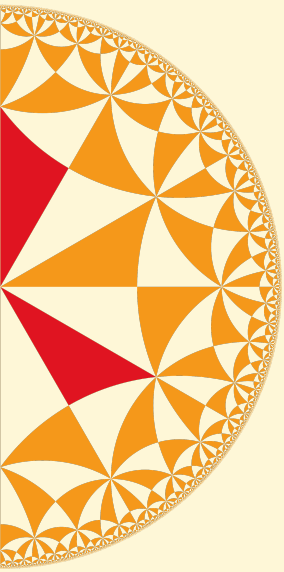
Université Grenoble Alpes



ANNALES DE
L'INSTITUT FOURIER

François Motte

Hilbert irreducibility, the Malle conjecture and the Grunwald problem

Tome 73, n° 5 (2023), p. 2099-2134.

https://doi.org/10.5802/aif.3567

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
73, 5 (2023) 2099-2134

HILBERT IRREDUCIBILITY, THE MALLE CONJECTURE AND THE GRUNWALD PROBLEM

by François MOTTE

Abstract. — The central result is a new version of the Hilbert Irreducibility Theorem which provides explicit bounds for the number of specializations of bounded height of two-variable polynomials over number fields K. As an application, starting from a regular finite Galois extension $F/K(T)$ of group G, we can count the number of specialized extensions F_{t_0}/K retaining the full Galois group G and that are of bounded discriminant norm $N_{K/\mathbb{Q}}(d_{F_{t_0}})$. Consequently, we contribute to the Malle conjecture on the number $N(K,G,y)$ of finite Galois extensions E of some number field K, of group G and of discriminant norm $N_{K/\mathbb{Q}}(d_E) \leqslant y$. For every number field K containing a certain number field K_0 (depending on G), we establish this lower bound: $N(K,G,y) \geqslant y^{\alpha(G)}$ for $y \gg 1$ and some specific exponent $\alpha(G)$ depending on G. We can also prescribe the local behaviour of the specialized extensions at some primes. We deduce new results on the local-global Grunwald problem, in particular for some non-solvable groups.

Résumé. — Le résultat central est une nouvelle version du théorème d'irréductibilité de Hilbert qui fournit des bornes explicites pour le nombre de spécialisations de hauteur bornée d'un polynôme à deux variables sur un corps de nombres K. Comme application, en démarrant d'une extension galoisienne finie régulière $F/K(T)$ de groupe G, nous pouvons compter le nombre d'extensions spécialisées F_{t_0}/K conservant le groupe G et dont la norme du discriminant de l'extension $N_{K/\mathbb{Q}}(d_{F_{t_0}})$ est majorée. En conséquence, nous contribuons à la conjecture de Malle sur le nombre $N(K,G,y)$ d'extensions finies galoisiennes E sur un corps de nombres K, de groupe G et de norme de discriminant $N_{K/\mathbb{Q}}(d_E) \leqslant y$. Pour chaque corps de nombres K contenant un certain corps de nombres K_0 (dépendant de G), nous établissons cette minoration : $N(K,G,y) \geqslant y^{\alpha(G)}$ pour $y \gg 1$ et pour un exposant spécifique $\alpha(G)$ dépendant de G. Nous pouvons aussi décrire le comportement local des extensions spécialisées en certains premiers. Nous déduisons ainsi de nouveaux résultats sur le problème local-global de Grunwald, en particulier pour certains groupes non résolubles.

Keywords: Galois extensions, Inverse Galois theory, Malle conjecture, Grunwald problem, Algebraic covers, Specialization, Diophantine geometry.
2020 *Mathematics Subject Classification:* 12E25, 12F12, 11R58, 11R44, 14Gxx, 11Rxx, 12Fxx.

1. Introduction

This paper is concerned with three classical topics: Hilbert's Irreducibility Theorem, the Malle conjecture and the Grunwald problem. There has been some progress in the recent years on each of these topics and our main results contribute to these developments. The three subsections below elaborate on this and give some references. Though of independent interest, the three topics are linked together through their role in Inverse Galois Theory. We start below with this surrounding aspect which was our original motivation. More explicitly, Theorem A and Theorem B describe our results on the Malle conjecture and the Grunwald problem. We present next Theorem C and its corollary on Hilbert's Irreducibility Theorem, which may be seen as the core achievement responsible for the other advances. We also refer to the figure at the end of the introduction that shows the hierarchy between the main statements of the paper.

1.1. The Malle conjecture

In inverse Galois theory, the Malle conjecture is about the number, say $N(K,G,y)$, with K a number field, G a finite group and y a positive number, of Galois extensions E/K (in a fixed algebraic closure $\overline{K}$ of K), with Galois group G and with ideal discriminant $d_{E/K}$ of norm $N_{K/\mathbb{Q}}(d_{E/K})$ bounded by y. It is well-known that this number is finite. The following conjecture is due to Malle [22]:

Conjecture 1.1. — *There exists a constant $a(G)>0$, depending only on G, such that for every $\varepsilon>0$, we have*

$$c_1 y^{a(G)} \leqslant N(K,G,y) < c_2 y^{a(G)+\varepsilon} \text{ for all } y \geqslant y_0$$

for positive constants c_1 (depending on G, K) and c_2, y_0 (depending on G, K, ε).

Malle also predicts the value of the expected exponent: $a(G)=(|G|(1-1/l))^{-1}$ where l is the smallest prime divisor of $|G|$.

This conjecture is known, with the Malle exponent, for abelian groups, thanks to some work of Wright [33]. Malle worked on the solvable case [22], [23], Klüners and Malle proved the conjecture (also over $\mathbb{Q}$) for nilpotent groups G using the Shafarevich result on the existence of at least one extension of group G [19]. Klüners also proved the lower bound part for dihedral groups of order $2p$ where p is an odd prime [18]. In this paper, we

are also interested in the lower bound part, in particular for non solvable groups, for which the conjecture is wide open. The following definition captures what we aim at.

DEFINITION 1.2. — *We say that a Malle type lower bound holds for G over K if there exists $\alpha(G) > 0$, depending only on G, such that*

$$N(K, G, y) \geqslant c_1 y^{\alpha(G)} \text{ for all } y \geqslant y_0$$

for some positive constants c_1, y_0 depending on K, G.

Obviously, this implies a positive answer to the inverse Galois problem for G over K.

Recall that G is said to be a *regular* Galois group over K_0 if there is a Galois extension $F/K_0(T)$ of group G that is K_0-*regular* (i.e. $F \cap \overline{K_0} = K_0$). Over $\mathbb{Q}$, regular Galois groups include S_n ($n \geqslant 1$) and many simple groups: A_n ($n \geqslant 5$), many $PSL_2(\mathbb{F}_p)$, the Monster group, etc. Our contribution is the following result, valid for any finite group G.

THEOREM A. — *Let G be a finite group. There exists a number field K_0 such that a Malle type lower bound holds for G over every number field K containing K_0. More precisely, the field K_0 can be any number field for which G is a regular Galois group over K_0.*

Our exponent $\alpha(G)$ will be given explicitly. It is smaller than $a(G)$; we explain why in Remark 2.4. There is a more general conjecture for not necessarily Galois extensions; see Section 2.5 where we explain what our approach gives in this situation.

Remarks 1.3.

(1) Theorem A generalizes a result of Dèbes [8, Theorem 1.1] who proved the special case $K = \mathbb{Q}$ and when G is supposed to be a regular Galois group over $\mathbb{Q}$. An important tool of his proof is an explicit version of Hilbert's Irreducibility Theorem due to Walkowiack [31, Theorem 3]. A central part of this paper is to generalize Walkowiak's result, originally proved for $K = \mathbb{Q}$, to any number field K; see Corollary C in Section 1.3.

