréductibilité de Hilbert. La suite du chapitre 3 le montre pourquoi, en reprenant la démonstration du théorème d'irréductibilité de Hilbert mais de manière effective.

2. Il s'agit du théorème 2.10.

Le résultat sur ce nombre est le suivant [3] :

Theorème. *Soient $F(T,Y) \in \mathcal{O}_K[T,Y]$ irréductible sur K, unitaire en Y et de degré total $d \geq 2$. Il existe des nombres $a_1, ..., a_4$ dépendant de K, tels que pour tout B assez grand, le nombre $N_T(F,B)$ de $t \in \mathcal{O}_K$ avec $H(t) \leq B$ et tels que $F(t,Y)$ ait une racine dans K vérifie*

$$N_T(F,B) \leq a_1 d^{a_2} (\log H)^{a_3} B^{[K:\mathbb{Q}]/n} (\log B)^{a_4}$$

(H peut désigner la hauteur du polynôme $F(T,Y)$).

Dans la fin du chapitre, la partie sur le théorème d'irréductibilité de Hilbert consiste à partir d'un polynôme irréductible $P(T,Y) \in \mathcal{O}_K[T,Y]$ et d'estimer le nombre de spécialisations $t \in \mathcal{O}_K$, de hauteur bornée par B, tel que le polynôme spécialisé $P(t,Y)$ reste irréductible dans $K[Y]$. On arrive à la conclusion que pour B suffisamment grand, le nombre de $t \in \mathcal{O}_K$ tels que $P(t,Y)$ reste irréductible sur $\mathcal{O}_K$ est plus grand que $\frac{1}{2}B^{\rho}$ [4].

Les chapitres 2 et 3 traitent de problèmes diophantiens et de spécialisations de polynômes tandis que le chapitre 4 est dédié aux implications des résultats obtenus en théorie inverse de Galois.

Le **chapitre 4** regroupe les résultats mis en lumière dans les chapitres 2 et 3 afin de prouver des théorèmes sur la conjecture de Malle et le problème de Grunwald. Il sont obtenus à partir de l'étude d'extensions régulières de $K(T)$ et de leur spécialisations. Le premier résultat principal de ce chapitre [5] porte sur le nombre $N(K,G,y)$ défini en §1.1.2 :

Theorème. *Soit G un groupe fini. Il existe un corps de nombres K_0 tel que sur tout corps de nombres K contenant K_0, on ait la propriété suivante :*
il existe $\alpha(G) > 0$, dépendant de G, tel que

$$N(K,G,y) \geq c_1 y^{\alpha(G)} \text{ pour tout } y \geq y_0$$

pour des constantes positives c_1, y_0 dépendantes de K, G.

Le deuxième résultat porte sur les notions de §1.1.3, le nombre de solutions à un type de problème de Grunwald donné peut être infini [6] :

Theorème. *Soit K un corps de nombres et G un groupe fini régulier sur K. Il existe un ensemble fini S_{exc} d'idéaux premiers de K avec la propriété suivante : si $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p} \in S})$ est un problème de Grunwald sur K avec $S \cap S_{exc} = \emptyset$, une infinité de solutions E/K au problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p} \in S})$.*

Ce nombre "infini" de solution peut être exprimé plus en détails dans l'esprit du théorème précédent. On peut également l'étendre au cas où G n'est pas régulier sur K. Dans ce cas, nous parlerons de M-solutions au problème de Grunwald. Nous renvoyons au chapitre 4 pour les notions et un énoncé détaillé en deux points.

3. Il s'agit du théorème 3.2.
4. Il s'agit du théorème 3.7.
5. Il s'agit du théorème 4.2.
6. Il s'agit du théorème 4.3.

1.3 Outils de travail

Soit K un corps de nombres. On note $\mathcal{O}_K$ l'anneau des entiers de K, ρ le degré $[K : \mathbb{Q}]$. On note par $\sigma : K \to \overline{K}$ un plongement de K dans une clôture algébrique de K. Le nombre de plongements différents est ρ.

1.3.1 Une hauteur sur un corps de nombres K

On note M_K l'ensemble des places sur K. Soit v une place de K au dessus d'un nombre premier p. On note K_v le complété de K pour v (ou $K_\mathfrak{p}$ lorsque l'on parle de l'idéal premier associé) et O_v le complété de $\mathcal{O}_K$ pour v.

Pour v une valuation sur $\mathbb{Q}$, on note $\mathbb{Q}_v$ le complété de $\mathbb{Q}$ pour cette valuation ; si v correspond à la valeur absolue usuelle, $\mathbb{Q}_v = \mathbb{R}$, si v est une valuation p-adique, $\mathbb{Q}_v = \mathbb{Q}_p$. L'unique valeur absolue sur K_v prolongeant la valeur absolue v sur $\mathbb{Q}_v$ est notée par $|.|_v$. Si v est ultramétrique, elle est normalisée de manière à coïncider avec la valeur absolue sur $\mathbb{Q}_v$, ce qui signifie $|p|_v = \frac{1}{p}$, où p est le nombre premier associé à la valuation. Si v est archimédienne, elle coïncide sur $\mathbb{Q}$ avec le module complexe.

La hauteur d'un entier algébrique $x \in \mathcal{O}_K$, parfois appelée *maison*, est définie par

$$H(x) = \max_{\sigma : K \to \overline{K}} |\sigma(x)| = \max_{\substack{v \in M_K \\ v/\infty}} |x|_v.$$

Il est concevable de généraliser la hauteur à tout K grâce à cette proposition.

Proposition 1.3. *Si $x \in \mathcal{O}_K$ vérifie $H(x) \leq 1$, alors x est une racine de l'unité ou $x = 0$.*

Démonstration. Supposons $x \neq 0$ et soit $P(X)$ le polynôme minimal de x et n son degré. Alors

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{\sigma : K \to \overline{K}} (X - \sigma(x)).$$

Comme $H(x) \leq 1$, pour tout $\sigma : K \to \overline{K}$, $|\sigma(x)| \leq 1$. En développant le produit de droite dans l'expression de $P(X)$, on obtient que pour tout $1 \leq k \leq n-1$,

$$|a_k| \leq \binom{n}{k} \leq 2^n.$$

Le même raisonnement s'applique pour les puissances x^r, $r \geq 1$; x^r est entier et $H(x^r) \leq 1$. Ainsi, les coefficients $a_{r,k}$ du polynôme minimal de x^r, de degré $\leq n$ vérifient $|a_{r,k}| \leq 2^n$ pour tout k.

Il n'y a donc qu'un nombre fini de coefficients qui apparaissent dans les polynômes minimaux des x^r. Il existe alors $r, s \geq 1$ tels que $x^r = x^{r+s}$.

Finalement $x^s = 1$ et x est une racine de l'unité □

Il en découle de cette proposition que si $x \neq 0$, $x \in \mathcal{O}_K$ alors,

$$H(x) = \max_{\sigma : K \hookrightarrow \overline{K}} (1, |\sigma(x)|) = \max_{\substack{v \in M_K \\ v/\infty}} (1, |x|_v).$$

La généralisation de la hauteur peut donc se faire à K, mais aussi pour un uplet et pour un polynôme à coefficients dans K :

— pour $x \in K$, $H(x) = \max_{v \in M_K} \max(1, |x|_v)$,

— pour $\underline{x} = (x_1, \cdots, x_n) \in K^n$,

$$H(x) = \max_{v \in M_K} (|x_1|_v, \cdots, |x_n|_v),$$

— la hauteur d'un polynôme P à coefficients $c_1, \cdots, c_n$ dans K est

$$H(P) = H(c_1, \cdots, c_n),$$

On remarque que pour $x \in \mathcal{O}_K$, $H(x) = H(1, x)$. Il faut tout de même porter attention à la définition de $H(x)$ pour $x \in K$ et $H(x)$ pour $x \in K^1$ qui peut paraître ambigue. Dans la thèse, nous utiliserons uniquement la hauteur sur $\mathcal{O}_K$, dans ce cas, il n'y a pas d'ambiguité.

En utilisant des notations H_v définies ci dessous, la généralisation de la hauteur pour des uplets se fait donc de la manière suivante :

— pour $\underline{x} = (x_1, \cdots, x_n) \in \mathcal{O}_K^n$,

$$H(\underline{x}) = \max_{v/\infty} H_v(\underline{x})$$

où $H_v(\underline{x})$ est la *v-hauteur* définie par

$$H_v(\underline{x}) = \max(|x_1|_v, \cdots, |x_n|_v),$$

— la hauteur d'un polynôme P à coefficients $c_1, \cdots, c_n$ dans $\mathcal{O}_K$ est

$$H(P) = H(c_1, \cdots, c_n).$$

On définit également la v-hauteur du polynôme $H_v(P) = H_v(c_1, \cdots, c_n)$.

Remarque 1.4. Comparaison avec la Hauteur de Weil

La hauteur de Weil est une hauteur classique sur les corps de nombres. Sous sa version additive, elle est définie pour un n-uplet $\underline{a} = (a_1, ..., a_n) \in K^n$ par

$$h_W(\underline{a}) = \frac{1}{[K : \mathbb{Q}]} \sum_v [K_v : \mathbb{Q}_v] \log(\max(|a_1|_v, ..., |a_n|_v))$$

où la somme est prise sur toutes les places v de K. La forme mutiplicative, plus utilisée, est

$$H_W(\underline{a}) = \exp(h(\underline{a})).$$

Cette définition ne dépend pas du corps K contenant les nombres $a_1, \cdots, a_n$; de ce fait, la hauteur de Weil est définie sur $\overline{\mathbb{Q}}^n$ en prenant pour K n'importe quel corps de nombres contenant les a_i, $i \in \{1, ..., n\}$.

Cette hauteur s'étend de la même manière que la maison aux polynômes P à coefficients dans K par $h(P) = h(p_1, ..., p_n)$ où les nombres $p_1, ..., p_n$ sont les coefficients du polynôme et la hauteur de Weil d'un nombre algébrique t est définie par $h(t) := h(1, t)$.

La raison pour laquelle nous préférons utiliser la maison plutôt que la hauteur de Weil est technique. Elle vient du fait qu'il est plus difficile de borner la hauteur d'une somme de deux éléments en utilisant la hauteur de Weil (qui compte un produit) plutôt que la maison (qui compte un max). Nous expliquons où notre hauteur est plus appropriée pour nos calculs dans la remarque 2.7.

Cependant, les deux hauteurs se comparent bien sur $\mathcal{O}_K$ et il semble plausible de parvenir à nos énoncés en utilisant la hauteur de Weil, tout comme le font d'autres auteurs qui ont généralisé les résultats de Heath-Brown (voir chapitre 2).

La comparaison entre notre hauteur H et la hauteur de Weil est la suivante : pour $x \in \mathcal{O}_K$, on a

$$H(x)^{1/\rho} \leq H_{\mathrm{W}}(x) \leq H(x).$$

1.3.2 Propriétés relatives à la hauteur

Dans cette partie, nous présentons quelques liens utiles entre la hauteur des éléments de K et la hauteur d'un polynôme à coefficients dans K. Dans la partie suivante, on comparera aussi la hauteur d'un élément avec la norme de l'idéal qu'il engendre.

Proposition 1.5. *Soit $\underline{x} = (x_1, \cdots, x_n)$ un n-uplet dans $\mathcal{O}_K^n$ ($n \in \mathbb{N}$), soit*

$$P(\underline{X}) \in K[\underline{X}] = K[X_1, ..., X_n]$$

un polynôme à n variables, $(x_1, \cdots, x_n) \in K^n$. On note par l le nombre de coefficients non nuls de P. Soit $\sigma : K \to \overline{\mathbb{Q}}$ un morphisme de corps. Alors,

1. $H(\underline{x}) = H(\sigma(\underline{x}))$,
2. $H(x_i) \leq H^+(\underline{x}) \leq H(x_1) \cdots H(x_n)$. $(i = 1, ..., n)$,
3. $H(P(x_1, \cdots, x_n)) \leq l.H^(P).M^{\deg(P)}$ *où* $M = \max_{i=1\cdots,n} H(x_i)$.

Démonstration. 1. est clair.

2. En utilisant la définition de la hauteur, on a

$$H(x_i) = \max_{v \in M_K} \max(|x_i|_v) \leq \max_{v \in M_K} \max(1, |x_1|_v, ..., |x_n|_v) \leq \prod_{i=1}^{m} \max_{v \in M_K} \max(1, |x_i|_v).$$

3. On écrit

$$P(\underline{X}) = \sum p_{\underline{a}} \underline{X}^{\underline{a}} = \sum p_{a_1, \ldots a_n} X_1^{a_1} ... X_n^{a_n}$$

et soit $d = \deg(P)$.

Pour une valuation archimédienne v, on a

$$|P(\underline{x})|_v \leq l. \max_{\underline{a}}(|p_{\underline{a}}|_v) M^d.$$

Alors,

$$\begin{aligned} H(P(\underline{x})) &= \max_{v/\infty}(|P(\underline{x})|_v) \\ &\leq l. \max_{v/\infty} H(P) M^d \end{aligned}$$

ce qui permet de conclure. □

Inégalités de Liouville

Soit $P \in \mathcal{O}_K[X]$ unitaire et $x \in \mathcal{O}_K$ une racine de P. On note $p_1, \cdots, p_n$ les coefficients de P. On rappelle que si $P \neq 0$ alors

$$H(P) = \max_{v \in M_K} H_v(P).$$

Les inégalités de Liouville sont généralement présentées pour la hauteur de Weil. On peut par exemple démontrer, pour un polynôme non unitaire dont le coefficient dominant est a_0 que

$$\begin{cases} \text{Si } v \text{ est archimédienne, } |x|_w < \dfrac{H_v(P) + |a_0|_v}{|a_0|_v} \\ \text{Si } v \text{ est ultramétrique, } |x|_w \leq \dfrac{H_v(P)}{|a_0|_v} \end{cases}$$

$$\begin{cases} \text{Si } v \text{ est archimédienne } |x|_w > \dfrac{|P(0)|_v}{H_v(P) + |P(0)|_v} \\ \text{Si } v \text{ est ultramétrique } |x|_w \geq \dfrac{|P(0)|_v}{H_v(P)} \end{cases}$$

Dans ces inégalités H_v désigne la v-hauteur de P au sens de la hauteur de Weil. Ces inégalités impliquent que $H_W(x) \leq 2H(P)$. Dans notre cas, on montre une majoration similaire valable sur $\mathcal{O}_K$ et pour P unitaire.

Proposition 1.6. *On a l'inégalité suivantes*

$$H(x) \leq 2H(P).$$

Démonstration. Le résultat est trivial si $x = 0$. Pour $x \neq 0$, on va montrer que pour toute place archimedienne v, $|x|_v \leq 2H_v(P)$ (ici, il s'agit de la v-hauteur pour notre hauteur).

On se fixe v une place archimédienne. Si $|x|_v = 1$ l'inégalité est claire, sinon on écrit $P(X) = X^n + a_1X^{n-1} + \cdots + a_0$ et on déduit de $x^n + a_1x^{n-1} + \cdots + a_0 = 0$ que

$$|x|_v^n \leq H_v(P)(|x|_v^{n-1} + \cdots + |x|_v + 1).$$

Comme $|x|_v > 1$ et $H_v(P) \geq 1$, on déduit

$$1 \leq H_v(P)(\frac{1}{|x|_v} + \cdots + \frac{1}{|x|_v^n}) < \frac{H_v(P)}{|x|_v - 1}.$$

Cela donne

$$|x|_v \leq H_v(P) + 1 \leq 2H_v(P)$$

et donc

$$H(x) \leq 2H(P).$$

□

1.3.3 Norme d'un idéal de $\mathcal{O}_K$

La norme d'un idéal (voir par exemple [Sam67, §3.5]) $J \subset \mathcal{O}_K$ est par définition le cardinal de l'ensemble quotient de $\mathcal{O}_K$ par J :

$$N_{K/\mathbb{Q}}(J) = \#\mathcal{O}_K/J.$$

La norme sur les idéaux est multiplicative, c'est-à-dire pour J_1 et J_2 deux idéaux de $\mathcal{O}_K$,

$$N_{K/\mathbb{Q}}(J_1.J_2) = N_{K/\mathbb{Q}}(J_1).N_{K/\mathbb{Q}}(J_2)$$

où $N_{K/\mathbb{Q}}(a)$ est la norme usuelle de l'élément $a \in \mathcal{O}_K$.

Pour $a \in \mathcal{O}_K$, $a \neq 0$, $N_{K/\mathbb{Q}}(a\mathcal{O}_K) = |N_{K/\mathbb{Q}}(a)| = \prod_{\sigma:K\to\overline{K}} |\sigma(a)| \leq H(a)^\rho$.

On se servira aussi du résultat suivant, analogue au fait qu'il n'existe qu'un nombre fini de nombre premiers p qui divisent un nombre réel $x \neq 0$.

Lemme 1.7. *Soit $a \in \mathcal{O}_K$, $a \neq 0$. Le nombre d'idéaux premiers $\mathfrak{p}$ qui divisent l'idéal $a\mathcal{O}_K$ est inférieur ou égal à $\log_2(H(a)^\rho)$.*

Démonstration. Soit n ce nombre de ces idéaux que l'on note $\mathfrak{p}_1, ..., \mathfrak{p}_n$. On a

$$a\mathcal{O}_K = \mathfrak{p}_1^{\alpha_1}...\mathfrak{p}_n^{\alpha_n}$$

où les α_i, $i \in \{1..n\}$, sont des nombres entiers strictement positifs. Ce qui donne

$$H(a)^\rho \geq \prod_{\sigma:K\to\overline{\mathbb{Q}}} |\sigma(a)| = |N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{n} N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{\alpha_i}.$$

Les idéaux $\mathfrak{p}_i$ étant des idéaux propres, leur norme est plus grande que 2, et donc :

$$H(a)^\rho \geq 2^n.$$

D'où le résultat. □

1.3.4 Inégalités de Lang-Weil

La proposition qui suit permet d'estimer le nombre $C(\mathbb{F}_q)$ de points rationnels d'une courbe algébrique sur un corps fini. Sans suspens, elles ont été démontrées par Lang et Weil [LW54, theorem 1]. On utilisera deux fois les inégalités de Lang-Weil, d'abord dans la démonstration du théorème 2.1 (§2.2.3), puis dans le chapitre 4, proposition 4.5.

Proposition 1.8 (Inégalités de Lang-Weil)**.** *Soient $\mathbb{F}_q$ un corps fini, $p(X_1, X_2) \in \mathbb{F}_q[T, Y]$ un polynôme absolument irréductible de degré d et C_p la courbe affine définie par l'équation $p(x_1, x_2) = 0$. On a alors*

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

Pour la démonstration de cette proposition, voir [FJ86, theorem 5.4.1].

Ces estimations s'étendent à des variétés en dimension supérieure [LW54]. Elles constituent une partie des *conjectures de Weil* qui ont été démontrées par Deligne.

1.3.5 Théorème de Bézout

Ce théorème de Géométrie Algébrique permet de compter le nombre de zéros communs à deux polynômes premiers entre eux.

Theorème 1.9 (Bézout)**.** *Soient k un corps algébriquement clos et $F(X, Y, Z)$ et $G(X, Y, Z)$ deux polynômes homogènes dans $k[X, Y, Z]$ et premiers entre eux. Alors les deux courbes algébriques $V(F) := \{(x, y, z) \in k^3 : F(x, y, z) = 0\}$ et $V(G)$ se coupent en un nombre fini de points dans $\mathbb{P}^2(k)$, plus précisément en $deg(F)deg(G)$ points comptés avec une multiplicité appropriée.*

Remarque 1.10. Le cas non homogène pour des polynômes à deux variables peut se ramener au cas homogène ; prenons deux polynômes $F(X, Y)$ et $G(X, Y)$ que l'on homogénéise. Les deux polynômes homogènes $F(X, Y, Z)$ et $G(X, Y, Z)$ construits restent premiers entre eux si les polynômes de départ $F(X, Y)$ et $G(X, Y)$ le sont. Par le théorème de Bezout, on obtient alors la conclusion que le nombre de zéros commun à $F(X, Y)$ et $G(X, Y)$ dans k^2 est au plus $\deg(F)\deg(G)$ (il est possible qu'il y en ait à l'infini).

1.3.6 Le théorème de densité de Chebotarev

Pour cette partie, on s'appuie essentiellement sur un article de Jean-Pierre Serre [Ser81]. Les références suivantes peuvent aussi être utiles : [SL96] ; [Neu79] ; [Win13].

Soit L/E une extension galoisienne de corps de nombres de groupe de Galois G, d_L le discriminant absolu de L, n_L le degré de L sur $\mathbb{Q}$. Soit $\mathfrak{p}$ un idéal premier de E non ramifié dans L et $\mathcal{P}$ un idéal premier de L au dessus de $\mathfrak{p}$. On désigne par $\overline{L}_{\mathcal{P}}$ et par $\overline{E}_{\mathfrak{p}}$ les corps résiduels $O_L/\mathcal{P}$ et $O_E/\mathfrak{p}$ respectivement.

Le *morphisme de Frobenius* est, par définition, le générateur du groupe $\mathrm{Gal}(\overline{L}_{\mathcal{P}}/\overline{E}_{\mathfrak{p}})$. On appelle *élément de Frobenius* associé à $\mathcal{P}/\mathfrak{p}$ tout antécédent du morphisme de Frobenius par $\varphi_{\mathcal{P}} : D_{\mathcal{P}} \to \mathrm{Gal}(\overline{L}_{\mathcal{P}}/\overline{E}_{\mathfrak{p}})$, où $D_{\mathcal{P}}$ désigne le groupe de décomposition associé à $\mathcal{P}$ (pour plus de détails voir [Neu79]). La classe de conjugaison dans G de chaque élément de Frobenius ne dépend que de $\mathfrak{p}$. On appelle *Frobenius de* $\mathfrak{p}$, noté $\mathrm{Frob}_{\mathfrak{p}}(L/E)$, un élément quelconque de cette classe.

L'idéal $\mathfrak{p}$ étant non ramifié, l'élément de Frobenius associé à $\mathcal{P}/\mathfrak{p}$ peut aussi être défini comme l'unique élément $\sigma_{\mathcal{P}} \in G$ vérifiant $\sigma_{\mathcal{P}}(x) \equiv x^{|\overline{L}_{\mathcal{P}}|} \mod \mathcal{P}$ pour tout $x \in O_L$ (c'est le cas par exemple dans [Ser81] §2.1).

Soit C une classe de conjugaison de G. Pour tout $x > 1$, la fonction $\pi_C(x)$ décompte le nombre d'idéaux premiers $\mathfrak{p}$ de E de norme $\leq x$, qui ne se ramifient pas dans L, et tels que $\mathrm{Frob}_p(L/E) \in C$. Le résultat suivant, conjecturé par Frobenius a été démontré par Chebotarev :

Theorème 1.11 (Chebotarev)**.**

$$\pi_C(x) \sim \frac{|C|}{|G|} \frac{x}{\ln x} \quad \textit{lorsque} \quad x \to +\infty.$$

On utilisera ce théorème dans le cas $L = K$, $E = \mathbb{Q}$, $C = \{1\}$. Cela signifie que $\pi_{\{1\}}(x)$ compte le nombre de premiers $p \in \mathbb{N}$ totalement décomposés et plus petits que x.

En conséquence directe du théorème nous utiliserons ces deux résultats

Corollaire 1.12.
— *pour* $x > 1$ *suffisamment grand,* $\pi_C(x) \geq \dfrac{|C|}{2|G|} \dfrac{x}{\ln x}$,
— *pour* $y > 1$ *suffisamment grand,* $\pi_C(y) \leq \dfrac{2|C|}{|G|} \dfrac{y}{\ln y}$.

On se servira aussi du résultat d'analyse suivant :
Si $a > 2$, l'inéquation $\dfrac{x}{\ln x} \geq a$ est vérifiée pour $x = 2a \ln a$. En effet, une étude de fonction élémentaire permet de montrer que $2 \ln a \leq a$, ce qui implique que $0 < \ln(2a \ln a) \leq 2 \ln a$, et ainsi $\dfrac{2a \ln a}{\ln(2a \ln a)} \geq a$.

CHAPITRE 2

Un théorème de Heath-Brown généralisé à un corps de nombres

2.1 Présentation de la démarche

Dans ce chapitre, on travaille sur le nombre de zéros entiers d'un polynôme à deux variables, que l'on notera $F(X_1, X_2)$. La recherche de points entiers de hauteur bornée sur une courbe est un problème classique pour lequel Heath-Brown a introduit une méthode dans l'espace projectif en 2002 [HB02] et qui a été développée sur les courbes et de manière plus explicite par Walkowiak en 2005 [Wal05].

2.1.1 L'ensemble $R(F, B)$ et son cardinal $N(F, B)$

Soit K un corps de nombres. On note par O_K l'anneau des entiers de K. Prenons un polynôme $F(X_1, X_2) \in O_K[X_1, X_2]$ (si $K = \mathbb{Q}$ alors $F(X_1, X_2)$ est à coefficients dans $\mathbb{Z}$). On rappelle la hauteur d'un élément $x \in O_K$:

$$H(x) = \max_{\sigma : K \to \overline{K}} |\sigma(x)| = \max_{\substack{v \in M_K \\ v/\infty}} |x|_v.$$

Pour tout nombre réel B, on définit :

$$R(F, B) = \{(x_1, x_2) \in O_K^2 \mid F(x_1, x_2) = 0,\ H(x_1) \leq B,\ H(x_2) \leq B\}$$

et son cardinal

$$N(F, B) = \#R(F, B).$$

L'approche de Walkowiak, ayant pour but de majorer le nombre $N(F, B)$ repose donc sur une idée de Heath-Brown qui consiste à séparer l'ensemble $R(F, B)$ en un nombre k de sous-ensembles. Chaque sous-ensemble est inclus dans l'ensemble des zéros d'un polynôme

$F_i(X_1, X_2)$. Le point important est d'obtenir une bonne majoration pour le nombre k de polynômes $F_i(X_1, X_2)$ obtenus.

L'étude de $N(F, B)$ est un problème classique qui a un intéret propre mais qui est directement lié au théorème d'irréductibilité de Hilbert. Dans ce contexte, on peut citer [SZ95b] où les auteurs ont amélioré une première borne effective pour le théorème d'irréductibilité de Hilbert de [Dèb96]. Pour l'étude de points entier sur une courbe, Bombieri et Pila ont introduit une méthode utilisant le déterminant en 1989 dans le but de donner des bornes uniformes pour les courbes planes affines sur $\mathbb{Q}$ [BP89].

C'est dans cette optique et en s'inspirant de cette méthode que Heath-Brown a developpé son résultat en 2002 [HB02]. Ce résultat a été étudié et affiné, aussi sur $\mathbb{Q}$, par Walkowiak qui a donné des bornes explicites pour le nombre $N(F, B)$ [Wal05]. Ces bornes explicites permettent de donner des résultats en théorie inverse de Galois (voir chapitre 4) et c'est dans ce contexte que nous démontrons nos résultats, qui étendent ceux de Walkowiak à tout corps de nombres.

Le résultat principal de Heath-Brown pour les courbes algébriques est le suivant : A partir d'un polynôme $F(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ dont on cherche à étudier les racines à coefficients entiers, on détermine une famille finie de polynômes dont l'ensemble de leur racines entières recouvre les racines entières de F.

Theorème (Heath-Brown)**.** *Soit $F(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ un polynôme irréductible sur $\mathbb{Q}$ de degré d, et soient $\varepsilon > 0$, $B > 1$ 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 que l'on ait la propriété suivante : il existe k polynômes $F_1, \cdots, F_k \in \mathbb{Z}[X_1, X_2]$, premiers avec $F(X_1, X_2)$ et de degré au plus D tels que chaque point de $R(F, B)$ est le zéro d'un des polynômes $F_j(X_1, X_2)$ $(j = 1, \cdots, k)$.

Ici, d est le degré total du polynôme $F(X_1, X_2)$ et $H(F)$ est la hauteur (sur $\mathbb{Q}$) de ce polynôme.

Le travail de Walkowiak a été de rendre ce théorème effectif et, grâce à lui, nous pouvons donner ce résultat :

Theorème (Walkowiak)**.** *Le nombre k des polynômes du théorème de Heath-Brown vérifie*

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

pour tout $D > d$.

Un lecteur attentif aura vite remarqué que ces résultats sont démontrés uniquement dans le cas $K = \mathbb{Q}$. Le but de ce chapitre est de généraliser le résultat obtenu par Walkowiak au cas où $F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$, ainsi que la majoration explicite du nombre $N(F, B)$ qu'a donnée Walkowiak par la suite. Ces résultats, qui ont un intérêt en soi dans le domaine de l'étude de points entiers sur une courbe, seront également utilisés dans les applications aux chapitres 3 et 4.

2.1.2 Énoncé du théorème de Heath-Brown effectif généralisé

Généraliser les résultats de Heath-Brown et de Walkowiak sur un corps de nombres arbitraire n'est pas une tâche aisée. En effet, nous avons affaire à quelques phénomènes qui s'appliquent sur un corps de nombres et qui n'apparaissent pas sur $\mathbb{Q}$. Par exemple, nous allons travailler par la suite avec une famille d'idéaux premiers de K. Dans le cas $\mathcal{O}_K = \mathbb{Z}$, les idéaux premiers correspondent aux nombres premiers, leur décomposition dans l'extension $K/\mathbb{Q}$ est triviale. Dans le cas général, la structure de $\mathcal{O}_K$ et de ses idéaux premiers demande du travail supplémentaire.

L'extension du résultat original de Heath-Brown aux corps de nombres arbitraires a été étudié par différents auteurs. Broberg [Bro04] et Chen [Che12] en sont deux exemples. Ils obtiennent des estimations qui peuvent aisément se comparer à la notre (bien que le résultat de Broberg n'est pas aussi explicite que celui de Chen (voir son corollaire 4.3) et que notre théorème 2.1 et de son application au calcul de $N(F, B)$, théorème 2.10).

Nos estimations vont se faire en deux temps : analyse locale pour chaque place et globalisation. On travaillera avec des idéaux premiers totalement décomposés. Cela conduit aussi à modifier certains arguments.

On se fixe un corps de nombres K, un polynôme $F(X_1, X_2)$ absolument irréductible (c'est à dire irréductible dans $\overline{K}[X_1, X_2]$). On utilisera les notations suivantes :

— ρ est le degré $[K : \mathbb{Q}]$,
— $d > 1$ est le degré total du polynôme $F(X_1, X_2)$,
— $H(F)$ est la hauteur du polynôme telle que définie dans le chapitre 1 section 3.

Le théorème que nous allons démontrer, analogue au résultat de Walkowiak sur $\mathbb{Q}$, est le suivant :

Theorème 2.1. *Soient B un nombre positif supposé grand (dépendant de K, d) et $D > d$. Alors il existe un nombre $k \geq 1$ et des polynômes $F_1, ..., F_k \in \mathcal{O}_K[X_1, X_2]$ premiers avec $F(X_1, X_2)$ dans $\overline{K}[X_1, X_2]$ et de degré $\deg(F_i) \leq D$, tels que chaque point de $R(F, B)$ soit le zéro d'au moins un des polynômes F_i. Ce nombre k est majoré par :*

$$c_2 d^3 \log^3(2d^3 H(F) B^{d-1})(B^{d^{-1}+6D^{-1}})^\rho$$

où c_2 est une constante dépendant uniquement de K.

Le théorème 2.1 peut se comparer au théorème 4.2 de [Che12]. La démonstration du théorème de Heath-Brown généralisée à un corps de nombre arbitraire est détaillée dans la section 2 et le calcul de la majoration de $N(F, B)$ dans la section 3.

2.2 Démonstration du théorème

Dans cette partie, nous allons construire le nombre k et les polynômes F_i, $i \in \{1, ..., k\}$ apparaissant dans le théorème 2.1. On travaille ici avec $F[X_1, X_2] \in \mathcal{O}_K[X_1, X_2]$ absolument irréductible dans $\overline{K}[X_1, X_2]$, de degré d et on se fixe $D > d$ et $B > 1$.

Comme F est irréductible, on a $d \geq 1$. Quitte à échanger X_1 et X_2, on peut supposer que $\deg_{X_1}(F) \geq 1$. Un premier des k polynômes que l'on va prendre en compte est le polynôme $\dfrac{\partial F}{\partial X_1}(X_1, X_2)$. Il est premier avec $F(X_1, X_2)$ et de degré $\leq d$ donc $\leq D$.

On se concentre maintenant sur ce sous-ensemble de $R(F, B)$:

$$S(F, B) = \{\underline{x} = (x_1, x_2) \in \mathcal{O}_K^2 : F(\underline{x}) = 0 \ , \ H(x_i) \leq B \ (1 \leq i \leq 2) \ , \ \frac{\partial F}{\partial X_1}(\underline{x}) \neq 0\},$$

et on cherche un nombre k'' de polynômes $F_i(X_1, X_2)$ pour couvrir ce sous-ensemble. Le nombre k de polynômes dans le théorème 2.1 sera ainsi égal à $1 + k'$.

2.2.1 Première étape : construction des ensembles du type $S(F, B, \mathfrak{p})$

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, on définit

$$S(F, B, \mathfrak{p}) = \{\underline{x} \in S(F, B) \mid \frac{\partial F}{\partial X_1}(\underline{x}) \notin \mathfrak{p}\}$$

et on a

$$S(F, B) = \bigcup_{\mathfrak{p} \text{ premier de } K} S(F, B, \mathfrak{p}).$$

Le lemme suivant montre que l'on peut ne considérer qu'un nombre fini d'idéaux premiers dans la précédente union. De plus, ces idéaux premiers peuvent être choisis totalement décomposés dans $K/\mathbb{Q}$.

Lemme 2.2. *Soient P un entier, $h(B) = \log_2(2d^3H^(F)B^{d-1})$ et $r = [\rho h(B)]+1$ (la notation [.] désignant la partie entière). Alors pour P assez grand dépendant de K, il existe r idéaux premiers de K distincts et totalement décomposés, $\mathfrak{p}_1, ...\mathfrak{p}_r$, tels que*

$$S(F, B) = \bigcup_{i=1}^{r} S(F, B, \mathfrak{p}_i)$$

et pour lesquels nous avons

$$P \leq N_{K/\mathbb{Q}}(\mathfrak{p}_i) \leq C_1 h(B)^2 \frac{P}{\log P} \log(\frac{P}{\log P})$$

pour une constante C_1 dépendant de K.

Démonstration. On fixe $\underline{x} = (x_1, x_2) \in S(F, B)$. Le lemme 1.7 permet de dire que le nombre d'idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que $\frac{\partial F}{\partial X_1}(\underline{x}) \in \mathfrak{p}$ est inférieur ou égal à $\log_2(H(\frac{\partial F}{\partial X_1}(\underline{x}))^\rho)$. La première étape de la démonstration est alors d'estimer la hauteur de

$$\frac{\partial F}{\partial X_1}(\underline{x}) \text{ pour } \underline{x} \in S(F, B).$$

On a $\frac{\partial F}{\partial X_1}(x_1, x_2) \neq 0$. On va appliquer la proposition 1.5 au polynôme $\frac{\partial F}{\partial X_1}$.

Le nombre l de monômes non nuls est majoré par le nombre de monômes de P, lui même majoré par $d(d+1)/2 \leq d^2$, le degré de ce polynôme est majoré par $d-1$. La hauteur du polynôme $\frac{\partial F}{\partial X_1}$ est majorée par $dH(F)$. En effet, en écrivant

$$F = \sum a_{ij} X_1^i X_2^j,$$

alors

$$\frac{\partial F}{\partial X_1} = \sum a_{ij} i X_1^{i-1} X_2^j.$$

Comme $i \in \mathbb{N}$, pour v une valuation archimédienne,

$$|a_{ij} \times i|_v = i|a_{ij}|_v \leq \deg_{X_1} P |a_{ij}|_v \leq d.|a_{ij}|_v.$$

Ainsi,

$$H(\frac{\partial F}{\partial X_1}) = \max_{v \in M_K}(|a_{ij} i|_v) \leq d \max_{v \in M_K}(|a_{ij}|_v) = dH(F).$$

On obtient alors par la propriété 1.5 :

$$H(\frac{\partial F}{\partial X_1}(x_1, x_2)) \leq l.H(\frac{\partial F}{\partial X_1}).B^{d-1} \leq d^3 H(F) B^{d-1}.$$

Travaillons dans la clôture galoisienne de $K/\mathbb{Q}$, que l'on note $\widehat{K}/\mathbb{Q}$. On note Γ le groupe de Galois de $\widehat{K}/\mathbb{Q}$. Les résultats autour du théorème de densité de Chebotarev appliqué à $\widehat{K}/\mathbb{Q}$ et au cas où la classe de conjugaison choisie est $C = \{1\}$ fournissent un ensemble de nombres premiers totalement décomposés dans $\mathcal{O}_{\widehat{K}}$. Ces nombres premiers seront eux aussi totalement décomposés dans $\mathcal{O}_K$. Le nombre $\pi_{\{1\}}(P)$ désigne les nombres premiers $p \leq P$ totalement décomposés dans $\mathcal{O}_K$.

Soit $x \geq 1$ tel que

$$\pi_{\{1\}}(x) \geq h(B) + 1 + \pi_{\{1\}}(P).$$

Un tel x existe et sera à déterminer. Il existe alors $[h(B)] + 1$ nombres premiers $p \in]P, x]$ totalement décomposés dans $\mathcal{O}_K$. Chaque nombre premier p donnant ρ idéaux premiers de norme égale à p, on aura ainsi $\rho[h(B)] + \rho$ idéaux premiers distincts et ce nombre est supérieur à r.

On choisit r de ces idéaux et on les note $\mathfrak{p}_1, ..., \mathfrak{p}_r$. Par le lemme 1.7, il existe un idéal, disons $\mathfrak{p}_i$ ($i \in \{1, ..., r\}$ tel que $\dfrac{\partial F}{\partial X_1}(x_1, x_2) \notin \mathfrak{p}_i$, c'est-à-dire $(x_1, x_2) \in S(F, B, \mathfrak{p}_i)$. Ainsi

$$S(F, B) = \bigcup_{i=1}^{r} S(F, B, \mathfrak{p}_i).$$

Il reste à déterminer un nombre x vérifiant $\pi_{\{1\}}(x) \geq h(B) + 1 + \pi_{\{1\}}(P)$ et le majorer afin d'estimer les normes des idéaux $\mathfrak{p}_i$ pour $i \in \{1, ..., r\}$. Par le théorème de densité de Chebotarev, on peut supposer x assez grand de sorte que $\pi_{\{1\}}(x) \geq \dfrac{x}{2|\Gamma| \log x}$. Une condition suffisante sur x devient

$$\frac{x}{2|\Gamma| \log x} \geq h(B) + 1 + \pi_{\{1\}}(P),$$

ou encore, grâce à l'inégalité $h(B) + 1 + \pi_{\{1\}}(P) \leq 3h(B)\pi_{\{1\}}(P)$, il suffit de choisir x tel que :

$$\frac{x}{\log x} \geq 6|\Gamma| h(B) \pi_{\{1\}}(P).$$

Rappelons que, selon §1.3.6, si $a > 2$, l'inégalité $\dfrac{x}{\log x} \geq a$ est vérifiée pour $x = 2a \log a$. On choisit alors x comme suit : $x = 2a \log a$ avec $a = 6|\Gamma| h(B) \pi_{\{1\}}(P)$.

Il ne reste plus qu'à majorer x. On peut supposer P assez grand en fonction de K pour que la majoration $\pi_{\{1\}}(P) \leq \dfrac{2P}{|\Gamma| \log P}$ soit vérifiée. Alors, pour $i = 1, \cdots, r$,

$$N_{K/\mathbb{Q}}(\mathfrak{p}_i) \leq x = 2a \log a \leq 12|\Gamma|\, h(B)\, \frac{2P}{|\Gamma| \log P}\, \log(6|\Gamma| h(B) \frac{2P}{|\Gamma| \log P}).$$

En conclusion, pour une constante C_1 dépendant de K, on a :

$$N_{K/\mathbb{Q}}(\mathfrak{p}_i) \leq C_1 h(B)^2 \frac{P}{\log P} \log(\frac{P}{\log P}).$$

□

Remarque 2.3. Le nombre P est ici arbitraire et supposé assez grand. La dépendance de P se fait en fonction de K. Nous le déterminerons plus tard afin d'optimiser les résultats. Au final, ce nombre dépendra de B et d. Pour qu'il soit assez grand, il suffira de supposer B lui-même assez grand. Le nombre B dépendra uniquement de K.

2.2.2 Deuxième étape : travail sur l'ensemble $S(F, B, \mathfrak{p})$ pour un $\mathfrak{p}$ fixé

Dans cette étape, on fixe un idéal $\mathfrak{p} \in \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$ et on travaille sur l'ensemble $S(F, B, \mathfrak{p})$. On rappelle que d'après le lemme 2.2, l'idéal $\mathfrak{p}$ fixé est au-dessus d'un nombre premier $p > P$ totalement décomposé et la norme de $\mathfrak{p}$ est égale à p.

Soit $\mathbb{F}_p = \mathcal{O}_K/\mathfrak{p}$ le corps résiduel de $\mathcal{O}_K$ par l'idéal premier $\mathfrak{p}$. Soit $\underline{t} = (t_1, t_2) \in \mathbb{F}_p^2$ F vu comme polynôme modulo $\mathfrak{p}$ tel que $\dfrac{\partial F}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$. On considère le sous ensemble suivant de $S(F, B, \mathfrak{p})$:

$$S(\underline{t}) = \{(x_1, x_2) \in S(F, B, \mathfrak{p}) : x_i = t_i \mod \mathfrak{p},\ i = 1, 2\}.$$

On a $S(F, B, \mathfrak{p}) = \bigcup_{\underline{t}} S(\underline{t})$ où $\underline{t}$ parcourt l'ensemble des points de F modulo p vérifiant $\dfrac{\partial F}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$. Pour $\underline{t}$ fixé, on va construire un polynôme qui s'annule en chaque point de $S(\underline{t})$. Ce polynôme sera l'un de ceux du théorème 2.1.

Pour $D > d$ fixé, on choisit un monôme $X_1^{m_1} X_2^{m_2}$ tel que le coefficient correspondant dans F ne soit pas nul, tel que $m_1 + m_2 = d$ et tel que m_1 soit maximal. On définit un ensemble $\mathcal{E}$ de monômes de degré inférieur ou égal à D :

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

On peut représenter l'ensemble $\mathcal{E}$ sur le plan par un ensemble de points à coordonnées strictement positif et délimité par la droite d'équation $e_1 + e_2 = D$.

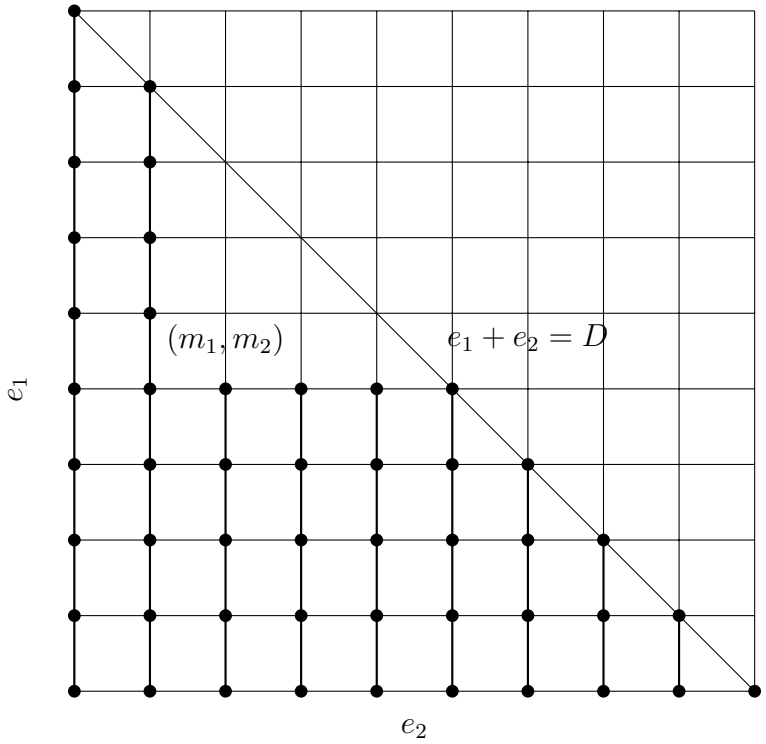


FIGURE 2.1 –

En travaillant avec cet ensemble, on ne fera pas de différence entre les exposants (e_1, e_2) et les monômes $X_1^{e_1} X_2^{e_2}$ correspondants.

Soit L le cardinal de $S(\underline{t})$ et par $\underline{x_i} = (x_{i1}, x_{i2})$ $i = 1, \cdots, L$, les éléments de $S(\underline{t})$. On note $E = \#\mathcal{E}$ et soit M la matrice de taille $L \times E$ ainsi définie :

$$M = (\underline{x_i}^{\underline{e}})_{1 \leq i \leq L,\ \underline{e} \in \mathcal{E}}.$$

Ou plus spécifiquement, en notant $\underline{X}^{\underline{e_1}}, ..., \underline{X}^{\underline{e_E}}$ les éléments de $\mathcal{E}$:

$$M = \begin{pmatrix} \underline{x_1}^{\underline{e_1}} & \cdots & \underline{x_1}^{\underline{e_E}} \\ \underline{x_2}^{\underline{e_1}} & \cdots & \underline{x_2}^{\underline{e_E}} \\ \vdots & \vdots & \vdots \\ \underline{x_L}^{\underline{e_1}} & \cdots & \underline{x_L}^{\underline{e_E}} \end{pmatrix} = \begin{pmatrix} x_{11}^{e_{11}} x_{12}^{e_{12}} & \cdots & x_{11}^{e_{E1}} x_{12}^{e_{E2}} \\ x_{21}^{e_{11}} x_{22}^{e_{12}} & \cdots & x_{21}^{e_{E1}} x_{22}^{e_{E2}} \\ \vdots & \vdots & \vdots \\ x_{L1}^{e_{11}} x_{L2}^{e_{12}} & \cdots & x_{L1}^{e_{E1}} x_{L2}^{e_{E2}} \end{pmatrix}$$

Enfin, on définit

$$E' = \sum_{i=1}^{E} (e_{i1} + e_{i2}).$$

On a la proposition suivante :

Proposition 2.4. *Si l'entier P est vérifie $P^{E(E-1)/2} \geq (E^E B^{E'})^\rho$, alors*

1. *le rang de la matrice M_2 est inférieur ou égal à $E - 1$,*
2. *il existe un polynôme $F_{\underline{t}}$ non nul de degré $\leq D$ tel que*
   - *$F_{\underline{t}}(\underline{x}) = 0$ pour tout $\underline{x}$ de $S(\underline{t})$,*
   - *$F_{\underline{t}}$ et F sont premiers entre eux.*

La preuve utilise un lemme permettant de se ramener à l'étude de polynômes en une variable qui est une version du lemme de Hensel. Cela permettra, entre autres, de pouvoir ordonner les monômes et de faire des simplifications. On désigne par $\widetilde{\mathcal{O}_K}$ le complété de $\mathcal{O}_K$ par la valuation déterminée par l'idéal premier $\mathfrak{p}$.