(2) In addition to the Malle type quantitative estimates given by Theorem A our approach makes it possible to impose some local constraints to the extensions E/K that we count. This "local" aspect of our contribution is shown in Theorem B that we present below in Section 1.2. In this introduction, we have preferred to present the two aspects: quantitative and local, in two separate statements. The

two aspects can however be conjoined. We refer to Theorem AB in Section 2.2, which unifies Theorem A and Theorem B, but is more involved.

(3) Regarding the quantitative aspect, similar conclusions to ours can also be drawn from a 2018 paper of Bilu [2]: based on an older paper of Dvornicich–Zannier [12], Bilu counts, for a cover $X \to \mathbb{P}^1_K$ of curves over a number field K (which is $\mathbb{Q}$ in [12]), the number of distinct residue fields when going through fibers of points of bounded height $\leqslant B$ [2, Corollary 1.4]. Combined with some version of Hilbert's Irreducibility Theorem (different than ours), he can show that most of these fibers are irreducible [2, Corollary 4.4], thus providing, when the original cover is Galois of group G, many different Galois extensions E/K with group G. We leave the reader check that counting extensions by discriminant is essentially equivalent to counting them by height as in [2] and so that conclusions à la Malle can be deduced from his approach.

(4) We also follow a specialization approach. The reason why we obtain some further local conclusions comes from our chosen version of the Hilbert Irreducibility Theorem to construct irreducible fibers of a Galois cover $X \to \mathbb{P}^1_K$: the basic argument is "to go to finite fields"; this provides some control of the Frobenius at some places in the specialized extensions (see Theorem 2.1).

1.2. The Grunwald problem

For every prime $\mathfrak{p}$ of a number field K, the completion of K is denoted by $K_\mathfrak{p}$. The completion of E is then the compositum $EK_\mathfrak{p}$ (with respect to any prime $\mathcal{P}$ above $\mathfrak{p}$). The Grunwald problem asks whether the following is true:

(∗). — *Given a finite set S of primes of K and some finite Galois extensions $(L^\mathfrak{p}/K_\mathfrak{p})_{\mathfrak{p}\in S}$ with Galois group embedding into G, there is a Galois extension E/K of group G whose completion $EK_\mathfrak{p}/K_\mathfrak{p}$ at $\mathfrak{p}$ is $K_\mathfrak{p}$-isomorphic to $L^\mathfrak{p}/K_\mathfrak{p}$ for every $\mathfrak{p} \in S$.*

Such an extension E/K is called a *solution* to the *Grunwald problem* $(G, (L^\mathfrak{p}/K_\mathfrak{p})_{\mathfrak{p}\in S})$.

The case of abelian, and more generally of solvable groups, has been studied by Grunwald, Wang [32] and Neukirch [25]: in particular, the answer is positive if G is of odd order. By a result of Saltman [26, Theorem 5.9], it is

also known to be positive for every group possessing a generic Galois extension; this includes some non-solvable groups, e.g., the symmetric group S_d ($d \geqslant 5$). But in general, some Grunwald problems exist with no solution, for example, if G is cyclic of order 8 and if S contains a prime of K lying over 2 [32]. Nowadays, it is expected that there should be an exceptional finite set S_{exc} of primes such that $(*)$ holds if the set S of primes is disjoint from S_{exc}. Several works have been devoted to this weak form [10, 11, 14]. It was recently established for supersolvable groups (e.g. nilpotent) over any number field [15]. For non solvable groups, a result due to Dèbes and Ghazi [10, Theorem 1.2] shows that any Grunwald problem $(L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S}$ (with $S \cap S_{\text{exc}} = \emptyset$), additionally assumed to be unramified, always has a solution if G is a regular Galois group over K.

Our result on this topic needs the following terminology from [10]. If $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ is a Grunwald problem over K and M/K is a finite Galois extension, denote by S_M the set of primes of M obtained by choosing one prime $\mathcal{P}$ of M over each $\mathfrak{p} \in S$. Denote by $(G, (L^{\mathfrak{p}}M_{\mathcal{P}}/M_{\mathcal{P}})_{\mathcal{P}\in S_M})$ the Grunwald problem over M induced by the base changes $M_{\mathcal{P}}/K_{\mathfrak{p}}$, $\mathfrak{p} \in S$. The base changed problem does not depend on the choice of the primes $\mathcal{P}$.

Note next that if M/K is totaly split at each $\mathfrak{p} \in S$ then $M_{\mathcal{P}} = K_{\mathfrak{p}}$ and $L^{\mathfrak{p}}M_{\mathcal{P}}/M_{\mathcal{P}} = L^{\mathfrak{p}}/K_{\mathfrak{p}}$ ($\mathfrak{p} \in S$). A solution E/M of the base changed Grunwald problem $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S_M})$ will be said to be an *M-solution* of the (original) Grunwald problem $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.

THEOREM B. — *Let G be a finite group and K be a number field.*

(1) *There exists a finite set S_{exc} of primes of K with the following property: if $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ is any unramified Grunwald problem over K with $S \cap S_{\text{exc}} = \emptyset$, then there exist a finite Galois extension M/K, totally split at each $\mathfrak{p} \in S$ and an infinite set of M-solutions E/M to the Grunwald problem $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.*
(2) *Furthermore, one can take $M = K$ if G is a regular Galois group over K, and the number of solutions E/K to the Grunwald problem which satisfies $N_{K/\mathbb{Q}}(d_{E/K}) \leqslant y$ is at least $c_1 y^{\alpha(G)}$ for all $y \geqslant y_0$ (where $\alpha(G)$ is the number that appears in Theorem A) and for some positive constants c_1, depending on K, G and y_0 depending on K, G, S.*

In particular, for all non solvable groups known to be regular groups over $\mathbb{Q}$, any unramified Grunwald problem has a large set (in the sense above) of solutions over $\mathbb{Q}$.

Remark 1.4. — Conclusions (1) and (2) of Theorem B respectively compare to Theorem 1.3 and Corollary 1.5 of [10]. The gain is quantitative in that we provide an estimate on the number of solutions to the Grunwald problems, which are merely asserted to exist in [10]. We again refer to Theorem AB, which is the strongest and most precise result regarding Inverse Galois Theory.

1.3. Diophantine results

We will start with a regular Galois extension $F/K(T)$ of group G and will use the set of extensions F_{t_0}/K obtained from $F/K(T)$ by specializing T to $t_0 \in K$ [(1)]. From the *Hilbert Irreducibility Theorem*, these specialized extensions are still Galois of group G for a large number of t_0.

The idea is, one one hand, to count the number of these specialized extensions and on the other hand, to show that some local conditions can be prescribed to these extensions. We will follow a method developed in [10] and [8] over $\mathbb{Q}$ and which has an important diophantine part.

A major tool will be an estimate, given an irreducible polynomial $P(T,Y)$, of the number $N_T(P,B)$ of specialization points t of bounded height such that $P(t,Y)$ has a root in K. This is a classical problem related to the Hilbert Irreducibility Theorem. In this context, the first totally explicit versions of Hilbert's Irreducibility Theorem were given in [6] and [29]. They were then improved in [31] by Walkowiak who obtained the best known bounds to our knowledge for $N_T(P,B)$.

We will prove the following result, which extends Walkowiak's result to any number field and is interesting for its own sake. Theorem C and Corollary C may in fact be the main contribution of the paper: they are indeed the main source of improvements in the previous results; and as an explicit version of Hilbert's Irreducibility Theorem, valid over any number field, Corollary C has some potential for other applications.

Denote by $\mathcal{O}_K$ the ring of integers of K. We will use the following height for elements $x \in \mathcal{O}_K$, sometimes called the *house* of x:

$$H(x) = \max(|x_1|, \dots, |x_d|)$$

where $x_1, \dots, x_d$ are the $\mathbb{Q}$-conjugates of x (see Section 3 for more on heights).

(1) Definition of specialized extensions is recalled in Section 2.