Lemme 2.5. *Soient $F(X_1, X_2) \in \widetilde{\mathcal{O}_K}[X_1, X_2]$ un polynôme à deux variables et $\underline{u} = (u_1, u_2) \in \widetilde{\mathcal{O}_K}^2$ tel que $F(\underline{u}) = 0$ et $\frac{\partial F}{\partial X_1}(\underline{u}) \notin \mathfrak{p}$. Alors pour tout entier $m \geq 1$, il existe $f_m(Y) \in \widetilde{\mathcal{O}_K}[Y]$ tel que si $F(\underline{x}) = 0$ pour un certain $\underline{x} = (x_1, x_2) \in \widetilde{\mathcal{O}_K}^2$ avec $\underline{x} \equiv \underline{u} \mod \mathfrak{p}$, alors*

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

Remarque 2.6. On peut positionner ce lemme dans le même genre que le théorème des fonctions implicites

Démonstration du lemme. La preuve se fait par récurrence sur m. On note

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

Pour $m = 1$, on définit $f_1(Y)$ par $f_1(x_2) = u_1$. Si $F(\underline{x}) = 0$ avec $x \equiv u \mod \mathfrak{p}$, alors $x_1 \equiv u_1 = f_1(x_2) \mod \mathfrak{p}$.

Pour $m \geq 1$, on définit f_{m+1} par

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

Soit $\underline{x} \in \widetilde{\mathcal{O}_K}^2$ tel que $\underline{x} \equiv \underline{u} \mod \mathfrak{p}$ et $F(x) = 0$. Par hypothèse de récurrence, on a $x_1 = f_m(x_2) + \alpha_1$ (où $\alpha_1 \in \mathfrak{p}^m$). La formule de Taylor tronquée modulo $\mathfrak{p}^{m+1}$ donne alors

$$0 = F(x_1, x_2) \equiv F(f_m(x_2), x_2) + \alpha_1 \frac{\partial F}{\partial X_1}(f_m(x_2), x_2) \mod \mathfrak{p}^{m+1}.$$

Or,

$$\frac{\partial F}{\partial X_1}(f_m(x_2), x_2) \equiv \frac{\partial F}{\partial X_1}(x_1, x_2) \equiv \frac{\partial F}{\partial X_1}(u_1, u_2) \mod \mathfrak{p}.$$

Et donc

$$\begin{aligned} \frac{\partial F}{\partial X_1}(f_m(x_2), x_2) &= \mu + \alpha_2 \quad (\alpha_2 \in \mathfrak{p}) \\ \alpha_1 \frac{\partial F}{\partial X_1}(f_m(x_2), x_2) &= \alpha_1 \mu + \alpha_1 \alpha_2 \\ \alpha_1 &\equiv -\mu^{-1} F(f_m(x_2, x_2) \mod \mathfrak{p}^{m+1} \end{aligned}$$

On pose

$$f_{m+1}(x_2) = f_m(x_2) - \mu^{-1} F(f_m(x_2, x_2)$$

Et on a

$$\begin{aligned} f_{m+1}(x_2) &\equiv x_1 - \alpha_1 + \alpha_1 \mod \mathfrak{p}^{m+1} \\ &\equiv x_1 \mod \mathfrak{p}^{m+1} \end{aligned}$$

□

Démonstration de la proposition 2.4.
Preuve de 1. Si $L < E$ alors on a directement le résultat. Supposons $L \geq E$. On considère un mineur d'ordre E, noté Δ. Quitte à permuter les éléments de $S(\underline{t})$, on peut considérer que $\Delta = \det[(\underline{x_i}^{\underline{e}})_{1 \leq i \leq E,\ \underline{e} \in \mathcal{E}}]$. C'est-à-dire

$$\Delta = \begin{vmatrix} \underline{x_1}^{\underline{e_1}} & \cdots & \underline{x_1}^{\underline{e_E}} \\ \underline{x_2}^{\underline{e_1}} & \cdots & \underline{x_2}^{\underline{e_E}} \\ \vdots & \vdots & \vdots \\ \underline{x_E}^{\underline{e_1}} & \cdots & \underline{x_E}^{\underline{e_E}} \end{vmatrix}$$

Nous allons montrer que $\Delta = 0$. Pour cela, on va montrer que la norme de Δ est à la fois divisible par une grande puissance p^ν de p et que la hauteur de Δ est bornée par un nombre A plus petit que p^ν et utiliser l'inégalité $N(a) \leq H(a)^\rho$ pour tout nombre $a \in \mathcal{O}_K$.

Pour chaque $i = 1, \cdots, E$, le couple $\underline{x_i} = (x_{i1}, x_{i2})$ est dans $S(\underline{t})$, en particulier $\underline{x_i} \equiv \underline{t}$ mod $\mathfrak{p}$. On a supposé de plus que $\dfrac{\partial F}{\partial X_1}(\underline{t}) \notin \mathfrak{p}$. On a alors

$$\frac{\partial F}{\partial X_1}(\underline{x_i}) \notin \mathfrak{p} \text{ et } F(\underline{x_i}) = 0 \quad (i = 1, \cdots, E).$$

Le lemme 2.5 s'applique à F en prenant pour $u \in \widetilde{\mathcal{O}_K}^2$ un relèvement de $\underline{t}$, et $\underline{x} = \underline{x_i}$ $(i = 1, \cdots, E)$; pour tout entier m supérieur à 1, il existe $f_m(Y) \in \widetilde{\mathcal{O}_K}[Y]$ tel que

$$x_{i1} \equiv f_m(x_{i2}) \mod \mathfrak{p}^m.$$

On note $\underline{w_i} = (w_{i,1}, w_{i,2}) = (f_m(x_{i,2}), x_{i,2})$ et on considère la matrice $M_0 = (\underline{w_i}^{\underline{e}})_{1 \leq i \leq E,\ \underline{e} \in \mathcal{E}}$ et son déterminant $\Delta_0 = \det(M_0)$. C'est à dire :

$$\Delta_0 = \begin{vmatrix} \underline{w_1}^{\underline{e_1}} & \cdots & \underline{w_1}^{\underline{e_E}} \\ \underline{w_2}^{\underline{e_1}} & \cdots & \underline{w_2}^{\underline{e_E}} \\ \vdots & \vdots & \vdots \\ \underline{w_E}^{\underline{e_1}} & \cdots & \underline{w_E}^{\underline{e_E}} \end{vmatrix} = \begin{vmatrix} f_m(x_{12})^{e_{11}} x_{12}^{e_{12}} & \cdots & f_m(x_{12})^{e_{E1}} x_{12}^{e_{E2}} \\ f_m(x_{22})^{e_{11}} x_{22}^{e_{12}} & \cdots & f_m(x_{22})^{e_{E1}} x_{22}^{e_{E2}} \\ \vdots & \vdots & \vdots \\ f_m(x_{E2})^{e_{11}} x_{E2}^{e_{12}} & \cdots & f_m(x_{E2})^{e_{E1}} x_{E2}^{e_{E2}} \end{vmatrix}$$

On obtient que quelque soit m,

$$\Delta \equiv \Delta_0 \mod \mathfrak{p}^m.$$

On va maintenant étudier la divisibilité en p de la norme de Δ_0.

On écrit $x_{12} = x$, $x_{i2} = x + y_{i2}$ pour $1 \leq i \leq E$, avec $y_{i2} := x_{i2} - x \in \mathfrak{p}$ car par définition de $S(\underline{t})$, $x_{i2} = t_2 \mod \mathfrak{p}$ pour $1 \leq i \leq E$, ce qui donne pour tout i, $y_{i2} = t_2 - x = 0 \mod \mathfrak{p}$.

On a alors pour $\underline{e} \in \mathcal{E}$.

$$\underline{w_i}^{\underline{e}} = f_m(x + y_{i2})^{e_1} (x + y_{i2})^{e_2} = g_{\underline{e}}(y_{i2})$$

où $g_{\underline{e}}(Y) \in \widetilde{\mathcal{O}_K}[Y]$. On obtient alors ce déterminant :

$$\Delta_0 = \begin{vmatrix} g_{\underline{e_1}}(y_{12}) & \cdots & g_{\underline{e_E}}(y_{i2}) \\ g_{\underline{e_1}}(y_{22}) & \cdots & g_{\underline{e_E}}(y_{22}) \\ \vdots & \vdots & \vdots \\ g_{\underline{e_1}}(y_{E2}) & \cdots & g_{\underline{e_E}}(y_{E2}) \end{vmatrix}$$

Chaque colonne de M_0 correspond à un polynôme $g_{\underline{e}}(Y)$. Nous ramenons l'étude à une seule variable et nous allons effectuer des opérations linéaires sur les colonnes, sans changer le déterminant de M_0 (au signe près), de façon à classer les colonnes par degré (en Y) strictement croissant. On illustrera le raisonnement par un exemple.

Plus précisément, nous feront des $\widetilde{\mathcal{O}_K}$-combinaisons linéaires sur les colonnes. Premièrement, on réordonne les colonnes par valuation Y-adique croissante. Les opérations sur les

colonnes donnent une matrice de ce type

$$\begin{pmatrix} a_{00}+\cdots & a_{11}y_{12}+\cdots & a_{21}y_{12}+\cdots & \cdots & a_{Eq}y_{12}^q+\cdots \\ a_{00}+\cdots & a_{11}y_{22}+\cdots & a_{21}y_{22}+\cdots & \cdots & a_{Eq}y_{22}^q+\cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{00}+\cdots & a_{11}y_{E2}+\cdots & a_{21}y_{E2}+\cdots & \cdots & a_{Eq}y_{E2}^q+\cdots \end{pmatrix}$$

Pour un certain entier q.

Ensuite, si deux colonnes correspondent à des polynômes $g_{\underline{e}}(Y)$ avec la même valuation Y-adique, disons δ, (c'est le cas dans notre exemple pour les colonnes 2 et 3), on réordonne les colonnes de manière à ce que la valuation $\mathfrak{p}$-adique du coefficient du monôme de valuation Y-adique δ grandit. Pour notre exemple, si la valuation $\mathfrak{p}$ adique de a_{11} est plus grande que celle de a_{21}, on préfèrera reordonner les colonnes pour obtenir

$$\begin{pmatrix} a_{00}+\cdots & a_{21}y_{12}+\cdots & a_{11}y_{12}+\cdots & \cdots & a_{Eq}y_{12}^q+\cdots \\ a_{00}+\cdots & a_{21}y_{22}+\cdots & a_{11}y_{22}+\cdots & \cdots & a_{Eq}y_{22}^q+\cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{00}+\cdots & a_{21}y_{E2}+\cdots & a_{11}y_{E2}+\cdots & \cdots & a_{Eq}y_{E2}^q+\cdots \end{pmatrix}$$

Ceci ne change pas la croisance en la valuation Y-adique des colonnes.

Maintenant, si s est le plus petit degré du polynôme dans la colonne 1, le monôme de degré s peut être retiré des colonnes 2 à E en ajoutant à celles-ci une $\widetilde{\mathcal{O}_K}$-multiple de la première colonne. En réitérant ce procédé, on classe les colonnes par degré en Y strictement croissant. Ceci est toujours possible si les colonnes sont linéairement indépendantes, et dans le cas contraire, on a directement $\Delta_0 = 0$.

A la fin de ce procédé, la l-ième colonne formée ne contient que des éléments dans $\mathfrak{p}^{l-1}$ car elle est constituée de polynômes en y_{i2} dont le premier terme est de degré supérieur à $l-1$ et $y_{i2} \in \mathfrak{p}$. Ainsi la norme $N(\Delta_0)$ est divisible par $p^{E(E-1)/2}$ et en choisissant m supérieur à $E(E-1)/2$, on obtient que $N(\Delta)$ est elle aussi divisible par $p^{E(E-1)/2}$.

Estimons maintenant la taille de $H(\Delta)$. On a $H(x_{ij}) \leq B$, $i = 1, \cdots, E$, $j = 1, 2$. Notons par S_E le groupe des permutations de E éléments et, pour $\sigma \in S_E$, $\varepsilon(\sigma)$ la signature de σ. On a

$$\Delta = \sum_{\sigma \in S_E} \varepsilon(\sigma) \prod_{i=1}^{E} \underline{x_{\sigma_i}}^{e_i}.$$

Pour v une place archimédienne,

$$\begin{aligned} |\Delta_v| &\leq E! \max_{1 \leq j \leq E} (|x_{j1}|^{e_{11}} |x_{j2}^{e_{12}}|) \times \cdots \times \max 1 \leq j \leq E |x_{j1}|^{e_{E1}} |x_{j2}|^{e_{E2}}) \\ &\leq E! B^{e_{11}+e_{12}} \times \cdots \times B^{e_{E1}+e_{E2}} \end{aligned}$$

On obtient alors si $\Delta \neq 0$:

$$\begin{aligned} H(\Delta) &= \max_{v/\infty} (|\Delta|_v) \\ &\leq E! B^{e_{11}+e_{12}} \times \cdots \times B^{e_{E1}+e_{E2}} \end{aligned}$$

En résumé, $N(\Delta)$ est divisible par $p^{E(E-1)/2}$ mais $N(\Delta) \leq H(\Delta)^\rho \leq (E^E B^{E'})^\rho$. On a alors montré que sous la condition $p^{E(E-1)/2} > (E^E B^{E'})^\rho$, alors $\Delta = 0$. Le nombre Δ désignant un mineur quelconque de M, le rang de M est inférieur à $E-1$. Comme $p \geq P$, il suffit de choisir $P^{E(E-1)/2} \geq (E^E B^{E'})^\rho$ pour arriver au résultat.

Remarque 2.7. L'utilisation de notre hauteur est particulièrement approprié pour l'extimation de $H(\Delta)$. L'utilisation de la hauteur de Weil amène naturellement à un exposant plus grand en B.

Preuve de 2. Le rang de la matrice M_2 étant inférieur à $E-1$, on peut en déduire qu'il existe une matrice $C = (c_{\underline{e}}) \in \mathcal{O}_K^E$ non nulle, telle que $M.C = 0$. Cette matrice nous permet de construire le polynôme $F_{\underline{t}}$ recherché :

$$F_{\underline{t}}(X_1, X_2) = \sum_{\underline{e} \in \mathcal{E}} c_{\underline{e}} X_1^{e_1} X_2^{e_2}.$$

C'est un polynôme non nul de degré inférieur à D et tel que $F_{\underline{t}}(x) = 0$ pour tout x de $S(\underline{t})$.

Pour montrer que $F_{\underline{t}}$ et F sont premiers entre eux, on se sert de l'argument donné par Walkowiak (voir [Wal05, §1.3.4]).

On écrit $F(X_1, X_2) = \sum_f a_f X_1^{f_1} X_2^{f_2}$ où $f = (f_1, f_2)$ parcourt l'ensemble des monômes de degré inférieur ou égal à d. Supposons que $F_{\underline{t}}$ et F ne soient pas premiers. Alors, comme $D > d$, il existe un polynôme G tel que $F_{\underline{t}} = FG$. On note par d' le degré de G. Il existe un monôme $X_1^{g_1} X_2^{g_2}$ dans G de coefficient non nul, tel que $g_1 + g_2 = d'$ et g_1 est maximal.

Alors le monôme $X_1^{m_1+g_1} X_2^{m_2+g_2}$ dans FG a un coefficient non nul. Comme $m_1 + g_1 \geq m_1$ et $m_2 + g_2 \geq m_2$, ce monôme n'est pas dans l'ensemble $\mathcal{E}$ (on peut se référer à la figure 2.1 pour illustrer le raisonnement). Ceci est impossible car les coefficients de $F_{\underline{t}}$ doivent être dans $\mathcal{E}$. Ceci prouve que F et $F_{\underline{t}}$ sont premiers entre eux. □

2.2.3 Fin de la démonstration

Sous la condition que P est suffisamment grand, par le lemme 2.2 et la proposition 2.4, nous avons donc construit un seul polynôme associé à un ensemble du type $S(\underline{t})$ lui-même à l'intérieur d'un ensemble du type $S(F, B, \mathfrak{p})$. Le nombre k vérifie

$$k = 1 + k' = 1 + \sum_{i=1}^{r} k''_{\mathfrak{p}_i}$$

où $k''_{\mathfrak{p}}$ est le nombre d'ensemble du type $S(\underline{t})$ dans $S(F, B, \mathfrak{p})$ et $r = [\rho \log_2(2d^3 H(F) B^{d-1})] + 1$. Le lemme suivant nous donne une majoration de $k''_{\mathfrak{p}}$:

Lemme 2.8. *On a*

$$k''_{\mathfrak{p}} \leq 2d^3 p.$$

Remarque 2.9. On rappelle que l'on doit supposer P suffisamment grand pour pouvoir appliquer le lemme 2.2. Le choix de P est donné dans la preuve du théorème 2.1. Ce choix est fait de manière à pouvoir directement appliquer la proposition 2.4. Nous verrons aussi que $P > B^{1/d}$ ce qui permettra de dire que B doit être suffisamment grand pour que P lui-même le soit.

Démonstration. Le nombre k'' est le nombre de points $\underline{t} \in \mathbb{F}_p^2$ vérifiant $\dfrac{\partial F}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$ et $F(\underline{t}) = 0$. Écrivons la décomposition $F(X_1, X_2) = \prod_{j=1}^{s} F_j(X_1, X_2)$ en irréductibles de $\overline{\mathbb{F}_p}[X_1, X_2]$. Certains de ces $F_j(X_1, X_2)$ sont à coefficients dans $\mathbb{F}_p$. Pour ceux qui ne le sont pas, on peut montrer par le même type de raisonnement que dans la propriété 2.3, qu'un zéro dans $\mathbb{F}_p^2$ d'un des F_j, est en fait un zéro double de F.

En effet si pour $\underline{t} = (t_1, t_2) \in \mathbb{F}_q^2$, $F_j(\underline{t}) = 0$, alors $\underline{t}$ est aussi un zéro pour un conjugué de F_j qui est un autre facteur de F. Il en résulte que t_1 est racine double de $F(X_1, t_2)$, et donc

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

(de même pour t_2).

Ce point $\underline{t}$ est alors un point singulier modulo $\mathfrak{p}$, il ne compte donc pas dans le nombre k'' cherché. On ne considère donc que les polynômes F_j qui sont à coefficients dans $\mathbb{F}_p$. Ceux-ci sont absolument irréductibles, leur nombre est inférieur à d et leur degré inférieur à d. D'après les inégalités de Lang-Weil [LW54, theorem 1], [FJ86, theorem 5.4.1] :

$$\begin{aligned} k''_{\mathfrak{p}} &\leq d(p + 1 + (d-1)(d-2)\sqrt{p}) \\ &\leq d(p + 1 + (d-1)(d-2)\sqrt{p}) \\ &\leq 2d^3 p \end{aligned}$$

□

Démonstration du théorème 2.1. D'après le lemme 2.2, $P \leq c_1 \log_2^2(2d^3 H(F) B^{d-1}) P$ où c_1 est une constante dépendant de K. Ce qui donne :

$$p \leq c_1 \log_2^2(2d^3 H(F) B^{d-1}) P$$

On peut alors dire que

$$k''_{\mathfrak{p}} \leq 2d^3 c_1 \log_2^2(2d^3 H(F) B^{d-1}) P.$$

Le nombre k est alors majoré par :

$$k_1 d^3 \log^3(2d^3 H(F) B^{d-1}) P.$$

où k_1 est encore une constante dépendant de K.

Pour continuer la majoration, il reste à préciser le nombre P. Pour cette majoration, on reprend la démonstration donnée par Walkowiak [Wal05, §1.3.5]. Par le lemme 2.2, le nombre premier p est plus grand que P. La condition donnée dans la preuve de la proposition 2.4 est $p^{E(E-1)/2} > (E^E B^{E'})^\rho$ où $E = \#\mathcal{E}$ et $E' = \sum_{e\in\mathcal{E}} e_1 + e_2$.
C'est-à-dire

$$p > (E^{M_1} B^{M_2})^\rho$$

où $M_1 := \dfrac{2}{(E-1)}$ et $M_2 := \dfrac{2E'}{E(E-1)}$.

L'ensemble $\mathcal{E}$ a été défini comme

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

où (m_1, m_2) est un exposant tel que $m_1 + m_2 = d$. On a $E = \#\mathcal{E}_1 - \#\mathcal{E}_2$ avec
$\mathcal{E}_1 = \{(e_1, e_2) \in \mathbb{Z}^2 : e_i \geq 0 \ (i = 1, 2),\ e_1 + e_2 \leq D\}$,
$\mathcal{E}_2 = \{(e_1, e_2) \in \mathbb{Z}^2 : e_i \geq 0 \ (i = 1, 2),\ e_1 + e_2 \leq D,\ e_i \geq m_i \ (i = 1, 2)\}$.
Le cardinal de $\mathcal{E}_1$ se détermine en donnant pour chaque choix de e_1 (entre 0 et D) le nombre de choix pour e_2 (de $D+1$ à 0).

$$\#\mathcal{E}_1 = (D+1) + D + (D-1) + ... + 1 = \frac{(D+1)(D+2)}{2}.$$

Le cardinal de $\mathcal{E}_2$ se détermine de la même manière. Les choix pour e_1 sont $m_1, m_1 + 1, ..., D - m_2$ et le nombre de choix pour e_2 correspondant à chaque e_1 choisi sont $(D - m_1 - m_2 + 1), ..., 2, 1$, Et $D - m_1 - m_2 + 1 = D - d + 1$.

$$\#\mathcal{E}_2 = 1 + 2 + ... + (D - d + 1) = \frac{(D-d+1)(D-d+2)}{2}.$$

On a donc, après calculs

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

On obtient $M_1 = \dfrac{2}{E-1} \leq \dfrac{2}{dD - d^2/2} \leq \dfrac{2D+2d}{2dD^2}$. C'est à dire

$$M_1 \leq \frac{2}{dD} + \frac{2}{D^2}$$

De la même manière, on peut estimer $E' = E'_1 + E'_2$ avec $E'_i = \sum_{e\in\mathcal{E}} e_i = \sum_{e\in\mathcal{E}_1} e_i - \sum_{e\in\mathcal{E}_2} e_i$.

On a $\sum_{e\in\mathcal{E}_1} e_i = \dfrac{D}{3}\dfrac{(D+1)(D+2)}{2}$,
et $\sum_{e\in\mathcal{E}_2} e_i = (m_i + \dfrac{D-d}{3})\dfrac{(D-d+1)(D-d+2)}{2}$.