Consider a polynomial $P(T,Y) \in \mathcal{O}_K[T,Y]$, irreducible in $K[T,Y]$ and monic in Y. For $B > 1$, let $N_T(P,B)$ be the number of $t \in \mathcal{O}_K$ with $H(t) \leqslant B$ and such that $P(t,Y)$ has a root in K.

COROLLARY C. — *There exist some positive constants $a_1, \dots, a_4$ depending on K such that for all suitably large B (depending on K), we have:*

$$N_T(P,B) \leqslant a_1 \deg(P)^{a_2} (\log H)^{a_3} B^{[K:\mathbb{Q}]/\deg_Y(P)} (\log B)^{a_4}$$

where $H = \max(e^e, H(P))$ and $H(P)$ is the height of P. [(2)]

The constant e^e appears for technical reasons in the proof of Corollary C in Section 3.4.

Recall that the total number of $t \in \mathcal{O}_K$ with $H(t) \leqslant B$ is asymptotic to $B^{[K:\mathbb{Q}]}$ (up to some multiplicative constant and a $\log B$ factor) [1, 28].

We stated this result as a "Corollary" as we will obtain it from a result in a more general context. Theorem C is about the following number $N(P,B)$ that we define for a polynomial $P(X_1,X_2) \in \mathcal{O}_K[X_1,X_2]$ irreducible and monic in X_2 as

$$N(P,B) = \#\{(x_1,x_2) \in \mathcal{O}_K^2 \ : \ P(x_1,x_2) = 0,\ H(x_1) \leqslant B,\ H(x_2) \leqslant B\}.$$

Bombieri and Pila introduced a determinant method in 1989 to give uniform bounds over $K = \mathbb{Q}$ [3]. In 2002, Heath-Brown improved on this method and obtained strong results which were refined, also over $\mathbb{Q}$, by Walkowiak who gave totally explicit bounds for the number $N(P,B)$ over $\mathbb{Q}$ [31]. Our Theorem C is inspired by Walkowiak's work but has to deal with several new phenomena occuring on an arbitrary number field: e.g. using prime ideals, Chebotarev density Theorem, norm, height on number field. Having such estimates available for any number field is crucial for our applications.

THEOREM C. — *If B is suitably large (depending on K), we have*

$$N(P,B) \leqslant c \deg(P)^{14} (\log B)^4 B^{[K:\mathbb{Q}]/\deg(P)}$$

where c is a constant depending on K.

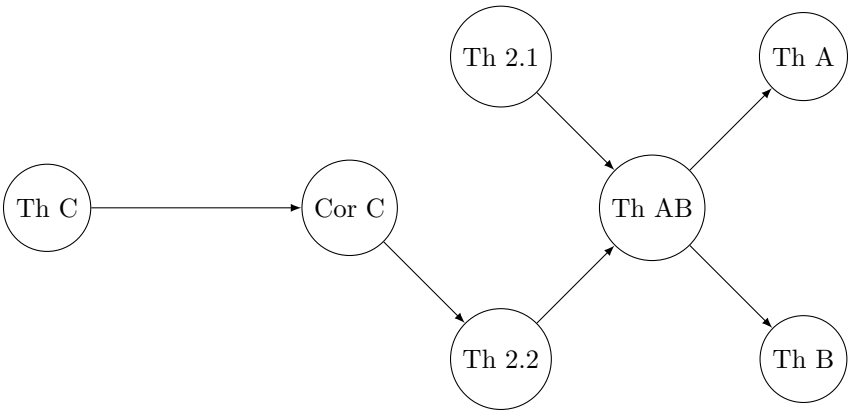
Remark 1.5. — Extending Heath-Brown's original result to arbitrary number fields has also been considered by other authors. Broberg [4] and Chen [5] notably obtained estimates that can be compared to ours. We note that Broberg's ones are not as explicit as Chen's and as our Theorem C and that, compared to Chen's Corollary 4.3, we replace a term B^{ε} by a

(2) see Section 3 for more details on the height $H(P)$.

positive power of $\log B$. Recall however that Heath-Brown, Broberg and Chen also have results in higher dimension.

The paper is organized as follows. In Section 2.1, we present two key results about specialization: Theorem 2.1 and Theorem 2.2. They are intermediate between the pure diophantine statements (Theorem C and Corollary C) and our applications (Theorem A and Theorem B). How we use them to obtain the applications is done in 3 steps and explained in Section 2. In Section 2.2, Theorem AB is stated. In Section 2.3, Theorem AB is shown to imply Theorems A and Theorem B. In Section 2.3, Theorem AB is proved assuming Theorems 2.1 and 2.2. Section 3 is dedicated to the proof of Theorem C and Corollary C. Finally, Theorems 2.1 and 2.2 are proved in Section 4.

The following figure summarizes the structure of our approach.



Acknowledgement

This work was done during my PhD. I would like to express my deep gratitude to my PhD supervisor, Pierre Dèbes. I am also grateful to the referees of my thesis, Arno Fehm and Lior Bary Soroker, and the anonymous referee of this paper for their valuable remarks.

2. Two specialization results and their applications

Both Theorem 2.1 and Theorem 2.2 deal with specializations of a regular Galois extension $F/K(T)$ of group G. The first one is a version of *Hilbert's*

Irreducibility Theorem: it explicitely produces many t_0 such that the specialized extention F_{t_0}/K is of group G. The second one shows that not so many of these specialized extensions F_{t_0}/K can be isomorphic.

We retain the following notation. Fix for the whole Section 2 a number field K of degree $\rho = [K : \mathbb{Q}]$, a finite group G and a K-regular Galois extension $F/K(T)$ of group G. Denote by r the number of branch points of $F/K(T)$ (or equivalently of the associated cover $f : X \to \mathbb{P}^1$) and the genus of F (or of X) by g. For a prime $\mathfrak{p}$ of K, the prime number lying below $\mathfrak{p}$ is denoted by $p_\mathfrak{p}$ and we have $\mathfrak{p} \cap \mathbb{Z} = p_\mathfrak{p}\mathbb{Z}$.

Given a point $t_0 \in K$ (or $t = \infty$), the specialization of $F/K(T)$ at t_0 is the residue extension of the integral closure of the localized ring $K[T]_{\langle T-t_0\rangle}$ in F at an arbitrary prime above $\langle T - t_0\rangle$. Denote it by F_{t_0}/K. If $P(T, Y) \in \mathcal{O}_K[T, Y]$ is what we call an *affine model* of $F/K(T)$, i.e. the minimal polynomial of some primitive element of $F/K(T)$ integral over $\mathcal{O}_K[T]$, then for all $t_0 \in K$ not in the finite list of roots of the discriminant $\Delta_P(T)$ of P with respect to Y, the specialization F_{t_0}/K is also the splitting field of $P(t_0, Y) \in K[Y]$.

2.1. Statements of Theorems 2.1 and Theorem 2.2

Theorem 2.1 below gives a lower bound for the number of 'good' specialization points t_0 of bounded height.

Our statement also involves some local conditions that the specialized extensions should satisfy. Given a set S of prime ideals of $\mathcal{O}_K$, one defines a *Frobenius data* on S as a collection $\mathcal{F}_S = (\mathcal{F}_\mathfrak{p})_{\mathfrak{p}\in S}$ of subsets $\mathcal{F}_\mathfrak{p} \subset G$, each $\mathcal{F}_\mathfrak{p}$ being a non-empty union of conjugacy classes of G. The set S is said to be over the interval $[a, b]$ if S is the set of all prime ideals over the prime numbers $p \in [a, b]$. Requiring that for each $\mathfrak{p} \in S$, the Frobenius $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K)$ lies in $\mathcal{F}_\mathfrak{p}$ will be the form of our local prescription to our specializations F_{t_0}/K. For example, if $\mathcal{F}_\mathfrak{p} = \{1\}$ for every $\mathfrak{p} \in S$, it is that F_{t_0}/K should be totally split at each prime $\mathfrak{p} \in S$.