Cela donne $E' \leq \frac{dD^2}{2} + \frac{dD}{2}$. Et après calculs

$$M_2 = \frac{2E'}{E(E-1)} \leq \frac{1}{d} + \frac{6}{D}.$$

On a alors une condition suffisante pour la condition $P > (E^{M_1}B^{M_2})^\rho$ qui est

$$P > (E^{2(dD)^{-1}+2D^{-2}}B^{d^{-1}+6D^{-1}})^\rho.$$

En remarquant que $E \leq 2dD$ et, par une étude de fonction élémentaire,

$$(2dD)^{2(dD)^{-1}+2D^{-2}} \leq e^8$$

pour $D > d$, on peut choisir

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

Le nombre P ainsi choisi vérifie la condition suffisante précédemment énoncée et on a de plus

$$P \leq (2^{13}B^{d^{-1}+6D^{-1}})^\rho.$$

On peut maintenant retourner à la majoration du nombre k pour $D > d$. On a clairement $P > B^{d^{-1}}$, ce qui nous permet, en supposant B assez grand, que P est lui même assez grand pour pouvoir appliquer le lemme 2.2.

D'après le lemme 2.2 et la proposition 2.4, on a

$$\begin{aligned} k &\leq k_1 d^3 \log^3(2d^3 H(F)B^{d-1})P \\ &\leq c_2 d^3 \log^3(2d^3 H(F)B^{d-1})(B^{d^{-1}+6D^{-1}})^\rho \end{aligned}$$

Où c_2 est la constante énoncée dans le théorème. □

2.3 Application au calcul de $N(F, B)$.

Le théorème de Heath-Brown généralisé aux corps de nombre va nous permettre de donner un résultat sur le nombre $N(F, B)$. On démontrera le théorème suivant :

Theorème 2.10. *Soient $F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$ irréductible sur K, unitaire en X_2 et de degré total $d \geq 1$. Pour B suffisamment grand, dépendant de K, on a*

$$N(F, B) \leq c_5 d^{14} \log^4(B)B^{\rho/d}$$

où c_4 est une constante dépendant uniquement de K.

Remarque 2.11. Noter que la borne ne dépend pas de la hauteur. C'est la propriété 2.14 qui permet de donner un résultat indépendant de la hauteur, grâce au *lemme de Siegel* (voir lemme 2.13. la borne du théorème 2.10 donné indépendamment de la hauteur $H(F)$ est un passage nécessaire dans notre démonstration du théorème 3.2 qui en découle et permet une utilisation simple de celui-ci pour les applications en théorie inverse de Galois.

2.3.1 Le cas non absolument irréductible

Si le polynôme F n'est pas absolument irréductible, c'est à dire non irréductible dans $\overline{K}[X_1, X_2]$, on a directement une majoration pour le nombre $N(F, B)$ sans utiliser le théorème 2.1.

Proposition 2.12. *Soit $F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$ de degré d, irréductible dans $K[X_1, X_2]$ et non absolument irréductible, alors $N(F, B) \leq 4d^4$.*

Démonstration. Nous allons majorer le nombre $N(F, B)$ indépendamment de B. Pour cela, on va compter le nombre d'éléments $x_1 \in \mathcal{O}_K$ tels qu'il existe un nombre $x_2 \in \mathcal{O}_K$ avec (x_1, x_2) annulant $F(X_1, X_2)$. Le raisonnement similaire avec x_2 nous permettra de conclure.

Le polynôme $F(X_1, X_2)$ n'étant pas absolument irréductible, on peut le décomposer en plusieurs facteurs irréductibles, en comptant les multiplicités, dans $\overline{\mathbb{Q}}[X_1, X_2]$.

Considérons un couple $(x_1, x_2) \in \mathcal{O}_K^2$ tel que $F(x_1, x_2) = 0$. Cela implique que

$$\varphi(x_1, x_2) = 0$$

pour un des facteurs irréductibles $\varphi \in \overline{K}[X_1, X_2]$ qui est aussi unitaire en X_2 et de degré $< d$. On a alors $\psi(x_1, x_2) = 0$ pour un K-conjugué de φ sur K qui est un autre facteur de F distinct de φ.

En effet, $\varphi(X_1, X_2) \notin K[X_1, X_2]$, sinon $F(X_1, X_2)$ ne serait pas irréductible dans $K[X_1, X_2]$. Il existe donc $\sigma \in Gal(\overline{K}/K)$ tel que $\psi = \sigma(\varphi) \neq \varphi$. Comme $\sigma(F) = F$, $\sigma(x_1) = x_1$ et $\sigma(x_2) = x_2$ alors ψ divise F et $\psi(x_1, x_2) = 0$. De plus, φ et ψ ne sont pas associés car s'ils l'étaient, étant donné qu'ils sont unitaires en X_2, alors ils seraient égaux.

Ainsi, le produit $\varphi\psi$ divise F. Le nombre x_1 est alors un zéro double du polynôme en une variable $F(X_1, x_2)$. Le nombre de x_1 vérifiant cette propriété et majoré par le nombre de racines du polynôme $disc_{X_2}(F)$. Ce polynôme est de degré au plus $(2d-1)d \leq 2d^2$.

En faisant le même raisonnement pour x_2, on obtient que le nombre total de points entiers annulant F est majoré par $2d^2.2d^2 = 4d^4$. On obtient $N(F, B) \leq 5d^4$ pour n'importe quel nombre B donné. □

2.3.2 Le cas absolument irréductible

On suppose maintenant que $F(X_1, X_2)$ est irréductible dans $\overline{K}[X_1, X_2]$. Pour les applications qui suivront ce résultat (voir chapitre 3), nous aurons besoin d'une majoration de $N(F, B)$ indépendante de la hauteur $H(F)$ de F. On utilise pour cela le *lemme de Siegel*. On renvoie à [MR14, chapitre 6] pour une démonstration de ce lemme sur un corps de nombres dont on donne un énoncé ci dessous.

Lemme 2.13. *[lemme de Siegel sur un corps de nombres] Soit K un corps de nombres et N, M des entiers tels que $1 \leq M < N$.Soit H_0 un nombre réel positif et $a_{ij} \in K$, $1 \leq i \leq N$, $1 \leq j \leq M$, des éléments non tous nuls de hauteur au plus H_0. Alors il existe un vecteur $x \in \mathcal{O}_K^N \backslash \{0\}$ tel que :*

$$\sum_{i=1}^{N} a_{ij} x_i = 0 \ , \ j = 1, ..., M$$

et tel que $\max_{1 \leq i \leq N} H(x_i) \leq C(CNH_0)^{M/(N-M)}$, où C est une constante absolue ne dépendant que de K.

On note par C la constante apparaissant dans le lemme 2.13. On a la proposition suivante :

Proposition 2.14. *Soit $F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$ un polynôme irréductible dans $K[X_1, X_2]$, de degré d. Alors*

$$\text{soit } N(F, B) \leq d^2 + 3 \text{ soit } H(F) \leq C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}.$$

Démonstration. Supposons que $N(F, B) > d^2 + 3$. On pose $R := d^2 + 4$, $N = (d+1)(d+2)/2$ et on suppose que F admet au moins R zéros $\underline{x_1}, ..., \underline{x_R}$ telles que

$$H(x_{ij}) \leq B \ (1 \leq i \leq N, j = 1, 2).$$

Le nombre de monômes possibles de degré inférieur ou égal à d en les variables x_{i1}, x_{i2} est $1 + 2 + ... + (d + 1) = N$. On pose $A = (a_{i,j})$ la matrice de taille $R \times N$ dont la i-ième ligne est formée de ces N monômes.

On note par f_j $(j = 1, \cdots, N$ les N coefficients (peut être nuls) de F. Etant donné que les élements $\underline{x_1}, ..., \underline{x_R}$ sont des zéros de F, en notant $f \in \mathcal{O}_K^N$ la matrice colonne dont les composantes sont les coefficients de F, on a :

$$Af = \begin{pmatrix} 1 & x_{11} & \cdots & x_{11}^d & x_{12} & \cdots x_{12} x_{11}^{d-1} & \cdots & x_{12}^d \\ 1 & x_{21} & \cdots & x_{21}^d & x_{22} & \cdots x_{22} x_{21}^{d-1} & \cdots & x_{22}^d \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{R1} & \cdots & x_{R1}^d & x_{R2} & \cdots x_{R2} x_{R1}^{d-1} & \cdots & x_{R2}^d \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_N \end{pmatrix} = 0$$

et la matrice A est solution du système $AX = 0$.

On note $l_1, ..., l_R$ les lignes de A. Dire que $AX = 0$ c'est dire que $l_i(X) = 0$, pour i entre 1 et R. La matrice A possède plus de lignes que de colonnes, le lemme de Siegel ne peut pas s'appliquer dans ce cas. Mais comme le système $AX = 0$ admet une solution non triviale f, le rang de la matrice A est strictement inférieur à N et on note par $M < N$ ce rang.

Quitte à re-numéroter les lignes, on peut considérer que le système $AX = 0$ est équivalent à $l_i(X) = 0, 1 \leq i \leq M$, ou encore $A'X = 0$ où A' est la matrice formée par les M premières lignes.

Comme $N > M$, le lemme de Siegel permet de dire que ce système admet une solution non nulle $g \in \mathcal{O}_K^N$ vérifiant

$$\max_{k=1,\dots,M} H(g_k) \leq C(CNB^d)^{M/(N-M)}.$$

car les $H(c_{i,j})$ sont tous majorés par B^d. La constante C dépend uniquement de K.

On déduit ensuite un polynôme $G(X_1, X_2)$ dont les coefficients sont les éléments de g. Le polynôme G est donc un polynôme non nul, à coefficients dans $\mathcal{O}_K$, de degré inférieur ou égal à d et tel que $G(x_{i1}, x_{i2}) = 0$ $(1 \leq i \leq N)$.

Par construction, F et G ont $d^2 + 4$ zéros en commun et sont de degré inférieur ou égal à d. D'après le théorème de Bézout, ces deux polynômes ne sont pas premiers entre eux. Le polynôme F étant irréductible, de degré d, on peut conclure que $G = aF$ pour un $a \in K$ (en supposant que F est unitaire en X_2, alors $a \in \mathcal{O}_K$ et $H(F) \leq H(aF)$). Et donc

$$H(F) \leq \max_{i=1,\dots,N} H(g_i) \leq C(CNB^d)^{M/(N-M)} \leq C(CNB^d)^N.$$

En remarquant que $N \leq 2d^2$, on arrive à la conclusion que

$$H(F) \leq C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}.$$

□

On peut maintenant majorer le nombre $N(F, B)$ cherché.

Démonstration du théorème 2.10. Le théorème 2.1 a majoré le nombre k de polynômes suffisants afin de couvrir l'ensemble des zéros (x_1, x_2) de F tels que $H(x_1) \leq B$ et $H(x_2) \leq B$:

$$k \leq c_2 d^3 \log^3(2d^3 H(F) B^{d-1})(B^{d^{-1}+6D^{-1}})^\rho \log^\rho(B)$$

où c_2 est une constante dépendant de K.

Pour majorer le nombre $N(F, B)$, on applique le théorème de Bézout et on compte les intersections de F avec chacun des F_i. Le nombre de points d'intersection entre les zéros des polynômes F et F_i est au plus $deg(F) \times deg(F_i) = d \times D$. Ce qui donne :

$$N(F, B) \leq \sum_{i=1}^{k} \deg(F) \deg(F_i) \leq kdD \leq c_2 d^4 D \log^3(2d^3 H(F) B^{d-1})(B^{d^{-1}+6D^{-1}})^\rho$$

où c_2 dépend de K.

On rappelle que la condition sur D est d'être choisi supérieur à d. On peut choisir

$$D = [dlog(B) + 1],$$

et en majorant $B^{6(dlog(B))^{-1}}$ par 2^9, on peut écrire :

$$N(F, B) \leq c_2' d^5 \log^3(2d^3 H(F) B^{d-1}) B^{\rho/d} \log(B).$$

La majoration $H(F) \leq C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}$ de la proposition 2.14 nous donne :

$$N(F,B) \leq c_3 d^5 D \log^3(d^3 C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3} B^{d-1})(B^{\rho/d} \log(B)).$$

Enfin,

$$\begin{aligned} &\log(d^3 C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3} B^{d-1}) \\ &= 3\log(d) + (5d^2)\log(C) + 8d^2\log(2) + 8d^2\log(d) + 4d^3\log(B) + (d-1)\log(B) \end{aligned}$$

Cette dernière quantité peut être majorée par $c_4 d^3 \log(B)$, on obtient :

$$N(F,B) \leq c_5 d^{14} \log^4(B) B^{\rho/d}.$$

□

CHAPITRE 3

Spécialisation et théorème d'irréductibilité de Hilbert effectif sur un corps de nombres

Le théorème d'irréductibilité de Hilbert permet spécialiser l'indéterminée T d'un polynôme irréductible $P(T,Y) \in K[T,Y]$ en une infinité de $t \in K$ tels que le polynôme spécialisé $P(t,Y)$ soit irréductible dans $K[Y]$. L'étude de l'effectivité dans ce théorème consiste soit à borner le plus petit t ayant la bonne propriété, soit, étant donné une borne $B > 1$, estimer le nombre de t de hauteur $H(t) \leq B$ ayant la bonne propriété.

La deuxième preuve du théorème d'irréductibilité de Hilbert date de 1927. Elle est due à Dörge [Dör27]. Elle repose sur l'approche de Hilbert et son résultat permet d'énoncer le théorème sous la forme suivante :

Theorème. *Soit $P(T,Y)$ un polynôme irréductible dans $\mathbb{Q}(T)[Y]$. Alors il existe δ tel que $0 < \delta < 1$ et $\#\{t \in \mathbb{Z} \mid P(T,Y)$ irreductible dans $\mathbb{Q}[Y]$ et $|t| \leq B\} = O(B^{1-\delta})$.*

Il faudra attendre 1929 grâce à un théorème dû à C.L. Siegel pour améliorer l'exposant $1-\delta$ en $\frac{1}{2}$. L'exposant $\delta = \frac{1}{2}$ est le meilleur possible en général. On peut remarquer que ce résultat ne précise pas les constantes dans le $O(.)$ et les premières démonstrations du théorème d'irréductibilité ne sont pas simples à rendre plus explicites.

D'autres recherches ont été menées sur le sujet [Fri74],[SZ95a], [Dèb86] et les premières majorations étaient plutôt lourdes. On peut noter, par exemple, que cette version effective du théorème pour un polynôme $P(T,Y) \in \mathbb{Q}[T,Y]$ fournit une majoration en "exponentielle" en le degré du polynôme.

Theorème. *[SZ95a]. Soit m le degré de P en T et n le degré de P en Y. Il existe un entier positif t tel que :*

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

et $P(t, Y)$ soit irréductible sur $\mathbb{Q}$.

Le nombre $H(P)$ est la hauteur du polynôme $P(T, Y)$.

On s'intéresse plus particulièrement à la méthode suivie par Walkowiak [Wal04], [Wal05], dont le but était de trouver une majoration polynômiale en $\log(H)$ et en le degré de P et de créer un algorithme de factorisation de polynômes à deux variables. En effet, une borne polynômiale est importante pour qu'un algorithme trouve en temps convenable un "bon" t.

Le travail conséquent de Walkowiak permet d'arriver à ce théorème général :

Theorème. *Il existe un entier positif t tel que*

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

et $P(t, Y)$ soit irréductible sur $\mathbb{Q}$.

De plus, la borne du théorème s'améliore en borne polynômiale cherchée lorsque l'extension de départ sur $\mathbb{Q}(T)$ donnée par le polynôme irréductible $P(T, Y)$ est galoisienne. Ce qui nous donne ce dernier résultat :

Theorème. *Dans le cas galoisien, il existe un entier positif t tel que*

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

et $P(t, Y)$ soit irréductible sur $\mathbb{Q}$ (où c est une constante absolue issue d'un théorème de L.Pyber en théorie des groupes).

La démarche suivie par Walkowiak utilise la démonstration de la forme explicite du théorème de Heath-Brown (voir chapitre 2) et ont été démontrés que sur le corps $\mathbb{Q}$ et où $P(T, Y)$ est à coefficients dans $\mathbb{Z}$. La généralisation du résultat de Heath-Brown à tout corps de nombres est alors une étape primordiale si on veut généraliser le résultat de Walkowiak sur le théorème d'irréductibilité de Hilbert.

Les résultats de ce chapitre découlent donc du théorème 2.10. Le *théorème de spécialisation* 3.2 est une étape classique dans la démonstration du théorème d'irréductibilité de Hilbert. Il donne une borne pour le nombre de $t \in O_K$ tels qu'un polynôme $F(T, Y)$, supposé irreductible dans $K[T, Y]$, spécialisé en $T \to t$ admet une racine dans O_K. Un résultat effectif de ce théorème nous permet d'énoncer une forme effective du théorème d'irréductibilité de Hilbert.

Le lien entre le théorème d'irréductibilité de Hilbert et le théorème de spécialisation est le suivant : il existe un certain ensemble de polynômes irréductibles $Q_1(T, Y), \cdots, Q_n(T, Y)$ tels que pour tout $t \in K$, si la spécialisation $P(t, Y)$ du polynôme $P(T, Y)$ est réductible

dans $K[Y]$, alors un des polynômes spécialisés $Q_1(t,Y),\cdots,Q_n(t,Y)$ admet une racine dans K.

Plus de détails sont donnés dans la démonstration du théorème d'irréductibilité. On démontre dans un premier temps le théorème 3.2 à partir du résultat du chapitre précédent (théorème 2.10). On démontre ensuite le théorème d'irréductibilité de Hilbert effectif en détaillant la construction des polynômes Q_i, $i=1,\cdots,n$. Le théorème 3.2 de la première section sera utilisé dans le chapitre suivant sur les applications en théorie inverse de Galois.

3.1 Un théorème de spécialisation

On considère un polynôme à deux variables $F(T,Y)\in O_K[T,Y]$, irréductible dans $K[T,Y]$, unitaire en Y et de degré ≥ 2. On désigne par :

— $m\geq 1$ le degré en T de F
— $n\geq 1$ le degré en Y de F
— d le degré total de F
— $H=\max(H(F),e^e)$

Le nombre H défini ainsi est utilisé dans la démonstration du théorème 3.2. On y travaillera avec un nombre $L_2=\log\log H$ qui devra etre ≥ 1. Le nombre H permet aussi de rendre le théorème 3.2 cohérent dans le cas spécial où $H(F)=1$. En effet, le théorème donne une borne pour le nombre $N_T(F,B)$ défini ci dessous comportant un facteur $\log H$.

Le nombre B sera un nombre réel que l'on devra supposer assez grand. Le résultat de cette section permet de borner le nombre de $t\in O_K$ pour lesquels la hauteur $H(t)$ est majorée par B et le polynôme spécialisé $F(t,Y)$ a une racine dans O_K. On notera ce nombre $N_T(F,B)$.

Pour $t\in O_K$, vérifiant $H(t)\leq B$, nous pouvons donner une majoration des eventuelles racines $y\in K$ (ou plus précisément $y\in O_K$ car $F(T,Y)$ est unitaire en Y) du polyôme $F(t,Y)$ en utilisant les inégalités de Liouville. On utilisera les inégalités de Liouville données en §1.3.2. On a le lemme suivant

Lemme 3.1. *Soit $F(T,Y)\in O_K[T,Y]$ irréductible sur K. Pour $t\in O_K, H(t)\leq B$, les hauteurs des nombres $y\in O_K$ tels que $F(t,y)=0$ sont majorées par $2(m+1)H(F)H(t)^m$.*

Démonstration. On considère le polynôme F en l'indéterminée Y et on écrit $F(T,Y)$ sous la forme

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

Ainsi, on a $F(t,Y)=Y^n+\cdots+a_n(t)$. Les polynômes en une variable $a_i(T)$ sont de degré au plus m (le nombre de termes est alors au plus $m+1$) et leurs coefficients sont parmi ceux de $F(T,Y)$, ce qui donne $H(a_i(T))\leq H(F)$, $i=1,\cdots,n$.

L'inégalité de Liouville permet de majorer la hauteur des nombres $y\in O_K$ solutions de l'équation $F(t,Y)=0$:

$$H(y)\leq 2H(F(t,Y)).$$

Or $H(F(t,Y)) = H(a_0(t),\cdots,a_n(t)) = \max_{1\leq i\leq n}\max_{v\in M_K}|a_i(t)|_v$.

Pour v une place archimédienne, $|a_i(t)|_v \leq (m+1)\max_{1\leq j\leq n}(|a_{ij}|_v)\max|t|_v^m$.
Alors $|a_i(t)|_v \leq (m+1)H_v(F)|t|_v^m$.

On a donc

$$\begin{aligned}\max_{1\leq i\leq n}\max_{v\in M_K}|a_i(t)|_v &\leq (m+1)\max_{v\in M_K}H_v(F)\max_{v\in M_K}|t|_v^m\\ &\leq (m+1)H(F)H(t)^m\end{aligned}$$

Et donc

$$H(y) \leq 2(m+1)H(F)H(t)^m.$$

Enfin, le nombre d'entiers $t\in O_K$ racine de $a_0(T)$ est majoré par m ; la hauteur $H(t)$ étant majorée par B, on obtient le résultat. □

Afin de majorer le nombre $N_T(F,B)$, On peut être tenté d'utiliser directement le lemme 3.1 en disant que $N_T(F,B)\leq N(F,B')$ avec $B' = 2(m+1)H(F)B^m$ mais nous n'obtiendront pas une bonne conclusion. La démonstration passe par la construction d'un autre polynôme G que nous allons donner dans la preuve du théorème suivant.

Theorème 3.2. *Il existe des nombres $a_1,...,a_4$ dépendant de K, tels que pour tout B assez grand, le nombre $N_T(F,B)$ de $t\in O_K$ avec $H(t)\leq B$ et tels que $F(t,Y)$ ait une racine dans K vérifie*

$$N_T(F,B) \leq a_1 d^{a_2}(\log H)^{a_3}B^{\rho/n}\log^{a_4}B$$

Remarque 3.3. Le nombre total de $t\in\mathcal{O}_K$ avec $H(t)\leq B$ est asymptitique à $B^{[K:\mathbb{Q}]}$ (à une constante multiplicative près et un facteur $\log B$) [Sch79] [Bar14]. L'étude de ce nombre a été menée par beaucoup d'auteurs et bon nombres de résultats utilisent ce dernier.

Concernant notre résultat et le comparant avec le nombre $N(B)$ de $t\in\mathcal{O}_K$ avec $H(t)\leq B$, on peut déduire que le nombre $N_T(F,B)$ est une quantité faible comparé à $N(B)$ lorsque B grandit et lorsque n grandit. Ceci permet de dire qu'il y a un nombre conséquent de "bons" t pour lesquels la propriété "$F(t,Y)$ n'a pas de racine" s'applique. Une implication directe de cette propriété est le théorème d'irréductibilité de Hilbert (voir §3.2) et les applications en théorie inverse de Galois (voir chapitre 4) où l'on démontre également un théorème type Hilbert à partir du théorème 3.2.

Démonstration. On définit deux nombres : $L_1 := \log(H)$ et $L_2 := \log(\log(H))$. Par définition de H, on a $L_2\geq 1$. Comme $F(T,Y)$ est unitaire en Y, on a $d\leq n+m-1$. Etant donné que $m\geq 1$ et $n\geq 1$, on a $d\leq mn\leq mnL_1/L_2$. On considère maintenant le polynôme

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

où $E = [mn\frac{L_1}{L_2}\frac{\log B}{\log\log B}]+1\leq 2mnL_1$. Ce polynôme est de degré $d' = \deg[G)$ vérifiant

$$nE\leq d'\leq nE+m$$

et tout zéro $(t, y) \in O_K^2$ de F correspond à un zéro de la forme $(t, y') = (t, y - t^E) \in O_K^2$ de G.

Par l'inégalité

$$H(a + b) \leq H(a) + H(b),$$

on a pour tout zéro (t, y') de G tel que $H(t) \leq B$,

$$H(y') \leq 2(m + 1)HB^m + B^E \leq 3(m + 1)HB^E.$$

En posant $B'' = 2(m + 1)HB^E$, on a

$$N_T(G, B) \leq N(G, B'').$$

On applique alors le théorème 2.10 au polynôme G avec B'' :

$$\begin{aligned} N(G, B'') &\leq c_5 d'^{14} \log^4(B'') B''^{\rho/d'} \\ &\leq c_5(nE + m)^{14} \log^4(3(m + 1)HB^E)(3(m + 1)HB^E)^{\rho/nE} \\ &\leq c_5(nE + m)^{14} \log^4(3(m + 1)HB^E)(3(m + 1)H)^{\rho/nE} B^{\rho/n} \end{aligned}$$

Les constructions de L_1 et L_2 nous permettent des majoration efficaces :

— la majoration $1/nE \leq L_2/L_1$ donne $H^{1/nE} \leq log(H)$,

— La majoration $1/nE \leq \dfrac{\log\log B}{m \log B}$ donne

$$B^{m\rho/nE} \leq B^{\rho \log\log B/\log B} = \log^\rho B.$$

On majore ensuite $nE + m$ par $3d^3 \log H \log B$ et $\log(2(m + 1)HB^E)$ par $4d^3 \log H \log B$. On obtient alors

$$N(G, B'') \leq c_5(3d^3 \log H \log B)^{14}(4d^3 \log H \log B)^4(2^\rho d^\rho \log^\rho H) \log^\rho B B^{\rho/n}).$$

Après calcul, on obtient que le nombre de $t \in O_K$ de hauteur inférieur à B tels que $F(t, Y)$ ait un zéro dans O_K est plus petit que

$$c_6 d^{54+\rho} \log^{18+\rho} H B^{\rho/n} \log^{18+\rho} B.$$

□

3.2 Un théorème de Hilbert effectif sur un corps de nombres.

Nous allons démontrer le théorème de Hilbert de façon effective. Soit $P(T,Y) \in \mathcal{O}_K[T,Y]$ un polynôme irréductible sur K. Le but est de trouver des spécialisations $t \in \mathcal{O}_K$ telles que le polynôme $P(t,Y) \in \mathcal{O}_K[Y]$ soit irréductible. Nous présenterons le théorème dans le cas général en explicitant les polynômes issus de la réduction standard permettant de se ramener à prouver l'absence de racines à des polynômes spécialisés $Q(t,Y)$. Cette réduction permettra d'utiliser le théorème 3.2 afin de borner les hauteurs des nombres t qui conviennent. Dans le cas où l'extension $E/K(T)$ définie par le polynôme $P(T,Y)$ est galoisienne, on peut concevoir (comme sur le cas $K = \mathbb{Q}$, voir [Wal05]) que la borne puisse être améliorée en une borne polynômiale en m, n et $log(H)$ qui sont le degré en T, le degré en Y et H le maximum entre la hauteur de P et e^e. Nous ne travaillerons ici que le cas général.

3.2.1 Réduction classique

On se ramène au cas où le polynôme $P(T,Y)$ est unitaire en Y. En effet, en écrivant

$$P(T,Y) = a_0(T)Y^n + a_1(T)Y^{n-1} \cdots + a_n(T),$$

on a

$$(a_0(T))^{n-1}P(T,Y) = (a_0(T)Y)^n + a_1(T)(a_0(T)Y)^{n-1} + \cdots + a_0(T)^{n-1}a_n(T).$$

On construit ainsi un polynôme $\mathcal{P}(T,Y)$ tel que

$$a_0(T)^{n-1}P(T,Y) = \mathcal{P}(T, a_0(T)Y)$$

ou encore

$$\mathcal{P}(T,Y) = a_0(T)^{n-1}P(T, Y/a_0(T)).$$

Ces égalités permettent d'écrire que pour les $t \in \mathcal{O}_K$ tels que $a_0(t) \neq 0$, $P(T,Y)$ est irréductible sur K si et seulement si $\mathcal{P}(T,Y)$ est irréductible sur K. On peut alors supposer le polynôme $P(T,Y)$ unitaire en Y en tenant compte que l'on a écarté les cas où $a_0(t) = 0$.

Considérons la décomposition du polynôme $P(T,Y)$ dans $\overline{K(T)}[Y]$:

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

et soit $D(T)$ le discriminant de P par rapport à Y. Pour les nombres complexes t tels que $D(t) \neq 0$, il existe un morphisme de spécialisation

$$\varphi_t : K[T, y_1, \cdots, y_n] \to \mathbb{C}$$

qui prolonge la spécialisation $T \to t$. Dans la suite nous considérerons les spécialisations $t \in \mathcal{O}_K$ qui vérifient la condition $D^\sigma(t) \neq 0$ pour tout $\sigma : K \to \overline{\mathbb{Q}}$, ce qui peut se résumer, en prenant en compte l'argument permettant de se ramener à un polynôme unitaire, à la condition

$$a_0(t) \prod_{\sigma:K\to\overline{\mathbb{Q}}} D^\sigma(t) \neq 0.$$

Pour $z \in K[T, y_1, \cdots, y_n]$, on note $z(t)$ l'image de z par le morphisme de spécialisation φ. Le polynôme spécialisé $P(t, Y)$ peut alors s'écrire :

$$P(t, Y) = \prod_{i=1}^{n} (Y - y_i(t)).$$

3.2.2 Estimations sur les polynômes P_ω

Les polynômes concernés par la réduction sont les polynômes $P_{w,j}$ construits ainsi : pour ω sous-ensemble de $\{1, \cdots, n\}$, et pour un entier positif $j \leq \#\omega$, $P_{w,j}(T, Y)$ est le polynôme minimal de $\tau_j(y_i : i \in \omega)$ sur $K(T)$, où τ_j désigne la j-ième fonction symétrique élémentaire. Les éléments y_i, $i = 1, \cdots, n$ étant entiers sur $\mathcal{O}_K[T]$ et $\mathcal{O}_K[T]$ étant intégralement clos, les polynômes $P_{w,j}$ sont unitaires et dans $\mathcal{O}_K[T, Y]$.

Lemme 3.4. *Soit $t \in \mathcal{O}_K$ tel que $P(t, Y)$ soit réductible sur $\mathbb{Q}$ et $D(t) \neq 0$. Alors il existe un sous ensemble $\omega \subset \{1, \cdots, n\}$ de cardinal $l \leq n/2$ et un $j \leq l$ tel que $P_{\omega,j}$ est irréductible dans $K[T, Y]$, $\deg_y(P_{\omega,j}) \geq 2$ et $P_{\omega,j}(t, Y)$ a un zéro dans $\mathcal{O}_K$. On notera P_ω ce polynôme.*

Démonstration. Le polynôme $P(t, Y)$ est réductible, on peut donc écrire

$$P(t, Y) = R(Y)S(Y)$$

où R et S sont des polynômes à coefficients dans $\mathbb{Q}$ avec $\deg(R) \leq \deg(S)$. Il existe alors un sous-ensemble ω de cardinal $l \leq n/2$ tel que

$$R(Y) = \prod_{i\in\omega} (Y - y_i(t)).$$

On peut aussi écrire le polynôme $P(T, Y)$ comme

$$P(T, Y) = \mathcal{R}(Y)\mathcal{S}(Y)$$

avec $\mathcal{R}(Y) = \prod_{i\in\omega}(Y - y_i) \in \overline{\mathbb{Q}(T)}[Y]$, de sorte que l'image par φ de $\mathcal{R}$ soit R.

$$P(T, Y) = \mathcal{R}(Y)\mathcal{S}(Y) \quad \xrightarrow{\varphi} \quad P(t, Y) = R(Y)S(Y)$$

Comme $P(T,Y)$ est irréductible, au moins un des coefficients de $\mathcal{R}(Y)$ est dans $\overline{K(T)}\backslash K(T)$. Ce coefficient, noté θ_ω, est du type $\tau_j(y_i : i \in \omega)$ pour un certain $j \leq l$. On sait de plus que comme $R(Y)$ est à coefficients dans K, alors $\theta_\omega(t) \in K$.

Le polynôme minimal de θ_ω : $P_{w,j}(T,Y)$ est de degré supérieur ou égal à 2 et le polynôme spécialisé $P_{w,j}(t,Y)$ étant unitaire, le zéro $\theta_\omega(t)$ de ce polynôme est en fait dans $\mathcal{O}_K$. □

Afin de rendre le théorème d'irréductibilité effectif, nous avons besoin :

— d'estimer le nombre de polynômes du type P_ω,
— d'estimer les degrés (total et en Y) des polynômes P_ω,
— d'estimer la hauteur des polynômes P_ω.

Pour obtenir ces estimations, on utilisera un outil classique d'effectivité : la mesure de Malher et les comparaisons entre la hauteur d'un polynôme et la mesure de Malher [HS00].

On note par $H_{\mathbb{C}}(P)$ la hauteur usuelle d'un polynôme à coefficients dans $\mathbb{C}$. C'est le maximum des modules des coefficients de P. Quant à la mesure de Malher, elle est définie pour un polynôme $P(X)$ à coefficients dans $\mathbb{C}$. On écrit $P(X) = a_d \prod_{i=1}^{d}(X - \alpha_i)$ et on définit la mesure de Malher par

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

Les comparaisons entre hauteur usuelle sur $\mathbb{C}$ et mesure de Malher sont données comme suit :

$$M(P) \leq \sqrt{1+d}\ H_{\mathbb{C}}(P) \quad \text{et} \quad \mathrm{H_{\mathbb{C}}(P)} \leq 2^{\mathrm{d}}\mathrm{M(P)}$$

où $|.|$ désigne le module complexe.

Le polynôme $P_\omega(T,Y)$ est le polynôme minimal de $\theta_\omega = \tau_j(y_i : i \in \omega)$ pour un certain $j \leq l$. Il divise donc le polynôme $\prod_{\#\omega=l} (Y - \tau_j(y_i : i \in \omega)) \in K[T,Y]$. On a par spécialisation pour $z \in \mathbb{C}$ tel que $D(z) \neq 0$:

— $\theta_\omega(z)$ est une fonction symétrique élémentaire en les $y_i(z)$, $(i = 1, ..., n)$.
— $P_\omega(z,Y)$ divise le polynôme $\prod_{\#\omega=l} (Y - \tau_j(y_i(z) : i \in \omega))$.

On a la proposition suivante :

Proposition 3.5. *Les polynômes P_ω donnés dans le lemme 3.4 ont les propriétés suivantes :*

— *leur nombre est majoré par 2^n,*
— *leur degré en Y (noté d_ω) est majoré par $\binom{n}{l}$,*
— *leur degré total est majoré par md_ω,*
— *leur hauteur $H(P_\omega)$ est majorée par $(2^{3n}(m+1)H(P))^{d_\omega}$.*

Démonstration.

— Le nombre de ces polynômes P_ω est le nombre de parties d'un ensemble $\{1, \cdots, n\}$ à l éléments. Il est donc inférieur à 2^n.

— Le polynôme $P_\omega(T, Y)$ divise le polynôme

$$\prod_{\#\omega=l} (Y - \tau_j(y_i : i \in \omega))$$

qui est de degré $\binom{n}{l}$. Le degré en Y de P_ω est donc inférieur ou égal à $\binom{n}{l}$.

— On écrit

$$P_\omega(T, Y) = \sum_{i=0}^{d_\omega} P_i(T) Y^{d_\omega - i}$$

avec $P_0(T) = 1$. Soit $t \in \mathbb{C}$ fixé avec $D(t) \neq 0$, disons $|t| \geq r \geq 1$ pour r suffisamment grand. Comme $P_\omega(T, Y)$ est irréductible dans $K[T, Y]$, les zéros de $P_\omega(T, Y)$ sont les conjugués θ_ω^τ de θ_ω ($\tau \in \mathrm{Gal}(\overline{K(T)}/K(T))$). Les éléments θ_ω^τ sont donc des fonctions symétriques d'un nombre l des y_i, $i = 1, \cdots, n$.

En écrivant

$$P_\omega(T, Y) = \prod_{\tau \in \mathrm{Gal}(\overline{K(T)}/K(T))} (Y - \theta_\omega^\tau),$$

on a

$$P_\omega(t, Y) = \prod_\tau (Y - \theta_\omega^\tau(t)).$$

Les zéros de $P_\omega(t, Y)$ sont donc les spécialisations en t des zéros de $P_\omega(T, Y)$, c'est à dire les spécialisations des θ_ω^τ. Ainsi, $\theta_\omega^\tau(t)$ est une fonction symétrique élémentaire d'un nombre l de $y_i(t)$, $i = 1, \cdots, n$. La j-ième fonction symétrique élémentaire ayant au plus 2^l termes, on peut majorer le module complexe $|\theta_\omega^\tau(t)|$:

$$\begin{aligned} |\theta_\omega^\tau(t)| &\leq 2^l \prod_{i=1}^{l} \max\{1, |y_i(t)|\} \\ &\leq 2^l \prod_{i=1}^{n} \max\{1, |y_i(t)|\} \\ &\leq 2^l M(P(t, Y)) \end{aligned}$$

En utilisant la majoration de la mesure de Malher par la hauteur complexe et le fait que pour $|t| \geq 1$, $H_\mathbb{C}(F(t, Y)) \leq (m+1) H_\mathbb{C}(F) |t|^m$, on obtient

$$\begin{aligned} |\theta_\omega^\tau(t)| &\leq 2^l \sqrt{n+1} H_\mathbb{C}(P(t, Y)) \\ &\leq 2^l \sqrt{n+1} (m+1) H_\mathbb{C}(P) |t|^m \end{aligned}$$

Comme $l \leq n/2$ alors

$$|\theta_\omega^\tau(t)| \leq 2^n (m+1) H_\mathbb{C}(P) |t|^m.$$

Cette majoration reste valable pour toutes les racines de $P_\omega(t,Y)$. De plus, $P_i(t)$ est, au signe près, la i-ième fonction symétrique élémentaire en les zéros de $P_\omega(t,Y)$. On a alors pour, $|t| \geq 1$, la majoration suivante :

$$\begin{aligned}|P_i(t)| &\leq 2^i(2^n(m+1)H_{\mathbb{C}}(P)|t|^m)^i \\ &\leq 2^{ni}(m+1)^i H_{\mathbb{C}}(P)^i|t|^{mi} = O(|t|^{mi})\end{aligned}$$

La croissance en t du polynôme P_i est en $O(t^{mi})$. Cela prouve que $\deg(P_i) \leq mi$ et donc

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

— On écrit encore $P_\omega(T,Y) = \sum_{i=0}^{d_\omega} P_i(T)Y^i$, $P_i(T) = \sum_j p_{i,j}T^j$.

Soit v une valuation archimédienne sur K. On peut écrire l'égalité $|.|_v = |.| \circ \sigma$ pour un $\sigma : K \to \overline{K}$ où $|.|$ désigne le module complexe de sorte que

$$|p_{ij}|_v = |p_{ij}^\sigma| \text{ et } H_{\mathbb{C}}(P^\sigma) = H_v(P).$$

Pour $z \in \mathbb{C}$, d'après les inégalités de Cauchy pour $r > 0$:

$$|p_{i,j}^\sigma| = |(P_i^\sigma)^{(j)}(0)/j!| \leq \sup_{|z|=r}|P_i^\sigma(z)|/r^j.$$

On choisit r égal à $1-\varepsilon > 0$ tel que pour tout $z \in \mathbb{C}$ avec $|z| = r$, $D^\sigma(z) \neq 0$ pour tout $\sigma : K \to \overline{\mathbb{Q}}$. Comme les $P_i^\sigma(z)$ désignent les coefficients de $P_\omega^\sigma(z,Y) \in \mathbb{C}[Y]$, on peut écrire la majoration

$$\max_{i,j}(|p_{ij}|_v) = H_v(P_\omega) \leq r^{-\deg_T P_\omega}\sup_{|z|=r} H_{\mathbb{C}}(P_\omega^\sigma(z,Y)) = r^{-\deg_T P_\omega}\max_{i=1,\cdots,d_\omega}|P_i^\sigma(z)|.$$

Le nombre ε peut être choisi aussi petit que l'on veut. On le choisit de sorte que $r^{-deg_T(P_\omega)} \leq 2$.

La majoration de la hauteur par la mesure de Malher permet d'écrire :

$$H_{\mathbb{C}}(P_\omega^\sigma(z,Y)) \leq 2^{d_\omega}M(P_\omega^\sigma(z,Y)) = 2^{d_\omega}\prod_{i=1}^{d\omega}\max\{1,|\alpha_{\sigma,i}(z)|\}$$

où les $\alpha_{\sigma,i}(z)$ sont les zéros de $P_\omega^\sigma(z,Y)$ dans $\mathbb{C}$.

Estimons maintenant les $|\alpha_{\sigma,i}(z)|$ pour $|z| = r$. On peut montrer, par le même raisonnement qu'avec les $\theta_\omega^\tau(t)$, que $\alpha_{\sigma,i}(z)$ est une fonction symétrique élémentaire en les zéros de $P^\sigma(z,Y)$. Remarquons tout de même que, dans ce cas, $\sigma : K \to \overline{K}$ alors que dans ce qui précédait, $\tau \in \mathrm{Gal}(\overline{K(T)}, K(T))$.

On prolonge $\sigma : K \to \overline{K}$ en $\sigma : \overline{K} \to \overline{K}$ de manière arbitraire, puis de façon naturelle à $\overline{K}((T^{1/e}))$ où e est l'indice de ramification au-dessus de zéro dans l'extension de $K(T)$ définie par les $y_1, ...y_n$. Par cette construction, on peut appliquer σ à $y_1, ..., y_n, \theta_\omega$. On note y_i^σ l'image de y_i par σ. On a alors

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

et par spécialisation, pour tout $z \in \mathbb{C}$ tel que $D^\sigma(z) \neq 0$,

$$P^\sigma(z, Y) = \prod_{i=1}^{n}(Y - y_i^\sigma(z)).$$

Les zéros de $P^\sigma(z, Y)$ sont donc les $y_i^\sigma(z)$ où les $y_i(z)$ sont les zéros de $P(z, Y)$ dans $\mathbb{C}$. On peut alors faire le même type de calcul que dans la majoration du degré des P_ω :

$$\begin{aligned}
|\alpha_{\sigma,i}(z)| &\leq \prod_{i=1}^{n} \max\{1, |y_i^\sigma(z)|\} \\
&\leq 2^l M(P^\sigma(z, Y)) \\
&\leq 2^l \sqrt{n+1} H_{\mathbb{C}}(P^\sigma(z, Y)) \\
&\leq 2^l \sqrt{n+1} \max_i\{|a_{\sigma,i}(z)|\}
\end{aligned}$$

où les $a_{\sigma,i}(z)$ sont les coefficients de $P^\sigma(z, Y)$ vus comme polynômes en Y. On a de plus les majorations $|a_{\sigma,i}(z)| \leq (m+1)H_{\mathbb{C}}(P^\sigma)\max\{1, |z|^m\}$, ce qui conduit à l'estimation

$$\begin{aligned}
|\alpha_{\sigma,i}(z)| &\leq 2^l \sqrt{n+1}(m+1)H_{\mathbb{C}}(P^\sigma) \\
&\leq 2^n(m+1)H_v(P).
\end{aligned}$$

Finalement, obtient la majoration

$$\begin{aligned}
H(P_\omega) &\leq \max_{v/\infty} H_v(P_\omega) \\
&\leq \max_{v/\infty} 2^{d_\omega}(2^n(m+1)H_v(P))^{d_\omega} \\
&\leq 2^{3nd_\omega}(m+1)^{d_\omega} \max_{v/\infty} H_v(P)^{d_\omega} \\
&\leq (2^{3n}(m+1)H(P))^{d_\omega}
\end{aligned}$$

□

3.2.3 Irréductibilité des polynômes spécialisés

On travaille maintenant avec un polynôme $P(T,Y)$ non nécessairement unitaire. On note $S(B)$ le nombre d'entiers algébriques $t \in \mathcal{O}_K$, $H(t) \leq B$ tels que $a_0(t) \prod_{\sigma:K\to\overline{\mathbb{Q}}} D^\sigma(t) \neq 0$ et $P(t,Y)$ soit réductible sur K et on suppose B suffisamment grand pour que les conditions du theorème 3.2 soient vérifiées.

Theorème 3.6. *Le nombre $S(B)$ vérifie*

$$S(B) \leq a_1 a_2^n m^{a_3} (\log H)^{a_4} B^{\rho/2} (\log B)^{a_5}.$$

Démonstration. Soit $S_\omega(B)$ le nombre d'entiers positifs $t \leq B$ tels que $a_0(t)D(t) \neq 0$ et tel que le polynôme spécialisé $P_\omega(t,Y)$ ait un zéro entier. D'après le lemme 3.4, on a l'inégalité

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

On estime alors le nombre $S(B)$ en estimant chacun des $S_\omega(B)$ grâce au théorème 3.2. Il existe des constantes a_1, a_2, a_3, a_4 dépendant uniquement du degré $[K:\mathbb{Q}]$ telles que pour B suffisamment grand :

$$\begin{aligned} S_\omega(B) &\leq a_1 \deg(P_\omega)^{a_2} \log^{a_3}(H(P_\omega)) B^{\rho/\deg_Y(P_\omega)} \log^{a_4} B \\ &\leq a_1 (m d_\omega)^{a_2} \log^{a_3}((2^{3n}(m+1)H(P))^{d_\omega}) B^{\rho/2} \log^{a_4} B \end{aligned}$$

avec $d_\omega \leq \binom{n}{l}$ pour un nombre $l \leq n/2$. Ce qui donne, pour d'autres toujours notées a_1, a_2, a_3, a_4, a_5 :

$$S_\omega(B) \leq a_1 a_2^n m^{a_3} \log^{a_4}(H) B^{\rho/2} \log^{a_5}(B).$$

En sachant que le nombre de polynômes du type P_ω étant majoré par 2^n et en prenant en compte le nombre de solutions de $a_0(t) \prod_{\sigma:K\to\overline{\mathbb{Q}}} D^\sigma(t) \neq 0$, ce qui ne change que la constante, on en déduit que le nombre de $t \in \mathcal{O}_K$, avec $H(t) \leq B$ tels que $P(t,Y)$ soit réductible sur K est plus petit que

$$a_1 a_2^n m^{a_3} (\log H)^{a_4} B^{\rho/2} (\log B)^{a_5}.$$

□

En utilisant cette réduction et les estimations associées, nous pouvons maintenant énoncer une version effective du théorème d'irréductibilité de Hilbert :

Theorème 3.7. *Pour B suffisamment grand dépendant de K, d, le nombre de $t \in \mathcal{O}_K$ tels que $P(t,Y)$ soit irréductible sur $\mathcal{O}_K$ est plus grand que $\frac{1}{2}B^\rho$.*

Démonstration. Soit N ce nombre. Il est égal à

$$\#\{t \in \mathcal{O}_K,\ H(t) \leq B\} - S(B).$$

Nous avons d'une part le résultat classique, voir [Sch79] :

$$\#\{t \in \mathcal{O}_K,\ H(t) \leq B\} \sim B^{\rho},$$

et d'autre part

$$S(B) \leq a_1 a_2^n m^{a_3} (logH)^{a_4} B^{\rho/2} (logB)^{a_5}.$$

L'équivalence en B de $S(B)$ est du type $B^{\rho/2}$, alors pour B suffisamment grand on a la conclusion voulue. □

CHAPITRE 4

Application des résultats obtenus

Les résultats obtenus dans les chapitres précédents sur la recherche de points rationnels et sur le théorème d'irréductibilité de Hilbert peuvent être utilisés dans le cadre de la conjecture de Malle.