Choose

- a prime number $p_{-1} \geqslant r^2g^2$ and such that every prime number p which is ramified in $K/\mathbb{Q}$ is $\leqslant p_{-1}$ and
- a prime number p_0 such that the interval $]p_{-1}, p_0[$ has at least as many prime numbers as there are conjugacy classes in G.

The primes p_{-1} and p_0 depend on K, r, g and K, r, g, G respectively. For $B > 1$, let S_B be the set of primes of K over the interval $[p_0, \log(B)/2]$.

THEOREM 2.1 (*Hilbert type*). — *There exists a number $c > 0$ (depending on $F/K(T)$) such that if B is suitably large (depending on $F/K(T)$), if $\mathcal{F}_B = (\mathcal{F}_\mathfrak{p})_{\mathfrak{p}\in S_B}$ is any Frobenius data on S_B, the number of $t_0 \in \mathcal{O}_K$ of height $H(t_0) \leqslant B$ such that*

- *the specialized extension F_{t_0}/K is of group G,*
- *for every $\mathfrak{p} \in S_B$, F_{t_0}/K is unramified and $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K) \in \mathcal{F}_\mathfrak{p}$.*

is at least $\dfrac{B^\rho}{c^{\log B/\log\log B}}$.

In the spirit of the Malle conjecture, we have to count not just the number of good specialization points t_0 but the number of different corresponding extensions F_{t_0}/K. Here enters the *Hilbert–Malle type Theorem* 2.2 below. The special case $K = \mathbb{Q}$ was proved by Dèbes [8, Theorem 1.3]. We generalize it to arbitrary number fields.

THEOREM 2.2 (*Hilbert–Malle type*). — *Let $B > 1$ be a real number. Let $\mathcal{H} \subset \mathcal{O}_K$ be a subset consisting of t_0 such that $\mathrm{Gal}(F_{t_0}/K) = G$ and $H(t_0) \leqslant B$. Denote by $\mathcal{N}(B,\mathcal{H})$ the number of corresponding specialized field extensions F_{t_0}/K when $t_0 \in \mathcal{H}$. There exist $E, \gamma \geqslant 0$ depending only on $F/K(T)$ such that if B is suitably large (depending on $F/K(T)$), we have*

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

Results in the same spirit, over $\mathbb{Q}$, can be found in [34], which itself is inspired by a paper of Dvornicich and Zannier [12]. In [34], Zannier gives various upper bounds for the number of $t_0 \in \mathbb{Z}$ with $|t_0| \leqslant B$ giving the same specialized field extension; these upper bounds should be compared to the denominator in the right-hand side of our inequality.

2.2. A unified version of Theorem A and Theorem B

Retain the notation and assumptions of Section 2. Fix an affine model $P(T,Y) \in \mathcal{O}_K[T,Y]$ of $F/K(T)$; note that P is monic in Y. If $\Delta_P(T)$ is the discriminant of P relative to Y, set $\delta_P = \deg(\Delta_P(T))$. Fix $\delta > \delta_P$. As in [8, §4], one can take $\delta = 3r|G|^4\log(|G|)$.

Given a finite set S of primes of K and a Frobenius data $\mathcal{F}$ on S, let $N(F/K(T), y, \mathcal{F})$ be the number of distinct Galois extensions F_{t_0}/K of group G obtained by specialization from $F/K(T)$ at some $t_0 \in K$, with discriminant of norm $N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leqslant y$ and such that for every $\mathfrak{p} \in S$, F_{t_0}/K is unramified in $\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K) \in \mathcal{F}_\mathfrak{p}$.

We say that a prime $\mathfrak{p}$ of K is *good* for $F/K(T)$ if $\mathfrak{p}$ does not divide $|G|$, the branch divisor $\mathbf{t} = \{t_1, \dots, t_r\}^{(3)}$ is étale at $\mathfrak{p}$ and there is no vertical ramification at $\mathfrak{p}$. We say that $\mathfrak{p}$ is *bad* otherwise (we refer to [10, §4] and [21, Definition 2.6] for precise definitions). We will use that there exist only finitely many bad primes.

The constant p_0 in Theorem AB below is the one that appears in Theorem 2.1.

THEOREM AB. — *For every number $y > 0$, consider the set S_y of primes $\mathfrak{p}$ of K over some prime $p \in [p_0, \frac{\log y}{2\rho\delta}]$ that are good for $F/K(T)$. If y is suitably large (depending on $F/K(T)$, δ), then for every Frobenius data $\mathcal{F}_y$ on S_y, we have*

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

Theorem AB is a generalization of Theorem 1.1 in [8] in that the base field is an arbitrary number field (and not just $K = \mathbb{Q}$ as in [8]).

2.3. Proof of Theorem AB assuming Theorems 2.1 and 2.2

Theorem 2.1 produces many "good" specialization points t_0 with arbitrarily bounded height $H(t_0)$. We explain below how to bound $H(t_0)$ in terms of some given number $y > 0$ to fullfill the required condition $N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leqslant y$.

Set $\delta^- = \frac{\delta+\delta_P}{2}$ (we have $\delta_P < \delta^- < \delta$) and $B = y^{1/\rho\delta^-}$.

PROPOSITION 2.3. — *For y suitably large, the specializations F_{t_0}/K of $F/K(T)$ at $t_0 \in \mathcal{O}_K$ such that $\Delta_P(t_0) \neq 0$, $H(t_0) \leqslant B$ and F_{t_0}/K is Galois of group G satisfy $N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leqslant y$.*

Proof. — The polynomial $P(t_0, Y)$ is in $\mathcal{O}_K[Y]$ (as $t_0 \in \mathcal{O}_K$), is monic, irreducible in $K[Y]$ and of degree $|G|$. Hence, if $y_0 \in \overline{K}$ is a root of $P(t_0, Y)$, then $1, y_0, \dots, y_0^{|G|-1}$ is a K-basis of F_{t_0}/K consisting of elements in $O_{F_{t_0}}$. Thus

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

As $\operatorname{disc}(1, y_0, \dots, y_0^{|G|-1}) = \operatorname{disc}(P(t_0, Y)) = \operatorname{disc}_Y(P(T, Y))_{T=t_0} = \Delta_P(t_0)$, we deduce

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

(3) Formally, $\mathbf{t}$ should be seen as the *divisor* $t_1 + \cdots + t_r$.

Straightforward estimates involving norms and height show next that

$$|N_{K/\mathbb{Q}}(\Delta_P(t_0))| \leqslant CB^{\rho\delta_P}$$

for some constant $C > 0$ depending on P and K; these estimates are detailed in Section 3.1. Hence we obtain:

$$N_{K/\mathbb{Q}}(d_{F_{t_0}/K}) \leqslant CB^{\rho\delta_P},$$

The log of this last term is

$$\log[CB^{\delta_P\rho}] \sim \frac{\rho\delta_P}{\rho\delta^-}\log y \text{ when } y \to \infty.$$

As $\delta_P < \delta^-$, conclude that for y suitably large in terms of $F/K(T)$ and δ, we have

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

We will apply Theorem 2.1 with $B = y^{1/\rho\delta^-}$ and Theorem 2.2 with the following choice of the set $\mathcal{H}$: the set of $t_0 \in \mathcal{O}_K$ satisfying the conclusions of Theorem 2.1 with $B = y^{1/\rho\delta^-}$. We can now proceed to the proof of Theorem AB.

As $\delta^- < \delta$, by the choice of B, we have $[p_0, \frac{\log y}{2\rho\delta}] \subset [p_0, \frac{\log B}{2}]$. Fix a Frobenius data $\mathcal{F}_y$ on S_y and extend it in an arbitrary way to a Frobenius data on $S_B \supset S_y$ of all the primes of K over the interval $[p_0, \frac{\log B}{2}]$.

According to Theorem 2.1, we have $|\mathcal{H}| \geqslant \frac{B^\rho}{c^{\log B/\log\log B}}$. From Theorem 2.2, there exist $E, \gamma \geqslant 0$ depending on $F/K(T)$ such that for y suitably large,

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

Denote the last lower bound by $f(B)$. The logarithm of $f(B)$ is asymptotic to $\rho(1-1/|G|)\log B$. From the choice of B, we finally obtain

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

Because $\delta > \delta^-$, we obtain that for y suitably large

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

and so

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

The inequality $N(F/K(T), y, \mathcal{F}_y) \geqslant \mathcal{N}(B,\mathcal{H})$ concludes the proof of Theorem AB.

2.4. Proof of Theorems A and B assuming Theorem AB

Concerning Theorem A, one proceeds as follows. The starting point is that every finite group G is known to be a regular Galois group over $\overline{\mathbb{Q}}$, and so over *some* number field, say K_0. This is a classical result that goes back to the Riemann Existence Theorem; this is explained e.g. in [30, §6.3], or in [7] (see §12 for the final descent from $\mathbb{C}$ to $\overline{\mathbb{Q}}$).

If K is a number field containing K_0, G is still a regular Galois group over K. Clearly $N(K,G,y)$ from Section 1.1 is bigger than $N(F/K(T),y,\mathcal{F}_y)$ from Theorem AB. Thus Theorem A, with $\alpha(G)=(1-1/|G|)/\delta$, follows immediately from Theorem AB.

Remark 2.4. — Our counted extensions are obtained by specialization of one single regular extention $F/K(T)$. There may be other extensions E/K (not coming from $F/K(T)$ by specialization) satisfying the same conditions. This explains why our constant $\alpha(G)$ is smaller than the Malle constant $a(G)$ (see [8, Lemma 4.1]).

To prove Theorem B, suppose first that G is a regular Galois group over K and fix a K-regular Galois extension $F/K(T)$ of group G. Consider an unramified Grunwald problem $(G,(L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$. For each $\mathfrak{p}\in S$, let $\mathcal{F}_{\mathfrak{p}}$ be the conjugacy class in G of the Frobenius of $L^{\mathfrak{p}}/K_{\mathfrak{p}}$ (which generates $\mathrm{Gal}(L^{\mathfrak{p}}/K_{\mathfrak{p}})$). Then for a Galois extension L/K of group G, unramified at $\mathfrak{p}$, we have $LK_{\mathfrak{p}}/K_{\mathfrak{p}}=L^{\mathfrak{p}}/K_{\mathfrak{p}}$ if and only if $\mathrm{Frob}_{\mathfrak{p}}(L/K)\in\mathcal{F}_{\mathfrak{p}}$. Theorem B(2) then follows from Theorem AB.

Namely, the set S_{exc} can be chosen as the set of primes $\mathfrak{p}$ of K such that either $\mathfrak{p}$ is over some prime number $p\in[2,p_0[$ [(4)] or $\mathfrak{p}$ is bad for $F/K(T)$. Here p_0 is the prime number defined in Section 2.1 from the group G, the branch point number r of $F/K(T)$ and the genus g of F. Given a set S of primes of K such that $S\cap S_{\mathrm{exc}}=\emptyset$, take y suitably large so that the interval $[p_0,\frac{\log y}{2\rho\delta^-}]$ contains all prime numbers under all primes of S. Applying Theorem AB with letting y go to ∞ yields infinitely many extensions L/K that are solution to any Grunwald problem $(G,(L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.

Consider now the general case (1) of Theorem B, i.e., G is not necessarily a regular Galois group over K. The definition of S_{exc} relies on results from [10]. A constant $c(G)$ is defined there, for which the following lemma is true.

(4) This interval does not depend on the Grunwald problem $(G,(L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$.

LEMMA 2.5. — *Given a finite group G and a number field K, there exist non negative integers r and g such that with*

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

the following holds. For every finite set S of primes of K with $S \cap S_{\text{exc}} = \emptyset$, there exists a finite Galois extension M/K totally split at each prime $\mathfrak{p} \in S$ and an M-regular Galois extension $F/M(T)$ of group G such that $F/M(T)$ has r branch points, the genus of F is g and each prime $\mathcal{P}$ of M over a prime $\mathfrak{p} \in S$ is good for $F/M(T)$.

Here $p_0 = p_0(r, g, G)$ is the prime number defined in Section 2.1 from K, G and the integers r, g from the statement.

A proof of this lemma is given in [10, §5].

As in Theorem B, let then $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$ be an unramified Grunwald problem over K with $S \cap S_{\text{exc}} = \emptyset$. Let M/K be the extension given by Lemma 2.5 for this S. Consider next the Grunwald Problem over the field M deduced by the base changes $M_{\mathcal{P}}/K_{\mathfrak{p}}$, $\mathfrak{p} \in S$. The first case applied with $(G, (L^{\mathfrak{p}}M_{\mathcal{P}}/M_{\mathcal{P}})_{\mathcal{P}\in S_M})$ produces an infinite number of M-solutions to the Grunwald problem $(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p}\in S})$. More specifically, note that if $\mathcal{P} \in S_M$, then $\mathcal{P}$ is unramified in $M/\mathbb{Q}$, $p_{\mathcal{P}} > p_0(r, g, G) = p_0(F/M(T))$ (because $S \cap S_{\text{exc}} = \emptyset$) and $\mathcal{P}$ is good for $F/M(T)$ (from Lemma 2.5): thus if $\mathcal{P} \in S_M$, $\mathcal{P}$ is not in the exceptional set of the first case for $F/M(T)$. This proves Theorem B.

2.5. Using Theorem AB for not necessarily Galois extensions

Denote by S_n the permutation group on n letters $1, \ldots, n$. For an extension E/K of degree n, we denote by $\hat{E}/K$ its Galois closure. The Galois group $\text{Gal}(\hat{E}/K)$ acts transitively on the n embeddings $E \hookrightarrow \overline{K}$. Fix a transitive subgroup G of S_n and let $G(1) \subset G$ be the stabilizing subgroup of the element 1. We say that the extension E/K has *Galois group* $G \subset S_n$ if G is the Galois group of $\hat{E}/K$ and E is the fixed field of $G(1)$ in $\hat{E}$. Consider the number

$$N(K, G \subset S_n, y) = \#\left\{ E/K \;\middle|\; \begin{matrix} E/K \text{ of Galois group } G \subset S_n, \\ N_{K/\mathbb{Q}}(d_{E/K}) \leqslant y \end{matrix} \right\}.$$

Theorem AB provides the following lower bound for $N(K, G \subset S_n, y)$.

(∗∗). — *If G is a regular Galois group over K, then*

$$N(K, G \subset S_n, y) \geqslant y^{\alpha} \text{ for every suitably large } y$$

where $\alpha = (1 - 1/|G|)/\delta$ with $\delta > \delta_P$ and $P(T, Y)$ is an affine model of some K-regular Galois extension $F/K(T)$ of group G.

(Indeed, to every Galois extension N/K of group G corresponds one intermediate extension E/K which satisfies $E = N^{G(1)}$ and $\hat{E} = N$. Furthermore, this extension is of degree n. The Galois extensions N/K provided by Theorem AB provide as many extensions E/K as requested in the general case; and we have $N_{K/\mathbb{Q}}(d_{E/K}) \leqslant N_{K/\mathbb{Q}}(d_{N/K})$.)

It would be desirable to prove the version of $(**)$ for which $P(T, Y)$ is an affine model of a degree n extension $F/K(T)$ whose Galois closure is a K-regular Galois extension of group G. This would make the parameter δ_P smaller and so the exponent α bigger in the main inequality. Dealing directly with not necessarily Galois extensions $F/K(T)$ seems natural but this has led us to technical difficulties and we have not pursued in this direction: for example, the Galois assumption is important in Theorem 4.4, which is a main tool in our approach.

3. Proof of the diophantine Theorem C and Corollary C

In this section, we prove Theorem C and Corollary C. We work over a fixed number field K of degree $[K : \mathbb{Q}] = \rho$.