Nous utiliserons ici les spécialisations d'une extension galoisienne régulière. On dira qu'une extension $F/K(T)$ est *K-régulière* (ou régulière s'il n'y a pas d'ambiguité) si

$$F \cap \overline{K} = K.$$

On dira que le groupe G est un groupe de Galois *régulier* sur K s'il existe une extension galoisienne régulière $F/K(T)$ de groupe G. Les exemples de groupes de Galois réguliers sur $\mathbb{Q}$ sont nombreux : S_n ($n \geq 1$) et beaucoup de groupes simples comme A_n ($n \geq 5$), des $PSL_2(\mathbb{F}_q)$, le Monstre, etc.

On rappelle que la conjecture de Malle traite du nombre $N(K, G, y)$ défini en 1.1.2 comme :

$$N(K, G, y) = \#\{E/K \text{ galoisienne } : Gal(E/K) = G, N_{K/\mathbb{Q}}(d_{E/K}) \leq y\}.$$

L'élément $d_{E/K}$ est un idéal de O_K et la norme $N_{K/\mathbb{Q}}(d_{E/K})$ est la norme que nous avons utilisé tout au long de cette thèse. Il s'agit d'un entier.

On s'intéresse ici à la partie minoration de la conjecture que l'on définira plus spécifiquement de la manière suivante :

Definition 4.1. On dit que l'on a une minoration du type Malle pour G sur K s'il existe $\alpha(G) > 0$, dépendant seulement de G, tel que

$$N(K, G, y) \geq c_1 y^{\alpha(G)} \text{ pour tout } y \geq y_0$$

pour des constantes positives c_1, y_0 dépendantes de K, G.

Remarquons qu'une minoration du type Malle fournit une réponse positive au problème inverse de Galois sur G. On démontrera ce résultat, valable pour tout groupe G :

Theorème 4.2. *Soit G un groupe fini. Il existe un corps de nombres K_0 tel que l'on a une minoration du type Malle pour G sur tout corps de nombres K contenant K_0. Plus précisément, le corps K_0 peut être choisi comme n'importe quel corps de nombres sur lequel G est régulier.*

L'exposant $\alpha(G)$ sera donné explicitement. Il est plus petit que la constante $a(G)$ annoncé par Malle dans sa conjecture [Mal04]. Nous expliquerons pourquoi dans 4.3, remarque 4.12.

Le théorème 4.2 généralise un résultat de Dèbes [Dèb17, theorem 1.1] qui a démontré qu'il existait une minoration du type Malle pour G sur $\mathbb{Q}$ et lorsque G est supposé régulier sur $\mathbb{Q}$.

Notre approche permet d'imposer des contraintes locales sur les extensions E/K que l'on compte. Ceci nous permet d'apporter également des résultats sur le problème de Grunwald énoncé en 1.1.3.

Pour exposer notre résultat sur ce sujet, on utilisera la terminologie suivante tirée de [Dèb17]. Si $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ est un problème de Grunwald sur K et M/K est une extension galoisienne finie, on note par S_M l'ensemble des idéaux premiers de M obtenus en choisissant un premier arbitraire $\mathcal{P}$ de M au dessus de chaque idéal premier $\mathfrak{p} \in S$. On note par $(G, (L^{\mathfrak{p}}M_{\mathcal{P}}/M_{\mathcal{P}})_{\mathcal{P}\in S_M})$ le problème de Grunwald sur M induit par *changement de base* $M_{\mathcal{P}}/K_{\mathfrak{p}}$, $\mathfrak{p} \in S$. Etant donné que l'extension M/K est galoisienne alors le problème induit par changement de base de dépend pas du choix de $\mathcal{P}$.

Remarquons ensuite que si l'extension M/K est totalement décomposée en chaque $\mathfrak{p} \in S$ alors $M_{\mathcal{P}} = K_{\mathfrak{p}}$ et $L^{\mathfrak{p}}M_{\mathcal{P}}/M_{\mathcal{P}} = L^{\mathfrak{p}}/K_{\mathfrak{p}}$ ($\mathfrak{p} \in S$). Dans ce cas, une solution E/M du problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S_M})$ induit par changement de base est appelé une *M-solution* du problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.

Le résultat de ce chapitre sur le problème de Grunwald est le suivant :

Theorème 4.3. *Soit G un groupe fini et K un corps de nombres.*

1. *Il existe un ensemble fini S_{exc} d'idéaux premiers de K avec la propriété suivante : si $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ est un problème de Grunwald sur K avec $S \cap S_{exc} = \emptyset$, alors il existe une extension galoisienne M/K, totalement décomposée en chaque $\mathfrak{p} \in S$ et une infinité de M-solutions E/M au problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.*
2. *De plus, on peut prendre $M = K$ si G est un groupe de Galois régulier sur K et le nombre de solutions E/K au problème de Grunwald qui vérifient $N_{K/\mathbb{Q}}(d_{E/K}) \leq y$ est plus grand que $c_1 y^{\alpha(G)}$ pour tout $y \geq y_0$ (où $\alpha(G)$ est le nombre qui apparait dans le théorème 4.2) et pour une constante strictement positive c_1, dépendant de K, G et y_0 dépendant de K, G, S.*

En particulier, pour tous les groupes non résolubles connus comme étant groupes de Galois réguliers sur $\mathbb{Q}$, tout problème de Grunwald a une infinité de solutions sur $\mathbb{Q}$.

Les théorèmes de la section 4.1 et la section 4.2 permettent d'établir les théorèmes 4.2 et 4.3 en démontrant un résultat intermédiaire combinant le comptage d'extensions et un ajout de contraintes locales.

Pour arriver à nos fins, nous démontrons, d'une manière différente que celle du chapitre 3, une version du théorème d'irréductibilité de Hilbert. Celle ci permettant des contraintes locales sur les extensions comptées. Les extensions désirées E/K seront obtenues par spécialisation d'une extension galoisienne régulière $F/K(T)$ de groupe de Galois G. A partir d'une extension $F/K(T)$ fixée, le théorème 4.4 produit explicitement beaucoup de spécialisations $t_0 \in \mathcal{O}_K$ de hauteur bornée telles que l'extension spécialisée F_{t_0}/K soit galoisienne et de groupe G. Le théorème 4.8 montre que le nombre d'extensions spécialisées F_{t_0}/K qui peuvent être isomorphes est restreint.

Le résumé de ce dernier chapitre, en association avec les résultats des chapitres précédents se présente comme suit. Les théorèmes 4.4 et 4.8 sont intermédiaires entre les énoncés purement diophanciens (théorème 2.10 et théorème 3.2) et les applications de ce chapitre (théorème 4.2 et théorème 4.3). Ces applications se donnent en 3 étapes. On établi d'abord dans les deux premieres sections les théorèmes 4.4 et 4.8. A partir de ceux-ci, on démontre ensuite le théorème 4.11. Ce dernier théorème est démontrer afin d'impliquer à la fois le théorème 4.2 et théorème 4.3. La figure suivante synthétise la démarche suivie.

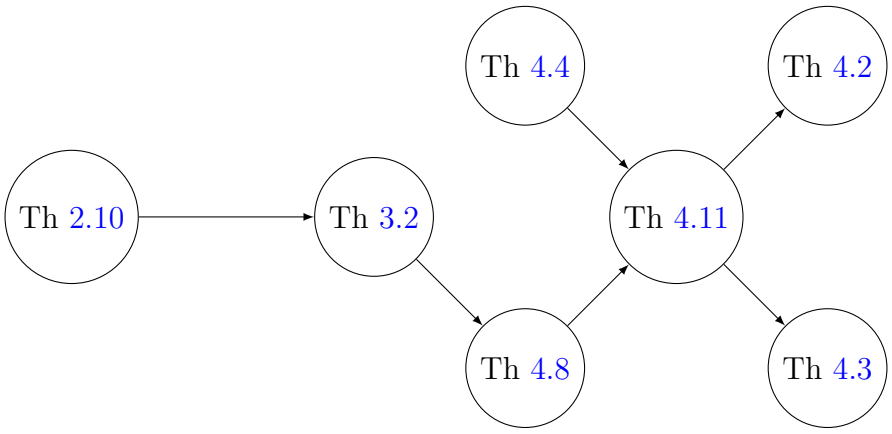


FIGURE 4.1 –

On se fixe les notations suivantes. Le corps de nombres fixé K est de degré $\rho = [K : \mathbb{Q}]$, le groupe fini G est K-régulier et on se donne une extension régulière galoisienne $F/K(T)$ de groupe G. On note r le nombre de points de branchement de $F/K(T)$. De manière équivalente, c'est aussi le nombre de points de branchement du K-revêtement associé $f : X \to \mathbb{P}^1$. Le genre de F (ou de X) est noté par g. Pour un idéal premier $\mathfrak{p}$ de K, le nombre premier en dessous de $\mathfrak{p}$ est $p_\mathfrak{p}$ et on a $\mathfrak{p} \cap \mathbb{Z} = p_\mathfrak{p}\mathbb{Z}$.

Etant donné un point $t_0 \in K$ (ou $t = \infty$), la spécialisation de $F/K(T)$ en t_0 est le corps

résiduel de la clôture intégrale de l'anneau localisé $K[T]_{\langle T-t_0\rangle}$ dans F en un idéal premier arbitraire au dessus de $\langle T-t_0\rangle$. On notera cette spécialisation F_{t_0}/K.

Soit $P(T,Y) \in \mathcal{O}_K[T,Y]$ le polynôme minimal d'un élément primitif de $F/K(T)$ entier sur $\mathcal{O}_K[T]$. Pour tout $t_0 \in K$ qui n'est pas dans l'ensemble fini des racines du discriminant de $P(T,Y)$ par rapport à Y, $\Delta_P(T)$, la spécialisation F_{t_0}/K est aussi le corps de décomposition de $P(t_0,Y) \in K[Y]$. On appelle un tel $P(T,Y)$ un *modèle affine* de $F/K(T)$.

Concernant les conditions locales que les extensions spécialisées doivent satisfaire, on utilise la notion de *donnée de Frobenius*. Etant donné un ensemble S d'idéaux premiers de $\mathcal{O}_K$, une donnée de Frobenius sur S est une collection $\mathcal{F}_S = (\mathcal{F}_\mathfrak{p})_{\mathfrak{p}\in S}$ de sous ensembles $\mathcal{F}_\mathfrak{p} \subset G$, où chaque $\mathcal{F}_\mathfrak{p}$ est une union non-vide de classes de conjugaison de G. L'ensemble S est dit *au dessus de l'intervalle* $[a,b]$ si S est l'ensemble de tous les idéaux premiers au dessus des nombres premiers $p \in [a,b]$. Notre prescription locale sur les spécialisations F_{t_0}/K consiste à demander que pour chaque $\mathfrak{p} \in S$, le Frobenius [1] $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K)$ est dans $\mathcal{F}_\mathfrak{p}$. Par exemple, si $\mathcal{F}_\mathfrak{p} = \{1\}$ pour tout $\mathfrak{p} \in S$, cela consiste à demander que F_{t_0}/K soit totalement décomposé en chaque $\mathfrak{p} \in S$.

4.1 Un théorème type Hilbert

On choisit
- Un nombre premier $p_{-1} \geq r^2g^2$ et tel que chaque nombre premier p qui est ramifié dans $K/\mathbb{Q}$ est $\leq p_{-1}$ et
- un nombre premier p_0 tel que l'intervalle $]p_{-1}, p_0[$ a au moins autant de nombres premiers qu'il y a de classes de conjugaison dans G.

Les premiers p_{-1} et p_0 dépendent de K, r, g et K, r, g, G respectivement. Pour $B > 1$, on définit S_B comme l'ensemble des idéaux premiers de K au dessus de l'intervalle $[p_0, \log(B)/2]$. Dans cette section, nous démontrons ce théorème :

Theorème 4.4 (*Type Hilbert*)**.** *Il existe un nombre $c > 0$ (dépendant de $F/K(T)$) tel que si B est suffisamment grand (dépendant de $F/K(T)$), si $\mathcal{F}_B = (\mathcal{F}_\mathfrak{p})_{\mathfrak{p}\in S_B}$ est une donnée de Frobenius sur S_B, le nombre de $t_0 \in \mathcal{O}_K$ vérifiant $H(t_0) \leq B$ et tels que*
- *l'extension spécialisée F_{t_0}/K est galoisienne de groupe G,*
- *pour chaque $\mathfrak{p} \in S_B$, F_{t_0}/K est non ramifié et $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K) \in \mathcal{F}_\mathfrak{p}$.*

$$\textit{est plus grand que } \frac{B^\rho}{c^{\log B/\log\log B}}.$$

La preuve de ce théorème se fait en plusieurs étapes. On dit qu'un idéal premier $\mathfrak{p}$ de K est *bon* pour $F/K(T)$ si $\mathfrak{p}$ ne divise pas $|G|$, le diviseur de branchement $\mathfrak{t} = \{t_1, \cdots, t_r\}$ [2] est étale en $\mathfrak{p}$ et s'il n'y a pas de ramification verticale en $\mathfrak{p}$. On dit que $\mathfrak{p}$ est *mauvais* sinon. La notion de diviseur de branchement est une notion complexe et fait part de nombreuses

1. Pour la définition du Frobenius, voir 1.3.6
2. Formellement, $\mathfrak{t}$ serait vu comme le diviseur $t_1 + \cdots + t_r$

recherches. Certains s'intéressent plus en profondeurs à ces propriétés (voir [DG12, §4] et [Leg16]). Une définition simple est claire est donnée dans [Leg16, Definition 2.6]. Ici, on utilisera le fait qu'il n'existe qu'un nombre fini de mauvais premiers.

Soient $\mathfrak{p}$ un bon premier pour $F/K(T)$ et $\mathcal{F}_\mathfrak{p}$ une union de classe de conjugaison de G, associée à $\mathfrak{p}$. Le résultat suivant généralise [Dèb17, proposition 5.1], prouvé dans le cas $K = \mathbb{Q}$.

Proposition 4.5. *l'ensemble*

$$\tau(\mathcal{F}_\mathfrak{p}) = \{t_0 \in \mathcal{O}_K \mid \ t_0 \notin \mathbf{t} \mod \mathfrak{p}, \ \ \mathrm{Frob}_\mathfrak{p}(F_{t_0}/K) \in \mathcal{F}_\mathfrak{p}\}$$

est une union de classes d'équivalences modulo $\mathfrak{p}$ *et le nombre* $\nu(\mathcal{F}_\mathfrak{p})$ *de ces classes d'équivalences satisfait*

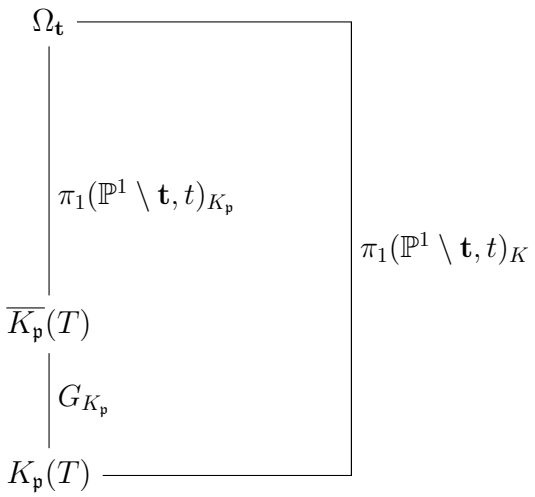
$$\nu(\mathcal{F}_\mathfrak{p}) \geq \frac{|\mathcal{F}_\mathfrak{p}|}{|G|} \times (q + 1 - 2g\sqrt{q} - |G|(r+1))$$
$$\nu(\mathcal{F}_\mathfrak{p}) \leq \frac{|\mathcal{F}_\mathfrak{p}|}{|G|} \times (q + 1 + 2g\sqrt{q})$$

où $q = N_{K/\mathbb{Q}}(\mathfrak{p})$.

Démonstration. La preuve reprend celle de [Dèb17, proposition 5.1]. On utilise sans distinction l'extension régulière $F/K(T)$ et le K-revêtement associé $f : X \to \mathbb{P}^1$.

On peut supposer que $\mathcal{F}_\mathfrak{p}$ consiste en une seule classe de conjugaison. On note par $K_\mathfrak{p}$ la complétion de K en la place $\mathfrak{p}$-adique $v_\mathfrak{p}$ et par $K_\mathfrak{p}^{ur}$ l'extension maximale non ramifiée de $K_\mathfrak{p}$. L'extension $K_\mathfrak{p}^{ur}/K_\mathfrak{p}$ est cyclique engendrée par le Frobenius de $K_\mathfrak{p}$. Elle correspond à la clôture algébrique $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$. Par correspondance, toute extension finie E non ramifiée de $K_\mathfrak{p}$ correspond à une extension finie cyclique E' de $\mathbb{F}_q$.

Soit $f_\mathfrak{p} = f \otimes_K K_\mathfrak{p}$. On note $\phi_\mathfrak{p} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{K_\mathfrak{p}} \to G$ la représentation du groupe fondamental de $f_\mathfrak{p}$. On note $\Omega_\mathbf{t}$ l'extension maximale non ramifiée au dessus de $\mathbf{t}$. Le diagramme suivant résume la situation



et la théorie de Galois fournit la suite exacte scindée

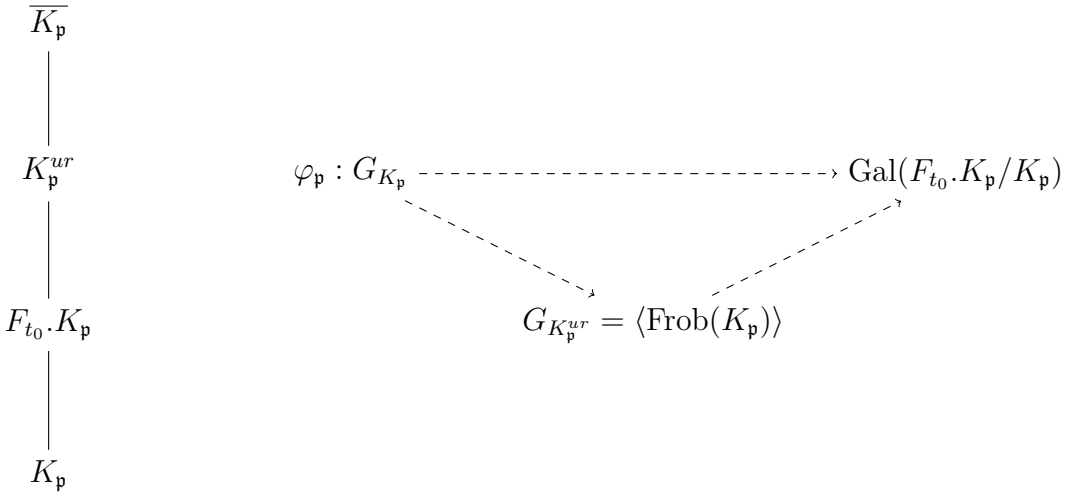
$$1 \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{K_\mathfrak{p}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to G_{K_\mathfrak{p}} \to 1$$

Soit $g_\mathfrak{p} \in \mathcal{F}_\mathfrak{p}$ et considérons l'unique épimorphisme (continu) $\mathrm{Gal}(K_\mathfrak{p}^{ur}/K_\mathfrak{p}) \to \langle g_\mathfrak{p} \rangle$ envoyant le Frobenius de $K_\mathfrak{p}$ sur $g_\mathfrak{p}$. Composé avec le morphisme $G_{K_\mathfrak{p}} \to \mathrm{Gal}(K_\mathfrak{p}^{ur}/K_\mathfrak{p})$, il fournit un épimorphisme (continu)

$$\varphi_\mathfrak{p} : G_{K_\mathfrak{p}} \to \langle g_\mathfrak{p} \rangle$$

qui correspond à une extension non ramifiée de $K_\mathfrak{p}$.

On considère $t_0 \in \mathcal{O}_K$ tel que $t_0 \notin \mathbf{t} \mod \mathfrak{p}$. D'après des résultats classiques dus à Grothendieck-Beckmann (on utilise la forme donnée dans [Leg16]), $\mathfrak{p}$ est non ramifié dans F_{t_0}/K et $F_{t_0}.K_\mathfrak{p} \subset K_\mathfrak{p}^{ur}$ où $K_\mathfrak{p}^{ur}$ est l'extension maximale non ramifiée de $K_\mathfrak{p}$. Nous avons donc les deux diagrammes suivants



Soit $s_{t_0} : G_{K_\mathfrak{p}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{K_\mathfrak{p}}$ la section canonique associée au $K_\mathfrak{p}$-point rationnel t_0. On a $t_0 \in \tau(\mathcal{F}_\mathfrak{p})$ si et seulement si la représentation galoisienne $\phi_\mathfrak{p} \circ s_{t_0} : G_{K_\mathfrak{p}} \to G$ de l'extension spécialisée $F_{t_0}.K_\mathfrak{p}/K_\mathfrak{p}$ est conjuguée dans G à $\varphi_\mathfrak{p}$.

On considère le revêtement tordu [3] $\widetilde{f_\mathfrak{p}}^{\varphi_\mathfrak{p}} : \widetilde{X_\mathfrak{p}}^{\varphi_\mathfrak{p}} \to \mathbb{P}^1$ obtenu en tordant $f_\mathfrak{p}$ par $\varphi_\mathfrak{p}$. D'après le twisting lemma [Dèb17, lemme 2.1], la seconde condition dans l'équivalence précédente est équivalente à l'existence d'un point $K_\mathfrak{p}$-rationnel au dessus de t_0 sur $\widetilde{X_\mathfrak{p}}^{\varphi_\mathfrak{p}}$. Comme $\mathfrak{p}$ est bon pour $F/K(T)$, le revêtement $\widetilde{f_\mathfrak{p}}^{\varphi_\mathfrak{p}}$ a une bonne réduction. On note par $\overline{g} : \overline{Y} \to \mathbb{P}^1_{\mathbb{F}_q}$ la fibre spéciale. En utilisant le lemme de Hensel, on obtient finalement

$$t_0 \in \tau(\mathcal{F}_\mathfrak{p}) \Leftrightarrow \exists \overline{x} \in \overline{Y}(\mathbb{F}_q) \text{ tel que } \overline{g}(\overline{x}) = \overline{t_0}.$$

D'après les inégalités de Lang-Weil, le nombre k de points $\mathbb{F}_q$-rationnels sur $\mathbb{P}^1(\mathbb{F}_q)$ vérifie

$$k \geq q + 1 - 2g\sqrt{q}.$$

Rappelons que, par [DG12], le nombre de points $\mathbb{F}_q$-rationnels $\overline{x} \in \widetilde{X_\mathfrak{p}}(\mathbb{F}_q)$ au dessus de $\overline{t_0}$ est $\mathrm{Cen}_G(g_\mathfrak{p})| = |G|/|\mathcal{F}_\mathfrak{p}|$, ce nombre est le même que le nombre de $\omega \in G$ tels que $\phi \circ s_{t_0} = \omega\varphi_\mathfrak{p}\omega^{-1}$. En prenant en compte les points rationnels qui peuvent apparaitre au dessus d'un point de branchement ou au dessus de ∞, on obtient la première inégalité. La seconde partie des inégalités de Lang-Weil fournissent la deuxième estimation. □

Soit $x > 0$ un nombre réel. Soient $S_{[p_0,x]}$ l'ensemble des tous les idéaux premiers de K au dessus de l'intervalle $[p_0, x]$ et $\mathcal{F}_{[p_0,x]}$ une donnée de Frobenius sur $S_{[p_0,x]}$. Ensuite, avec l'ensemble $S_{]p_{-1},p_0[}$ défini comme l'ensemble des idéaux premiers au dessus de l'intervalle $]p_{-1}, p_0[$, on définit $S_x = S_{[p_0,x]} \cup S_{]p_{-1},p_0[}$.