3.1. Basic data and generalized Heath-Brown result

3.1.1. The height

Recall that M_K is the set of places of K and for $v \in M_K$, denote by K_v the completion of K for v, by O_v its valuation ring, and by $\mathbb{Q}_v$ the completion of $\mathbb{Q}$ for v ($\mathbb{Q}_p$ for a finite place and $\mathbb{R}$ for an archimedean place). The places are normalized in such a way they are equal to the usual absolute value on $\mathbb{Q}_v$. We denote by ρ_v the degree $[K_v : \mathbb{Q}_v]$.

The height of $x \in \mathcal{O}_K$ is $H(x) = \max_{\sigma : K \hookrightarrow \overline{K}} |\sigma(x)| = \max_{\substack{v \in M_K \\ v/\infty}} |x|_v$.

We generalize the height to tuples and polynomials as follows:

- for $\underline{x} = (x_1, \dots, x_n) \in \mathcal{O}_K^n$, $H(\underline{x}) = \max_{v/\infty} H_v(\underline{x})$, where $H_v(\underline{x}) = \max(|x_1|_v, \dots, |x_n|_v)$,
- the height of a polynomial P with coefficients $c_1, \dots, c_n$ in $\mathcal{O}_K$ is $H(P) = H(c_1, \dots, c_n)$. We also define $H_v(P) = H_v(c_1, \dots, c_n)$.

Remark 3.1. — The reason why we prefer to use H rather than more usual heights like the Weil height $H_{\mathrm{W}}(x) = \prod_{v\in M_K} \max(1,|x|_v)^{\rho_v/\rho}$ (for $x \in K$) is mostly technical. The two heights compare well over $\mathcal{O}_K$: for $x \in \mathcal{O}_K$, we have $H(x)^{1/\rho} \leqslant H_{\mathrm{W}}(x) \leqslant H(x)$.

3.1.2. Preliminary lemmas

The following notation and properties are used all along this section. For Theorem C, we consider a polynomial $P(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$.

For Corollary C, we prefer to denote the indeterminates by T and Y, as they do not play the same role.

Both polynomials are assumed to be irreducible over K. We let

- m be the degree of P in X_1 (or in T),
- n be the degree of P in X_2 (or in Y),
- d be the total degree of P (we may and will assume that $d \geqslant 2$).

The following statement collects different properties used in this paper.

PROPOSITION 3.2. — *Let $\underline{x} = (x_1, \dots, x_n)$ be a n-tuple in $\mathcal{O}_K^n$ ($n \in \mathbb{N}$), let $Q(\underline{X}) \in \mathcal{O}_K[\underline{X}] = \mathcal{O}_K[X_1, \dots, X_n]$ be a polynomial in n variables with l non-zero coefficients. Let $\sigma : K \to \overline{\mathbb{Q}}$ be a field morphism. Then we have*

(1) $H(\underline{x}) = H(\sigma(\underline{x}))$.
(2) $H(x_i) \leqslant H(\underline{x}) \leqslant H(x_1)\cdots H(x_n)$. $(i = 1, \dots, n)$.
(3) $H(Q(x_1, \dots, x_n)) \leqslant l \cdot H(Q) \cdot M^{\deg(Q)}$ *where* $M = \max_{i=1,\dots,n} H(x_i)$.

Proof.

(1). — It is clear.

(2). — Using the definition, we have

$$H(x_i) = \max_{v/\infty} \max(|x_i|_v) \leqslant \max_{v/\infty} \max(|x_1|_v, \dots, |x_n|_v) \leqslant \prod_{i=1}^{m} \max_{v/\infty} \max(|x_i|_v).$$

(3). — We write $Q(\underline{X}) = \sum p_{\underline{a}} \underline{X}^{\underline{a}} = \sum p_{a_1,\dots,a_n} X_1^{a_1} \dots X_n^{a_n}$ and set $d = \deg(Q)$.

For every archimedean place v, we have

$$|Q(\underline{x})|_v \leqslant l \cdot \max_{\underline{a}}(|p_{\underline{a}}|_v) M^d.$$

Whence

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

□

IDEALS IN $\mathcal{O}_K$ AND NORM. — *The norm of an ideal $J \subset \mathcal{O}_K$ is the cardinality of the quotient ring $N_{K/\mathbb{Q}}(J) = \#\mathcal{O}_K/J$ (see* [27, §3.5] *for more details). For $a \in \mathcal{O}_K$, $a \neq 0$,*

$$N_{K/\mathbb{Q}}(a\mathcal{O}_K) = |N_{K/\mathbb{Q}}(a)| = \prod_{\sigma : K \to \overline{\mathbb{Q}}} |\sigma(a)| \leqslant H(a)^\rho.$$

We can now prove the inequality

$$|N_{K/\mathbb{Q}}(\Delta_P(t_0))| \leqslant CB^{\rho\delta_P} \text{ if } H(t_0) \leqslant B$$

stated in the proof of Proposition 2.3.

Proof. — Using the inequality between norm and height, we obtain:

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

Then, as Δ_P is a polynomial of degree δ_P and has at most $1+\delta_P$ non-zero coefficients, Proposition 3.2(3) yields

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

□

We will also use the following result.

LEMMA 3.3. — *Let $a \in \mathcal{O}_K$. The number of primes $\mathfrak{p}$ of K which divide the ideal $a\mathcal{O}_K$ is less than or equal to $\rho \log_2(H(a))$.*

Proof. — Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals of $\mathcal{O}_K$ dividing $a\mathcal{O}_K$. As $\mathcal{O}_K$ is a Dedekind domain, we have $a\mathcal{O}_K = \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n$ are positive integers. Then

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

As $N_{K/\mathbb{Q}}(\mathfrak{p}_i) \geqslant 2$, $i = 1, \ldots, n$, we obtain $H(a)^\rho \geqslant 2^n$, thus proving the lemma. □

3.1.3. A generalized Heath-Brown result

For every real number $B > 1$, set

$$R(P,B) = \{(x_1, x_2) \in \mathcal{O}_K^2 \mid P(x_1, x_2) = 0,\ H(x_1) \leqslant B,\ H(x_2) \leqslant B\},$$

and

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

Our approach for bounding the number $N(P,B)$ follows an idea of Heath-Brown [16] which Walkowiak made effective (both in the case $K = \mathbb{Q}$). We

generalize to the case of an arbitrary number field K. The method consists in splitting the set $R(P,B)$ in k subsets, each being the zero set of some polynomial $P_i \in \mathcal{O}_K[X_1,X_2]$ relatively prime with P, $i=1,\dots,k$. The Bezout theorem then yields the desired bound for $N(P,B)$. An important point is to have a good upper bound for the number k of polynomials P_i. To this end, we prove the following effective generalized Heath-Brown result.

THEOREM 3.4. — *Let $P(X_1,X_2) \in \mathcal{O}_K[X_1,X_2]$ be a polynomial, irreducible in $\overline{K}[X_1,X_2]$ of degree d, let B be a suitably large real number (depending on ρ, d) and let $D > d$ be an integer. There exist a number $k \geqslant 1$ and some polynomials $P_1,\dots,P_k \in \mathcal{O}_K[X_1,X_2]$ relatively prime with P in $\overline{K}[X_1,X_2]$ and of degree $\deg(P_i) \leqslant D$, such that every point $(x_1,x_2) \in R(P,B)$ is a zero of at least one of $P_1,\dots,P_k$. Furthermore, the integer k is bounded from above by:*

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

where c_2 is a constant depending only on K.

Remark 3.5. — This theorem is true for all integers $D > d$. In the proof of Theorem C, we will use it with $D = [d\log(B)+1]$ (where $[.]$ is the integral part of a real number).

Theorem 3.4 can be compared to Theorem 4.2 of [5] which is more involved but has interesting features (see [5, Remark 4.4])

3.2. Proof of Theorem 3.4

Fix $D > d$ and $B > 1$. The condition that B should be suitably large appears in Section 3.2.3. We explain below how to construct the polynomials $P_1,\dots,P_k$, that appear in Theorem 3.4. As P is irreducible, we have $d \geqslant 1$. Up to exchanging X_1 and X_2, one may assume that $\deg_{X_1}(P) \geqslant 1$.