On définit également la donnée de Frobenius $\mathcal{F}_x$ sur S_x en ajoutant à la donnée de Frobenius $\mathcal{F}_{[p_0,x]}$ des conditions locales sur les premiers de K au dessus de l'intervalle $]p_{-1}, p_0[$ de cette manière : à chaque classe de conjugaison de G, on associe un idéal premier $\mathfrak{p} \in S_{]p_{-1},p_0[}$ de sorte que chaque classe de conjugaison de G apparait dans la donnée de Frobenius ; pour les autres idéaux premiers dans $S_{]p_{-1},p_0[}$, on prend $\mathcal{F}_\mathfrak{p} = G$ ($\mathcal{F}_\mathfrak{p}$ peut être choisi arbitrairement). Soit $I = \prod_{\mathfrak{p} \in S_x} \mathfrak{p}$ et $\{p_1, \cdots, p_n\}$ l'ensemble des nombres premiers dans l'intervalle $]p_{-1}, x]$.

Lemme 4.6. *On a* $I = \prod_{1 \leq i \leq n} (p_i\mathcal{O}_K)$ *et* $I \cap \mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}$.

Démonstration. L'ensemble S_x est l'ensemble de tous les idéaux premiers de K au-dessus de $p_1, \cdots, p_n$. Or, chacun de ces idéaux premiers sont non ramifiés dans K d'après la définition de p_{-1}, on obtient alors

$$I = \prod_{\mathfrak{p}/p_1} \mathfrak{p} \cdots \prod_{\mathfrak{p}/p_n} \mathfrak{p} = (p_1\mathcal{O}_K) \cdots (p_n\mathcal{O}_K).$$

3. voir [Dèb17, §2.1] et [DG12] pour le revêtement tordu et le twisting lemma

Pour $i \in \{1, \cdots, n\}$, on a $p_i\mathcal{O}_K \cap \mathbb{Z} = p_i\mathbb{Z}$. L'argument suivant montre que

$$(p_1\mathcal{O}_K) \cdots (p_n\mathcal{O}_K) \cap \mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

L'inclusion $\supset$ est évidente : $p_1 \dots p_n \in (p_1\mathcal{O}_K) \dots (p_n\mathcal{O}_K) \cap \mathbb{Z}$. comme $\mathbb{Z}$ est un anneau principal, l'idéal $(p_1\mathcal{O}_K) \dots (p_n\mathcal{O}_K) \cap \mathbb{Z}$ is de la forme $a\mathbb{Z}$ pour un $a \in \mathbb{Z}$.

Or $(p_1\mathcal{O}_K) \dots (p_n\mathcal{O}_K) \cap \mathbb{Z} \subset p_i\mathcal{O}_K \cap \mathbb{Z}$. On en déduit que $p_i \mid a$, $i = 1, \cdots, n$ et comme $p_1, \cdots, p_n$ sont distincts, $p_1 \dots p_n \mid a$ d'où l'égalité voulue. □

L'intersection $\bigcap_{\mathfrak{p} \in S_x} \tau(\mathcal{F}_\mathfrak{p})$ est notée $\tau(S_x, \mathcal{F}_x)$. Par le théorème des restes chinois, $\tau(S_x, \mathcal{F}_x)$ contient $\mathcal{N}(S_x, \mathcal{F}_x) = \prod_{\mathfrak{p} \in S_x} \nu(\mathcal{F}_\mathfrak{p})$ classes d'équivalences modulo I. La proposition suivante est une forme plus précise et plus technique du théorème 4.4. On utilisera les notations suivante.

- pour une donnée de Frobenius $\mathcal{F}_S = (\mathcal{F}_\mathfrak{p})_{\mathfrak{p} \in S}$, la densité de $\mathcal{F}_S$, notée $\chi(\mathcal{F}_S)$, est le produit de tous les $|\mathcal{F}_\mathfrak{p}|/|G|$ pour $\mathfrak{p} \in S$,
- pour un réel positif, x, le nombre $\pi(x)$ est le nombre de nombres premiers $\leq x$ et $\Pi(x)$ est le produit de tous les premiers $p \leq x$. On a $\pi(x) \sim x/\log x$ and $\log(\Pi(x)) \sim x$ lorsque $x \to +\infty$.
- pour un ensemble S d'idéaux premiers de K, le nombre $\Pi(S)$ est le produit de tous les nombres premiers p tels que $p = p_\mathfrak{p}$ pour un des idéaux $\mathfrak{p} \in S$.

Proposition 4.7. *1. Si $t_0 \in \mathcal{O}_K$ est un représentant d'une des classes d'équivalence modulo I dans $\tau(S_x, \mathcal{F}_x)$ alors $\mathrm{Gal}(F_{t_0}/K) = G$ et $t_0 \in \tau(\mathcal{F}_\mathfrak{p})$ pour chaque $\mathfrak{p} \in S_x$.*

2. Si x est suffisamment grand,

$$\mathcal{N}(S_x, \mathcal{F}_x) \geq \chi(\mathcal{F}_x) \times \frac{\Pi(x)^\rho}{(\Pi(p_{-1}))^\rho} \times \left(\frac{1}{2r|G|}\right)^{\rho\pi(x)}.$$

3. Fixons une $\mathbb{Z}$-base $\underline{e} = (e_1, \cdots, e_n)$ de $\mathcal{O}_K$ et notons $H(\underline{e})$ la hauteur de $\underline{e}$. Pour chaque classe d'équivalence modulo I dans $\tau(S_x, \mathcal{F}_x)$, il existe un représentant $t_0 \in \mathcal{O}_K$ de hauteur $H(t_0) \leq \dfrac{\rho H(\underline{e})}{\Pi(p_{-1})}\Pi(x)$.

Démonstration. 1. D'après la définition de $\tau(S_x, \mathcal{F}_x)$, on a $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K) \in \mathcal{F}_\mathfrak{p}$ pour chaque $\mathfrak{p} \in S_x$. Par la condition de Frobenius sur les premiers de $S_{]p_{-1}, p_0[} \subset S_x$, le sous-groupe $\mathrm{Gal}(F_{t_0}/K) \subset G$ rencontre toutes les classes de conjugaison de G, donc c'est le groupe G en entier d'après un lemme de Jordan [Jor72].

2. En utilisant la proposition 4.5, on a, pour $q = N(\mathfrak{p})$ avec $\mathfrak{p} \in S_x$.

$$\begin{aligned}
\mathcal{N}(S_x, \mathcal{F}_x) &= \prod_{\mathfrak{p} \in S_x} \nu(\mathcal{F}_\mathfrak{p}) \\
&\geq \prod_{\mathfrak{p} \in S_x} \frac{|\mathcal{F}_\mathfrak{p}|}{|G|} \times (q + 1 - 2g\sqrt{q} - |G|(r+1)) \\
&\geq \chi(\mathcal{F}_x) \times \prod_{\mathfrak{p} \in S_x} q \times \prod_{\mathfrak{p} \in S_x} \left(1 + \frac{1}{q} - \frac{2g}{\sqrt{q}} - \frac{(r+1)|G|}{q}\right)
\end{aligned}$$

Comme dans [Dèb17], en utilisant que $g < r|G|/2-1$ (si $|G| > 1$; par la formule de Riemann-Hurwitz) et que $q \geq r^2|G|^2$ pour chaque $\mathfrak{p} \in S_x$ (par le choix de p_{-1}), on a

$$1 + \frac{1}{q} - \frac{2g}{\sqrt{q}} - \frac{(r+1)|G|}{q} \geq \frac{1}{2r|G|}.$$

Comme tous les idéaux premiers de S_x sont non ramifiés, on a

$$\prod_{\mathfrak{p} \in S_x} N(\mathfrak{p}) = \Pi(S_x)^\rho = \left(\frac{\Pi(x)}{\Pi(p_{-1})}\right)^\rho$$

et $\mathrm{card}(S_x) \leq \rho\pi(x)$. Ainsi, on obtient

$$\mathcal{N}(S_x, \mathcal{F}_x) \geq \chi(\mathcal{F}_x) \times \frac{(\Pi(x))^\rho}{(\Pi(p_{-1}))^\rho} \times \left(\frac{1}{2r|G|}\right)^{\rho\pi(x)}.$$

3. On a $\mathcal{O}_K = \{\sum_{i=1}^{\rho} m_i.e_i \quad | \quad m_i \in \mathbb{Z} \quad i = 1, \cdots, \rho\}$ et donc

$$\mathcal{O}_K/I = \{\sum_{i=1}^{\rho} \overline{m_i}.\overline{e_i} \mid \overline{m_i} \in \mathbb{Z}/\mathbb{Z} \cap I \quad i = 1, \cdots, \rho\}.$$

D'après le lemme 4.6, $\mathbb{Z}/\mathbb{Z} \cap I = \mathbb{Z}/\Pi(S_x)\mathbb{Z}$. Chaque classe d'équivalence modulo I dans $\tau(S_x, \mathcal{F}_x)$ a un représentant $t = \sum_{i=1}^{\rho} m_i.e_i$ dans $\mathcal{O}_K$ tel que $1 \leq m_i \leq \Pi(S_x)$, $i = 1, \cdots, \rho$. On a alors pour chaque place archimédienne v,

$$|t|_v = \left|\sum_{i=1}^{\rho} m_i.e_i\right| \leq \rho\Pi(S_x) \max_{1 \leq i \leq \rho}(|e_1|_v, \cdots, |e_\rho|_v).$$

Ainsi, $H(t) \leq \rho\Pi(S_x)H(e_1, \cdots, e_\rho) = \dfrac{\rho H(\underline{e})}{\Pi(p_{-1})}\Pi(x)$. □

Preuve du théorème 4.4. Pour un nombre positif B, on définit $x = p_B$ comme le plus grand nombre premier vérifiant $\Pi(p_B).p_B \leq B$ et q_B est le nombre premier suivant. Comme $\Pi(q_B) = \Pi(p_B).q_B$, on a

$$p_B\Pi(p_B) \leq B < q_B^2\Pi(p_B) \leq 4p_B^2\Pi(p_B);$$

la dernière inégalité utilise le résultat classique $q_B \leq 2p_B$.

En prenant le logarithme de ces termes, on obtient

$$\frac{\log(\Pi(p_B))}{p_B} + \frac{\log p_B}{p_B} \leq \frac{\log B}{p_B} \leq \frac{\log(\Pi(p_B))}{p_B} + \frac{2\log 2p_B}{p_B}$$

ce qui montre que

$$p_B \sim \log B \quad \text{lorsque } B \to \infty.$$

Fixons maintenant un nombre positif B qui satisfait les conditions suivantes :
— $\frac{\log B}{2} \leq p_B \leq 2\log B$,
— $p_B \geq \dfrac{\rho H(\underline{e})}{\Pi(p_{-1})}$,
— $\pi(p_B) \leq 2\log B/\log\log B$,
— p_B est assez grand pour que le proposition 4.7 puisse être appliquée avec $x = p_B$.
Il suffit de prendre B suffisamment grand, dépendant de K, $H(\underline{e})$, $\Pi(p_{-1})$.

Comme dans le théorème 4.4, soit S_B l'ensemble des idéaux premiers de K au-dessus de l'intervalle $[p_0, \dfrac{\log B}{2}]$. L'intervalle $[p_0, \log B/2]$ est contenu dans l'intervalle $[p_0, p_B]$ de la proposition 4.7. Soit $\mathcal{F}_B$ une donnée de Frobenius sur S_B. On l'étend à une donnée de Frobenius $\mathcal{F}_x = \mathcal{F}_{p_B}$ sur l'ensemble $S_x = S_{p_B}$ des premiers au-dessus de l'intervalle $[p_{-1}, p_B]$ (en définissant $\mathcal{F}_\mathfrak{p}$ de manière arbitraire sur chaque $\mathfrak{p}$ au dessus d'un nombre premier dans $[\log B/2, p_B]$).

Ensuite, on utilise la proposition 4.7 avec $x = p_B$, l'ensemble S_{p_B} et la donnée de Frobenius $\mathcal{F}_{p_B}$. Remarquons que la majoration pour $H(t_0)$ dans la proposition 4.7 (3) peut être remplacée par $H(t_0) \leq p_B\Pi(p_B)$ et donc aussi par $H(t_0) \leq B$. Par la proposition 4.7 (2), le nombre $\mathcal{N}$ de $t_0 \in \mathcal{O}_K$ tels que $\mathrm{Gal}(F_{t_0}/K) = G$, $H(t_0) \leq B$ et pour tout $\mathfrak{p} \in S_B$, $\mathrm{Frob}_\mathfrak{p}(\mathrm{F_{t_0}/K}) \in \mathcal{F}_\mathfrak{p}$ vérifie

$$\mathcal{N} \geq \chi(\mathcal{F}_{p_B}) \times \frac{\Pi(p_B)^\rho}{(\Pi(p_{-1}))^\rho} \times \left(\frac{1}{2r|G|}\right)^{\rho\pi(p_B)}.$$

De plus, on a

$$\chi(\mathcal{F}_{p_B}) = \prod_{\mathfrak{p}\in S_{p_B}} \frac{|\mathcal{F}_\mathfrak{p}|}{|G|} \geq \frac{1}{|G|^{|S_{p_B}|}} \geq \frac{1}{|G|^{\rho\pi(p_B)}}.$$

et
— $\Pi(p_B)^\rho = \dfrac{(4p_B^2\Pi(p_B))^\rho}{(2p_B)^{2\rho}} \geq \dfrac{B^\rho}{(2p_B)^{2\rho}}$,
— $(2p_B)^{2\rho} \leq c_1^{\log B/\log\log B}$ pour une constante c_1 dépendant de $F/K(T)$.
Finalement, en utilisant que $\pi(p_B) \leq 2\rho\log B/\log\log B$, on obtient

$$\mathcal{N} \geq \frac{B^\rho}{c^{\log B/\log\log B}}$$

pour une constante c dépendant de $F/K(T)$. □

4.2 Un théorème type Hilbert-Malle

Pour la conjecture de Malle, on doit, non pas seulement compter les bonnes spécialisations t_0, mais aussi compter le nombre d'extensions différentes correspondantes F_{t_0}/K. C'est le but de cette section et du théorème 4.8. Le cas particulier $K = \mathbb{Q}$ a été prouvé par Pierre Dèbes dans [Dèb17], on le généralise à un corps de nombres arbitraire :

Theorème 4.8 (*type Hilbert-Malle*). *Soit $B > 1$ un nombre réel. Soit $\mathcal{H} \subset \mathcal{O}_K$ un sous ensemble qui composé de t_0 tels que $\mathrm{Gal}(F_{t_0}/K) = G$ and $H(t_0) \leq B$. On note par $\mathcal{N}(B, \mathcal{H})$ le nombre d'extensions spécialisées correspondantes F_{t_0}/K lorsque $t_0 \in \mathcal{H}$. Il existe $E, \gamma \geq 0$ dépendants de $F/K(T)$ tels que si B est suffisamment grand (dépendant de $F/K(T)$), on a*

$$\mathcal{N}(B, \mathcal{H}) \geq \frac{|\mathcal{H}| - E}{B^{[K:\mathbb{Q}]/|G|}(\log B)^{\gamma}}.$$

La preuve combine les résultats diophantiens du chapitre 3 avec le résultat suivant :

Theorème 4.9. *Soit $F/K(T)$ une extension galoisienne régulière de groupe G. Il existe un entier $N \leq |Aut(G)|$ et des polynômes $\widetilde{P}_1, \cdots, \widetilde{P}_N \in \mathcal{O}_K[U, T, Y]$, irréductibles dans $\overline{K(U)}(T)[Y]$, de degré $\deg_Y(\widetilde{P}_i) = |G|$, unitaires en Y et un ensemble fini $\varepsilon \subset K$ tels que les assertions suivantes soient vraies :*

- *toutes les courbes affines $\widetilde{P}_i(U, t, y) = 0$ (sur $\overline{K(U)}$) sont de même genre g_F,*
- *pour chaque $u_0 \in \mathcal{O}_K \backslash \varepsilon$, $\widetilde{P}_i(u_0, T, Y)$ est irréductible dans $\overline{K}(T)[Y]$ et la courbe affine $\widetilde{P}_i(u_0, t, y)$ est de genre g_F, $i = 1, \cdots, N$,*
- *pour chaque $t_0 \in \mathcal{O}_K$ qui n'est pas un point de branchement de $F/K(T)$,*

$$F_{t_0}/K = F_{u_0}/K \iff \exists i \in \{1, \cdots, N\}, \exists y_0 \in K : \widetilde{P}_i(u_0, t_0, y_0) = 0.$$

Ce résultat est le cas particulier de [Dèb18, theorem 2.16] pour lequel $F/K(T) = L/K(T)$. Chaque polynôme $\widetilde{P}_i$ est un modèle affine du $K(U)$-revêtement régulier $\widetilde{f}_i : \widetilde{X}_i \to \mathbb{P}^1_{K(U)}$ du théorème et qui est obtenu en tordant f_i avec lui même ($i = 1, \cdots, N$). A part pour un nombre fini, les K-points sur $\widetilde{X}_i|_{u_0}$ qui apparaissent dans [Dèb18] correspondent aux zéros (t_0, y_0) du polynôme $\widetilde{P}_i(u_0, T, Y)$, $i = 1, \cdots N$. L'existence de l'entier $N \leq |Aut(G)|$ apparait dans la preuve du théorème [Dèb18, theorem 2.16].

Estimations diophantiennes. Les constantes c_i ci dessous, $i = 1, 2, 3$ ne dependent que de l'extension $F/K(T)$. On a pour $u_o \in \mathcal{O}_K$ tel que $H(u_0) \leq B$ et pour $i = 1, \cdots, n$:

- $\deg(\widetilde{P}_i(u_0, T, Y)) \leq \deg(\widetilde{P}) = c_1$
- $\deg_Y(\widetilde{P}_i(u_0, T, Y)) = \deg_Y(\widetilde{P}) = |G|$
- $H(\widetilde{P}_i(u_0, T, Y)) \leq c_2 H(u_0)^{c_3} \leq c_2 B^{c_3}$

Pour des nombres réels $g, D, H, B \geq 0$ et $d_Y \geq 2$, on considère tous les polynômes $Q(T, Y) \in \mathcal{O}_K[T, Y]$ unitaires en Y et irréductibles dans $\overline{K}(T)[Y]$ tels que

- $\deg_Y(Q) = d_Y$
- $\deg(Q) \leq D$
- $H(Q) \leq H$
- la courbe $Q(t, y) = 0$ est de genre $\leq g$.

Pour chaque polynômes $Q(T, Y)$, le nombre de $t \in \mathcal{O}_K$ de hauteur $H(t) \leq B$ et tels que $Q(t, y) = 0$ pour un certain $y \in \mathcal{O}_K$ est un nombre fini. On note par $Z(g, D, d_Y, H, B)$ le cardinal maximal de tous ces ensembles finis lorsque $Q(T, Y)$ parcours tous les polynômes satisfaisant les conditions précédentes.

Comme dans le théorème 4.8, soit $B > 1$ et $\mathcal{H} \subset \mathcal{O}_K$ un sous ensemble composé de t_0 tels que $\mathrm{Gal}(F_{t_0}/K) = G$ et $H(t_0) \leq B$. D'après le théorème 4.9, pour chaque $u_0 \in \mathcal{H}$, le nombre de $t_0 \in \mathcal{H}$ tels que $F_{t_0}/K = F_{u_0}/K$ est $\leq N\, Z(g_F, c_1, |G|, c_2 B^{c_3}, B)$.

Soit E le cardinal de ε du théorème 4.9, on obtient

$$\mathcal{N}(B, \mathcal{H}) \geq \frac{|\mathcal{H}| - E}{N Z(g_F, c_1, |G|, c_2 B^{c_3}, B)}.$$

D'après le théorème 3.2, on a

$$Z(g_F, c_1, |G|, c_2 B^{c_3}, B) \leq c_5 B^{\rho/|G|} (\log B)^{c_6}.$$

Finalement,

$$\mathcal{N}(B, \mathcal{H}) \geq \frac{|\mathcal{H}| - E}{B^{\rho/|G|} (\log B)^{\gamma}}.$$

4.3 Applications à la conjecture de Malle

4.3.1 Cas galoisien

Cette section aboutit à la démonstration du théorème 4.2. On travaille toujours avec un corps K et un groupe G régulier sur K. On se fixe l'extension régulière $F/K(T)$ et un modèle affine $P(T, Y) \in \mathcal{O}_K[T, Y]$ de $F/K(T)$; remarquons que $P(T, Y)$ est unitaire en Y. Si $\Delta_P(T)$ est le discriminant de P relativement à Y, on note $\delta_P = \deg(\Delta_P(T))$ et on se fixe enfin $\delta > \delta_P$. Comme dans [Dèb17, §4], on peut par exemple prendre $\delta = 3r|G|^4 \log(|G|)$ mais les théorèmes démontrés seront valides pour tout $\delta > \delta_P$.

Les théorèmes 4.2 et 4.3 seront présentés comme conséquence du théorème 4.11, présenté dans cette section, qui associe le comptage d'extensions spécialisées avec des contraintes locales. Le théorème 4.2 est une conséquence directe du théorème 4.11. Un peu de travail sera à faire pour démontrer le théorème 4.3.

Etant donné un ensemble fini S d'idéaux premiers de K et une donnée de Frobenius $\mathcal{F}$ sur S, soit $N(F/K(T), y, \mathcal{F})$ le nombre d'extensions galoisiennes distinctes F_{t_0}/K de groupe G obtenues par spécialisation de $F/K(T)$ en un $t_0 \in K$, dont la norme du discriminant vérifie $|N_{K/\mathbb{Q}}(d_{F_{t_0}/K})| \leq y$ et telles que pour tout $\mathfrak{p} \in S$, F_{t_0}/K est non ramifiée en $\mathfrak{p}$ et $\mathrm{Frob}_{\mathfrak{p}}(F_{t_0}/K) \in \mathcal{F}_{\mathfrak{p}}$.

Le théorème 4.4 produit beaucoup de bonnes spécialisations t_0 dont la hauteur $H(t_0)$ est majorée par un nombre positif B donné. La proposition qui suit explique comment borner $H(t_0)$ en fonction d'un certain nombre donné $y > 0$ pour satisfaire la condition $|N_{K/\mathbb{Q}}(d_{F_{t_0}/K})| \leq y$.

On pose $\delta^- = \dfrac{\delta + \delta_P}{2}$ (on a $\delta_P < \delta^- < \delta$) et $B = y^{1/\rho\delta^-}$.

Proposition 4.10. *Pour y suffisamment grand, la spécialisation F_{t_0}/K de $F/K(T)$ en $t_0 \in \mathcal{O}_K$ telle que $\Delta_P(t_0) \neq 0$, $H(t_0) \leq B$ et F_{t_0}/K est galoisienne de groupe G vérifie $N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leq y$.*

Démonstration. Le polynôme $P(t_0, Y)$ est dans $\mathcal{O}_K[Y]$ (comme $t_0 \in \mathcal{O}_K$), est unitaire, irréductible dans $K[Y]$ et de degré $|G|$. Ainsi, si $y_0 \in \overline{K}$ est une racine de $P(t_0, Y)$, alors $1, y_0, \cdots, y_0^{|G|-1}$ est une K-base de F_{t_0}/K qui est composée d'éléments dans $O_{F_{t_0}}$. Cela donne

$$\mathrm{disc}(1, y_0, \cdots, y_0^{|G|-1}) \in d_{F_{t_0}/K}.$$

Comme

$$\mathrm{disc}(1, y_0, \cdots, y_0^{|G|-1}) = \mathrm{disc}(P(t_0, Y)) = \mathrm{disc}_Y(P(T, Y))_{T=t_0} = \Delta_P(t_0),$$

On en déduit

$$N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leq |N_{K/\mathbb{Q}}(\Delta_P(t_0))|.$$

En utilisant l'inégalité entre la norme et la hauteur (voir 1.3.3), on obtient :

$$N_{K/\mathbb{Q}}(\Delta_P(t_0)) \leq H(\Delta_P(t_0))^\rho$$

Ensuite, comme Δ_P est un polynôme de degré δ_P et a au plus $1 + \delta_P$ coefficients non nuls, la proposition 1.5 (3) donne

$$\begin{aligned} N_{K/\mathbb{Q}}(\Delta_P(t_0)) &\leq [(1+\delta_P)H(\Delta_P)H(t_0)^{\delta_P}]^\rho \\ &\leq (1+\delta_P)^\rho H(\Delta_P)^\rho B^{\delta_P \rho}. \end{aligned}$$

On en déduit que

$$N_{K/\mathbb{Q}}(\Delta_P(t_0)) \leq C B^{\rho\delta_P}$$

pour une constante $C > 0$ dépendant de P et K. On obtient alors :

$$N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leq C B^{\rho\delta_P},$$

Le log de ce dernier terme est

$$\log[C B^{\delta_P \rho}] \sim \frac{\rho\delta_P}{\rho\delta^-} \log y \quad y \to \infty$$

Comme $\delta_P < \delta^-$, on peut conclure que pour y assez grand, en fonction de $F/K(T)$ et δ, on a

$$N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leq y.$$

□

On peut maintenant énoncer et démontrer la forme unifiée des théorèmes 4.2 et 4.3. La constante p_0 du théoreme 4.11 ci-dessous est celle qui intervient dans le théorème 4.4.

Theorème 4.11. *Pour tout nombre $y > 0$, on considère l'ensemble S_y d'idéaux premiers $\mathfrak{p}$ de K au dessus de $[p_0, \frac{\log y}{2\rho\delta}]$ qui sont bons pour $F/K(T)$* [4]*. Si y est suffisamment grand (dépendant de $F/K(T)$, δ), alors pour toute donnée de Frobenius $\mathcal{F}_y$ sur S_y, on a*

$$N(F/K(T), y, \mathcal{F}_y) \geq y^{(1-1/|G|)/\delta}.$$

Démonstration. Nous allons appliquer le théorème 4.4 avec $B = y^{1/\rho\delta^-}$ et le théorème 4.8 avec comme ensemble $\mathcal{H}$ choisi, l'ensemble des $t_0 \in \mathcal{O}_K$ vérifiant les conclusions du théorème 4.4 avec $B = y^{1/\rho\delta^-}$.

Comme $\delta^- < \delta$, par le choix de B, on a $[p_0, \frac{\log y}{2\rho\delta}] \subset [p_0, \frac{\log B}{2}]$. On se fixe une donnée de Frobenius $\mathcal{F}_y$ sur S_y que l'on étend de manière arbitraire en une donnée de Frobenius sur $S_B \supset S_y$ sur tous les idéaux premiers de K au dessus de l'intervalle $[p_0, \frac{\log B}{2}]$.

D'après le théorème 4.4, on a $|\mathcal{H}| \geq \frac{B^\rho}{c^{\log B/\log\log B}}$ et d'après le théorème 4.8, il existe $E, \gamma \geq 0$ dépendant de $F/K(T)$ tel que pour y suffisamment grand,

$$\begin{aligned}\mathcal{N}(B, \mathcal{H}) &\geq \frac{|\mathcal{H}| - E}{B^{\rho/|G|}(\log B)^\gamma} \\ &\geq \frac{B^{\rho-\rho/|G|}}{(\log B)^\gamma\, c^{\log B/\log\log B}} - \frac{E}{B^{\rho/|G|}(\log B)^\gamma}\end{aligned}$$

On note la dernière minoration par $f(B)$. Le logarithme de $f(B)$ est asymptotique à $\rho(1-1/|G|)\log B$. Par le choix de B, on obtient finalement :

$$\log(f(B)) \sim \frac{\delta}{\delta^-}\log(y^{(1-1/|G|)/\delta}).$$

Enfin, comme $\delta > \delta^-$, on obtient que pour y assez grand $\log(f(B)) > \log(y^{(1-1/|G|)/\delta})$ et donc

$$\mathcal{N}(B, \mathcal{H}) \geq y^{(1-1/|G|)/\delta}.$$

L'inégalité $N(F/K(T), y, \mathcal{F}_y) \geq \mathcal{N}(B, \mathcal{H})$, due à la proposition 4.10, conclut la preuve du théorème. □

Remarque 4.12. Les extentions comptées sont obtenues par spécialisation d'une seule extension régulière $F/K(T)$. Il est possible que d'autres extensions E/K (ne provenant pas de $F/K(T)$ par spécialisation) vérifient les mêmes conditions. Ceci explique pourquoi la constante obtenue $\alpha(G) = \frac{1-1/|G|}{\delta}$ est plus petite que la constante $a(G)$ (voir aussi [Dèb17, lemma 4.1]).

Pour être plus précis, on peut choisir $\alpha = \frac{1-1/|G|}{2|G|\deg_T P}$ où $P(T, Y)$ est un modèle affine d'une extension galoisienne K-régulière de groupe G.

4. Pour la définition de bon premier, voir la section 4.1

La preuve du théorème 4.2 découle rapidement du théorème 4.11. Le corps K_0 et l'extension $F/K(T)$ sont donnés par le résultat classique de théorie inverse de Galois :

Theorème. *Pour tout groupe fini G, il existe un corps de nombre K_0 dépendant de G tel que l'on puisse construire un revêtement algébrique galoisien $f : X \to \mathbb{P}^1$ défini sur K_0 et de groupe G.*

Remarque 4.13. On peut traduire ce théorème en terme d'extensions de corps par : "Il existe un corps de nombre assez grand K_0 sur lequel G est groupe de Galois régulier". Ce théorème puissant est devenu classique en théorie inverse de Galois dont une preuve est présente dans [**?**, §1]. Cependant, il n'a pas été chose aisée de le démontrer et la preuve de ce résultat a généré de nouvelles pistes de recherches en théorie inverse de Galois, notamment par l'étude des extensions régulières.

Par extension des scalaires, si G est régulier sur K_0, il le sera aussi sur tout corps K contenant K_0. Clairement, le nombre $N(K, G, y)$ du théorème 4.2 est plus grand que $N(F/K(T), y, \mathcal{F}_y)$ du théorème 4.11. Ainsi, le théorème 4.2 (avec $\alpha(G) = (1-1/|G|)/\delta$) s'en déduit grâce au théorème 4.11.

4.3.2 Une généralisation aux extensions non nécessairement galoisiennes

Notons par S_n le groupe des permutations de n lettres $1, \cdots, n$. Pour une extension E/K de degré n, on note par $\hat{E}/K$ sa clôture galoisienne. Le groupe de Galois $\mathrm{Gal}(\hat{E}/K)$ agit transitivement sur les n plongements $E \hookrightarrow \overline{K}$. Fixons G un sous-groupe transitif de S_n et soit $G(1) \subset G$ le sous groupe stabilisateur de l'élément neutre 1. On dira que l'extension E/K a pour *groupe de Galois* $G \subset S_n$ si G est le groupe de Galois de $\hat{E}/K$ et E est le sous-corps fixé par $G(1)$ dans $\hat{E}$. On considère le nombre

$$N(K, G \subset S_n, y) = \#\{E/K \mid E/K \text{ de groupe de Galois } G \subset S_n, |N_{K/\mathbb{Q}}(d_{E/K})| \leq y\}.$$

On peut alors donner le théorème suivant :

Theorème 4.14. *Si G est un groupe de Galois régulier sur K, alors il existe $\alpha > 0$ tel que*

$$N(K, G \subset S_n, y) \geq y^{\alpha} \text{ pour tout } y \text{ suffisamment grand}$$

où $\alpha = (1-1/|G|)/\delta$ avec $\delta > \delta(P)$ et $P(T, Y)$ un modèle affine d'une extension galoisienne K-régulière $F/K(T)$ de groupe G.

Remarque 4.15. Le cas particulier $G(1) = \{1\}$ correspond au cas où l'action $G \subset S_n$ est libre et transitive, ou de manière équivalente, où l'extension E/K est galoisienne de groupe G. Comme la preuve suivante le montre, on déduit le cas général à partir de ce cas particulier.

Démonstration. A chaque extension galoisienne N/K de groupe G correspond une extension intermédiaire E/K qui satisfait $E = N^{G(1)}$ et $\hat{E} = N$. de plus, cette extension est de degré n.

En effet, comme G est un groupe de permutation transitif, l'orbite de $\{1\}$ est de cardinal n. La formule des classes implique que $G(1)$ est d'indice n. L'extension $N^{G(1)}/K$ fixée par $G(1)$ est donc de degré n.

Le dernier point qu'il reste à vérifier est que $\hat{E} = N$. Soit H le plus grand sous-groupe normal de G qui est contenu dans $G(1)$. La clôture galoisienne de $N^{G(1)}$ est N^H. Mais comme H est un sous-groupe normal, pour chaque $g \in G$, on a $H = H^g \subset G(1)^g = G(i)$ (où $i = g(1)$). On a ainsi $H \subset \bigcap_{i=1}^{n} G(i)$ et H est alors le sous-groupe trivial. finalement, $N^H = N$.

La preuve du théorème 4.14 suit aisément : les extensions galoisiennes N/K données par le théorème 4.2 fournissent autant d'extensions E/K que demandées dans le cas général. Notons que la norme $N_{K/\mathbb{Q}}(d_{E/K})$ est plus petite que $N_{K/\mathbb{Q}}(d_{N/K})$. □

4.4 Application au problème de Grunwald

Nous allons maintenant démontrer le théorème 4.3 à partir du théorème 4.11. La preuve, tout comme le théorème, peut se découper en deux parties ; l'une où le groupe G est supposé groupe de Galois régulier sur K, et l'autre dans le cas général.

4.4.1 Cas où G est un groupe de Galois régulier sur K

On suppose que G est régulier sur K et on se fixe une extension K-régulière $F/K(T)$ de groupe G. Soit $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ un problème de Grunwald non ramifié. Pour chaque $\mathfrak{p} \in S$, soit $\mathcal{F}_{\mathfrak{p}}$ la classe de conjugaison dans G du Frobenius de $L^{\mathfrak{p}}/K_{\mathfrak{p}}$ (qui génère $\mathrm{Gal}(L^{\mathfrak{p}}/K_{\mathfrak{p}})$). Alors, pour une extension galoisienne L/K de groupe G, non ramifiée en $\mathfrak{p}$, on a $LK_{\mathfrak{p}}/K_{\mathfrak{p}} = L^{\mathfrak{p}}/K_{\mathfrak{p}}$ si et seulement si $\mathrm{Frob}_{\mathfrak{p}}(L/K) \in \mathcal{F}_{\mathfrak{p}}$.

L'ensemble S_{exc} peut être choisi comme l'ensemble des idéaux premiers $\mathfrak{p}$ de K tels que soit $\mathfrak{p}$ est au dessus d'un nombre premier $p \in [2, p_0[$ [5], soit $\mathfrak{p}$ est mauvais pour $F/K(T)$. Le nombre p_0 est celui défini dans la section 4.1 à partir du groupe G, du nombre de points de branchements r de $F/K(T)$ et du genre g de F.

Etant donné un ensemble S d'idéaux premiers de K tels que $S \cap S_{exc} = \emptyset$, on prend y suffisamment grand de sorte que l'intervalle $[p_0, \dfrac{\log y}{2\rho\delta^-}]$ contienne tous les nombre premiers en dessous des premiers de S. En appliquant le théorème 4.11 et en faisant tendre y vers ∞, on obtient une infinité d'extensions L/K qui sont solutions au problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.

5. Cet intervalle ne dépend pas du problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.

4.4.2 Cas général

On considère maintenant le cas général, i.e., G n'est pas nécessairement groupe de Galois sur K. La définition de S_{exc} est reliée à des résultats de [DG12]. Une constante $c(G)$ y est définie, pour laquelle le lemme suivant est valide.

Lemme 4.16. *Etant donné un groupe fini G et un corps de nombres K, il existe des entiers positifs r et g tels que, avec*

$$S_{exc} = \{\mathfrak{p} \text{ prime of } K \mid p_{\mathfrak{p}} \mid 6|G| \text{ or } p_{\mathfrak{p}} \leq \max(p_0, c(G))\}$$

on a la propriété suivante. Pour chaque ensemble fini S d'idéaux premiers de K avec $S \cap S_{exc} = \emptyset$, il existe une extension galoisienne finie M/K totalement décomposée en chaque premier $\mathfrak{p} \in S$ et une extension M-régulière $F/M(T)$ de groupe G telle que $F/M(T)$ a r points de branchements, le genre de F est g et chaque idéal premier $\mathcal{P}$ de M au-dessus d'un premier $\mathfrak{p} \in S$ est bon pour $F/M(T)$.

Ici p_0 est le nombre premier défini dans §4.1 à partir de K, G et des entiers r, g provenant du lemme précédent.

Une preuve de ce lemme est donnée en §5 de [DG12].

Comme dans le théorème 4.3, soit $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ un problème de Grunwald non ramifié au dessus de K avec $S \cap S_{exc} = \emptyset$. Soit M/K une extension donnée par le lemme 4.16 pour ce S. On considère maintenant le problème de Grunwald sur le corps M déduit par changement de base $M_{\mathcal{P}}/K_{\mathfrak{p}}$, $\mathfrak{p} \in S$. Le premier cas appliqué avec $(G, (L^{\mathfrak{p}}M_{\mathcal{P}}/M_{\mathcal{P}})_{\mathcal{P}\in S_M})$ produit une infinité de M-solutions au problème de Grunwald $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$. Plus spécifiquement, notons que si $\mathcal{P} \in S_M$, alors $\mathcal{P}$ est non ramifié dans $M/\mathbb{Q}$, $p_{\mathcal{P}} > p_0(r, g, G) = p_0(F/M(T))$ (car $S \cap S_{exc} = \emptyset$) et $\mathcal{P}$ est bon pour $F/M(T)$ (par le lemme 4.16). Ainsi, si $\mathcal{P} \in S_M$, $\mathcal{P}$ n'est pas dans l'ensemble exceptionnel du premier cas pour $F/M(T)$. Ce qui prouve le théorème.

Bibliographie

[Bar14] Fabrizio Barroero. Counting algebraic integers of fixed degree and bounded height. *Monatsh. Math.*, 175(1) :25–41, 2014. 43

[BP89] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2) :337–357, 1989. 11, 22

[Bro04] Niklas Broberg. A note on a paper by R. Heath-Brown : "The density of rational points on curves and surfaces" [Ann. of Math. (2) **155** (2002), no. 2, 553–595 ; mr1906595]. *J. Reine Angew. Math.*, 571 :159–178, 2004. 23

[Che12] Huayi Chen. Explicit uniform estimation of rational points II. Hypersurface coverings. *J. Reine Angew. Math.*, 668 :89–108, 2012. 23

[Coh81] S. D. Cohen. The distribution of Galois groups and Hilbert's irreducibility theorem. *Proc. London Math. Soc. (3)*, 43(2) :227–250, 1981. 10

[Dèb09] Pierre Dèbes. Arithmétique des revêtements de la droite. http://math.univ-lille1.fr/~pde/pub.html, 2009. 6

[Dèb86] Pierre Dèbes. G-fonctions et théorème d'irreductibilité de Hilbert. *Acta Arith.*, 47(4) :371–402, 1986. 40

[Dèb96] Pierre Dèbes. Hilbert subsets and S-integral points. *Manuscripta Math.*, 89(1) :107–137, 1996. 22

[Dèb17] Pierre Dèbes. On the Malle conjecture and the self-twisted cover. *Israel J. Math.*, 218(1) :101–131, 2017. 54, 57, 59, 61, 62, 64, 66

[Dèb18] Pierre Dèbes. Groups with no parametric Galois realizations. *Ann. Sci. Éc. Norm. Supér. (4)*, 51(1) :143–179, 2018. 63

[DG12] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier (Grenoble)*, 62(3) :989–1013, 2012. 9, 57, 59, 69

[DLAN17] Cyril Demarche, Giancarlo Lucchini Arteche, and Danny Neftin. The Grunwald problem and approximation properties for homogeneous spaces. *Ann. Inst. Fourier (Grenoble)*, 67(3) :1009–1033, 2017. 9

[Dör27] Karl Dörge. Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes. *Math. Ann.*, 96(1) :176–182, 1927. 40

[FJ86] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1986. 19, 33

[Fri74] Michael Fried. On Hilbert's irreducibility theorem. *J. Number Theory*, 6 :211–231, 1974. 40

[Har07] David Harari. Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini. *Bull. Soc. Math. France*, 135(4) :549–564, 2007. 9

[HB02] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. of Math. (2)*, 155(2) :553–595, 2002. 11, 21, 22

[Hil92] David Hilbert. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 110 :104–129, 1892. 10

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction. 47

[HW18] Yonatan Harpaz and Olivier Wittenberg. Zéro-cycles sur les espaces homogènes et problème de Galois inverse. 2018. 9

[Jor72] Camille Jordan. Recherches sur les substitutions. *J. Liouville*, 17 :351–367, 1872. 60

[Klü06] Jürgen Klüners. Asymptotics of number fields and the Cohen-Lenstra heuristics. *Jux*, 18(3) :607–615, 2006. 8

[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572 :1–26, 2004. 8

[Leg16] François Legrand. Specialization results and ramification conditions. *Israel J. Math.*, 214(2) :621–650, 2016. 57, 58

[Len74] H. W. Lenstra, Jr. Rational functions invariant under a finite abelian group. *Invent. Math.*, 25 :299–325, 1974. 6

[LW54] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76 :819–827, 1954. 19, 33

[Mal02] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2) :315–329, 2002. 7, 8

[Mal04] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2) :129–135, 2004. 7, 8, 54

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999. 7

[MR14] M. Ram Murty and Purusottam Rath. *Transcendental numbers*. Springer, New York, 2014. 36

[Neu79] Jürgen Neukirch. On solvable number fields. *Invent. Math.*, 53(2) :135–164, 1979. 9, 19, 20

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008. 6

[Sal82] David J. Saltman. Generic Galois extensions and problems in field theory. *Adv. in Math.*, 43(3) :250–283, 1982. 6

[Sam67] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967. 18

[Sch79] Stephen Hoel Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4) :433–449, 1979. 43, 52

[Sch91] Wolfgang M. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1991.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54) :323–401, 1981. 19, 20

[SL96] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2) :26–37, 1996. 19

[Swa69] Richard G. Swan. Invariant rational functions and a problem of Steenrod. *Invent. Math.*, 7 :148–158, 1969. 6

[SZ95a] Andrzej Schinzel and Umberto Zannier. The least admissible value of the parameter in Hilbert's irreducibility theorem. *Acta Arith.*, 69(3) :293–302, 1995. 11, 40, 41

[SZ95b] Andrzej Schinzel and Umberto Zannier. The least admissible value of the parameter in Hilbert's irreducibility theorem. *Acta Arith.*, 69(3) :293–302, 1995. 22

[Vos70] V. E. Voskresenskiĭ. On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $Q(x_1, \cdots, x_n)$. *Izv. Akad. Nauk SSSR Ser. Mat.*, 34 :366–375, 1970. 6

[Wal04] Yann Walkowiak. *Effectivité dans le théorème d'irréductiblité de Hilbert*. PhD thesis, Université des Sciences et Technologie de Lille, 2004. 41

[Wal05] Yann Walkowiak. Théorème d'irréductibilité de Hilbert effectif. *Acta Arith.*, 116(4) :343–362, 2005. 21, 22, 32, 34, 41, 45

[Wan48] Shianghaw Wang. A counter-example to Grunwald's theorem. *Ann. of Math. (2)*, 49 :1008–1009, 1948. 9

[Win13] Bruno Winckler. Théorème de Chebotarev effectif. working paper or preprint, November 2013. 19

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1) :17–50, 1989. 7, 8

Résumé

Nous contribuons à la conjecture de Malle sur le nombre d'extensions galoisiennes finies E d'un corps de nombres K donné, de groupe de Galois G et dont la norme du discriminant est bornée par y. Nous établissons une minoration de ce nombre pour tout groupe fini G et sur tout corps de nombres K contenant un certain corps de nombres K'. Pour ce faire, on part d'une extension galoisienne régulière $F/K(T)$ que l'on spécialise. On démontre une version forte du théorème d'Irréductibilté de Hilbert qui compte le nombre d'extensions spécialisées et pas seulement le nombre de points de spécialisation. Nous arrivons aussi à prescrire le comportement local en certains premiers des extensions spécialisées. En conséquence, on déduit de nouveaux résultats sur le problème local-global de Grunwald, en particulier pour certains groupes non résolubles. Afin d'arriver à nos fins, nous démontrons des résultats en géométrie diophantienne sur la recherche de points entiers sur des courbes algébriques.

Abstract

We contribute to the Malle conjecture on the number of finite Galois extensions E of some number field K of Galois group G and of discriminant of norm bounded by y. We establish a lower bound for every group G and every number field K containing a certain number field K'. To achieve this goal, we start from a regular Galois extension $F/K(T)$ that we specialize. We prove a strong version of the Hilbert Irreducibility Theorem which counts the number of specialized extensions and not only the specialization points. We can also prescribe the local behaviour of the specialized extensions at some primes. Consequently, we deduce new results on the local-global Grunwald problem, in particular for some non-solvable groups. To reach our goals, we prove some results in diophantine geometry about the number of integral points on an algebraic curve.