We take one of the polynomials P_i, $i=1,\dots,k$ to be $\frac{\partial P}{\partial X_1}$; it is relatively prime to P and of degree $\leqslant d$. So we may next focus on the subset

$$S(P,B) = \left\{ \underline{x} \in R(P,B) \;\middle|\; \frac{\partial P}{\partial X_1}(\underline{x}) \neq 0 \right\} \subset R(P,B),$$

and look for k' polynomials P_i to cover this subset. The number k in Theorem 3.4 will be equal to $1+k'$.

3.2.1. First step: constructing subsets $S(P,B,\mathfrak{p}) \subset S(P,B)$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and

$$S(P,B,\mathfrak{p}) = \left\{ \underline{x} \in S(P,B) \;\middle|\; \frac{\partial P}{\partial X_1}(\underline{x}) \notin \mathfrak{p} \right\}.$$

We have

$$S(P,B) = \bigcup_{\mathfrak{p} \text{ prime of } K} S(P,B,\mathfrak{p}).$$

The following lemma shows that one can take finitely many primes $\mathfrak{p}$ in the previous union and that these primes can be chosen to be totally split in $K/\mathbb{Q}$.

LEMMA 3.6. — *Let $\mathcal{P}$ be an integer, $h(B) = \log_2(2d^3H(P)B^{d-1})$ and $r = [\rho h(B)] + 1$. Then for $\mathcal{P}$ suitably large (depending on K), there exist r totally split prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of K such that $S(P,B) = \bigcup_{i=1}^{r} S(P,B,\mathfrak{p}_i)$ and for which we furthermore have*

$$\mathcal{P} \leqslant N_{K/\mathbb{Q}}(\mathfrak{p}_i) \leqslant C_1 h(B)^2 \, \frac{\mathcal{P}}{\log \mathcal{P}} \, \log\left(\frac{\mathcal{P}}{\log \mathcal{P}}\right)$$

for a constant C_1 depending on K.

Proof. — Fix $\underline{x} = (x_1, x_2) \in S(P,B)$; we have $\frac{\partial P}{\partial X_1}(\underline{x}) \neq 0$. The number of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\frac{\partial P}{\partial X_1}(\underline{x}) \in \mathfrak{p}$ is at most $\rho \log_2(H(\frac{\partial P}{\partial X_1}(\underline{x})))$ from Lemma 3.3. The height of $\frac{\partial P}{\partial X_1}(\underline{x})$ can be estimated using Proposition 3.2: the number l of the non-zero monomials of $\frac{\partial P}{\partial X_1}$ is bounded by $d(d+1)/2 \leqslant d^2$, its degree by $d-1$ and its height by $dH(P)$, whence

$$H\left(\frac{\partial P}{\partial X_1}(x_1,x_2)\right) \leqslant l \cdot H\left(\frac{\partial P}{\partial X_1}\right) \cdot B^{d-1} \leqslant d^3 H(P) B^{d-1}.$$

Consider the Galois closure $\widehat{K}/\mathbb{Q}$ of $K/\mathbb{Q}$ and its Galois group Γ. Denote by $\pi_{\{1\}}(x)$ the number of primes $p \leqslant x$, totally split in $\mathcal{O}_{\widehat{K}}$.

Fix an integer $\mathcal{P} > 0$. We choose $x > 0$ such that

$$(*) \qquad \pi_{\{1\}}(x) \geqslant h(B) + 1 + \pi_{\{1\}}(\mathcal{P}).$$

More specifically, we take x as follows: $x = 2a \log a$ with

$$a = 6\,|\Gamma|\, h(B)\, \pi_{\{1\}}(\mathcal{P}).$$

We have $a > 6\,|\Gamma|\,\pi_{\{1\}}(\mathcal{P})$ and for $\mathcal{P}$ suitably large, depending on K, it is easily checked that $\frac{x}{\log x} \geqslant a$ and so, as $h(B) \geqslant 1$,

$$\frac{x}{2|\Gamma| \log x} \geqslant 3\, h(B)\, \pi_{\{1\}}(\mathcal{P}) \geqslant h(B) + 1 + \pi_{\{1\}}(\mathcal{P}).$$

This implies that $\pi_{\{1\}}(x) \geqslant h(B)+1+\pi_{\{1\}}(\mathcal{P})$ as from the Chebotarev density Theorem and the Prime Number Theorem, we have $\pi_{\{1\}}(x) \geqslant \frac{x}{2|\Gamma|\log x}$, for x suitably large.

From $(*)$, there exist at least $[h(B)]+1$ prime numbers $p \in]\mathcal{P}, x]$ that are totally split in $K/\mathbb{Q}$. Every such prime number p provides ρ primes of K of norm equal to p. Hence we have $\rho[h(B)]+\rho$ distinct prime ideals totally split in K and of norm $\leqslant x$. Furthermore, this number $\rho[h(B)]+\rho$ is $\geqslant r$ as $r=[\rho h(B)]+1$.

We choose r of these ideals which we denote by $\mathfrak{p}_1,\dots,\mathfrak{p}_r$. By Lemma 3.3 the number of ideals which divide $\frac{\partial P}{\partial X_1}(x_1,x_2)$ in $\mathcal{O}_K$ is $\leqslant \rho h(B) < r$. Then there exists an ideal, say $\mathfrak{p}_i$ ($i \in \{1,\dots,r\}$), such that $\frac{\partial P}{\partial X_1}(x_1,x_2) \notin \mathfrak{p}_i$, which means that $(x_1,x_2) \in S(P,B,\mathfrak{p}_i)$. Thus we obtain $S(P,B) = \bigcup_{i=1}^{r} S(P,B,\mathfrak{p}_i)$.

Now, also from the Chebotarev Theorem, $\pi_{\{1\}}(\mathcal{P}) \leqslant \frac{2\mathcal{P}}{|\Gamma|\log \mathcal{P}}$ for $\mathcal{P}$ suitably large depending on K. So for $i=1,\dots,r$,

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

We conclude that for some constant C_1 depending on K we have

$$N_{K/\mathbb{Q}}(\mathfrak{p}_i) \leqslant C_1 h(B)^2 \frac{\mathcal{P}}{\log\mathcal{P}}\log\left(\frac{\mathcal{P}}{\log\mathcal{P}}\right). \qquad \square$$

3.2.2. Working on $S(P,B,\mathfrak{p})$ for a fixed $\mathfrak{p} \in \{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$

For the next steps, we choose a monomial $X_1^{m_1}X_2^{m_2}$ such that the corresponding coefficient in P is non-zero, $m_1+m_2=d$ and m_1 is maximal. We let then $\mathcal{E}$ be the following set of monomials

$$\mathcal{E} = \{X_1^{e_1}X_2^{e_2} \mid e_i \geqslant 0,\ i=1,2,\ e_1 < m_1 \text{ or } e_2 < m_2,\ e_1+e_2 \leqslant D\}.$$

We sometimes identify a monomial $X_1^{e_1}X_2^{e_2}$ and the corresponding pair (e_1,e_2) of integers.

Fix $\mathfrak{p} \in \{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$. Recall from Lemma 3.6 that $N_{K/\mathbb{Q}}(\mathfrak{p}) = p \geqslant \mathcal{P}$ and $D > d$. Let $\mathbb{F}_p = \mathcal{O}_K/\mathfrak{p}$ be the residue field of $\mathfrak{p}$. For every zero $\underline{t}=(t_1,t_2) \in \mathbb{F}_p^2$ of P modulo $\mathfrak{p}$ such that $\frac{\partial P}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$, consider then the following subset of $S(P,B,\mathfrak{p})$:

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

We have $S(P,B,\mathfrak{p}) = \bigcup_{\underline{t}} S(\underline{t})$ where $\underline{t}$ ranges over the points that satisfies $\frac{\partial P}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$. Fix such a $\underline{t}$. We have $\frac{\partial P}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$. The goal

now is to construct one polynomial (one of those in Theorem 3.4) that vanishes at all points of $S(\underline{t})$.

Denote by $\underline{x_i} = (x_{i1}, x_{i2})$, $i = 1, \dots, L$, the elements of $S(\underline{t})$ (with $L = \mathrm{card}(S(\underline{t}))$).

Set $E = \#\mathcal{E}$ and let M be the $L \times E$ matrix

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

More specifically, if $\mathcal{E} = \{\underline{X}^{\underline{e_1}}, \dots, \underline{X}^{\underline{e_E}}\}$,

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

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

PROPOSITION 3.7. — *Assume that $\mathcal{P}^{E(E-1)/2} \geqslant (E^E B^{E'})^\rho$. Then we have the following.*

(1) *The rank of M is $\leqslant E - 1$,*
(2) *There exists a polynomial $P_{\underline{t}}[X_1, X_2] \in \mathcal{O}_K[X_1, X_2]$ of degree $\leqslant D$ such that*
   - *$P_{\underline{t}}(\underline{x}) = 0$ for all $\underline{x} \in S(\underline{t})$,*
   - *$P_{\underline{t}}$ and P are relatively prime in $K[X_1, X_2]$.*

The proof uses the following lemma which is some version of Hensel's lemma and reduces the problem from two to one variable. We refer to [31] Lemma 1.2 for a proof (mod p^m there just has to be replaced by mod $\mathfrak{p}^m$).

LEMMA 3.8. — *Let $P(X_1, X_2) \in \widetilde{\mathcal{O}_K}[X_1, X_2]$ be a polynomial in two variables with coefficients in the completion $\widetilde{\mathcal{O}_K}$ of $\mathcal{O}_K$ for the prime ideal $\mathfrak{p}$. Let $\underline{u} = (u_1, u_2) \in \widetilde{\mathcal{O}_K}$ such that $P(\underline{u}) = 0$ and $\frac{\partial F}{\partial X_1}(\underline{u}) \notin \mathfrak{p}$. For every integer $m \geqslant 1$, there exists $f_m(Y) \in \widetilde{\mathcal{O}_K}[Y]$ such that if $P(\underline{x}) = 0$ for a certain $\underline{x} = (x_1, x_2) \in \widetilde{\mathcal{O}_K}^2$ with $\underline{x} = \underline{u} \mod \mathfrak{p}$, then $x_1 = f_m(x_2) \mod \mathfrak{p}^m$ (for every $m \geqslant 1$).*

Proof of Proposition 3.7. — First, note that (2) easily follows from (1). As the rank of M is $\leqslant E-1$, there exists a non-zero matrix $C = (c_{\underline{e}}) \in \mathcal{O}_K^E$, such that $MC = 0$. We use this matrix to construct our polynomial $P_{\underline{t}}$:

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

This non-zero polynomial is of degree $\leqslant D$ and $P_{\underline{t}}(x) = 0$ for every $x \in S(\underline{t})$.

Furthermore, assume that there exists some polynomial Q such that $P_t = PQ$. Denote by d' the degree of Q. There exists a monomial $X_1^{g_1}X_2^{g_2}$, with non-zero coefficient in Q, such that $g_1 + g_2 = d'$ and g_1 is maximal. Then the monomial $X_1^{m_1+g_1}X_2^{m_2+g_2}$ in PQ has a non-zero coefficient. As $m_1 + g_1 \geqslant m_1$ and $m_2 + g_2 \geqslant m_2$, this monomial is not in $\mathcal{E}$. This proves that P and P_t are relatively prime.

Proof of 1. If $L < E$ the result is clear. Suppose that $L \geqslant E$ and consider a minor, say Δ, of order E. Up to permuting the lines and columns, one may assume that $\Delta = \det[(\underline{x_i}^{\underline{e}})_{1\leqslant i\leqslant E,\ \underline{e}\in\mathcal{E}}]$, or more specifically

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

We will show that $\Delta = 0$. To do this, we will show that the norm of Δ is divisible by a big power p^ν of p and the height of Δ is bounded by a number A such that $A^\rho < p^\nu$ and use the inequality $N(a) \leqslant H(a)^\rho$ for every $a \in \mathcal{O}_K$.

For each $i = 1, \ldots, E$, the pair $\underline{x_i} = (x_{i1}, x_{i2})$ is in $S(\underline{t})$, in particular $\underline{x_i} = \underline{t} \mod \mathfrak{p}$. Furthermore, we have assumed that $\frac{\partial P}{\partial X_1}(\underline{t}) \notin \mathfrak{p}$. So we have

$$\frac{\partial P}{\partial X_1}(\underline{x_i}) \notin \mathfrak{p} \text{ and } P(\underline{x_i}) = 0 \ (i = 1, \ldots, E).$$

We apply Lemma 3.8 with P, $\underline{u} = (u_1, u_2) \in \widetilde{\mathcal{O}_K}^2$ taken to be a lift of $\underline{t} = (t_1, t_2)$, and with $\underline{x}$ taken to be $\underline{x_i}$ $(i = 1, \ldots, E)$. Conclude that with $f_m(Y)$ the polynomials from Lemma 3.8, we have $x_{i1} = f_m(x_{i2}) \mod \mathfrak{p}^m$ (for every $m \geqslant 1$ and $i = 1, \ldots, E$).

Set

$$\underline{w_i} = (w_{i1}, w_{i2}) = (f_m(x_{i2}), x_{i2}),$$

consider the matrix $M_0 = (\underline{w_i}^{\underline{e}})_{1\leqslant i\leqslant E,\ \underline{e}\in\mathcal{E}}$ and set $\Delta_0 = \det(M_0)$. For every $m \geqslant 1$, we have

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

Because of the definition of $S(\underline{t})$, $x_{i2} = t_2 \mod \mathfrak{p}$. Thus x_{i2} can be written as $x_{i2} = u_2 + y_{i2}$ where u_2 is independent of i and $y_{i2} \in \mathfrak{p}$ for all $i = 1, \ldots, E$.

For $\underline{e} \in \mathcal{E}$, we then have

$$\underline{w_i}^{\underline{e}} = f_m(u_2 + y_{i2})^{e_1}(u_2 + y_{i2})^{e_2} = g_{\underline{e}}(y_{i2})$$

for some polynomial $g_{\underline{e}}(Y) \in \widetilde{\mathcal{O}_K}[Y]$.

Next, we study the divisibility by p of the norm of Δ_0. Every column of M_0 corresponds to a polynomial $g_{\underline{e}}(Y)$. We claim that we can make some substitutions and $\widetilde{\mathcal{O}_K}$-linear combinations on the columns, without changing the determinant of M_0 (up to the sign), in such a way to organize the columns by strictly growing Y-adic valuation. First, reorder the columns by growing Y-adic valuation. If some columns correspond to polynomials with the same Y-adic valuation, say δ, reorder the columns in such a way that the $\mathfrak{p}$-adic valuations of the coefficient of the monomial with valuation δ grow. Next if a is the smallest degree of some monomial, in first column, the degree a monomial can be removed in every other column by adding to it a $\widetilde{\mathcal{O}_K}$-multiple of first column. Iterating this process proves the claim.

In the end, after substituting y_{i2} for Y in row i, column l has only elements in $\mathfrak{p}^{l-1}$ because it consists of polynomials in y_{i2} where the first term is of degree $\geqslant l-1$ and $y_{i2} \in \mathfrak{p}$. Thus, the norm $N_{K/\mathbb{Q}}(\Delta_0)$ is divisible by $p^{E(E-1)/2}$. By choosing $m \geqslant E(E-1)/2$, we obtain that $N_{K/\mathbb{Q}}(\Delta)$ is divisible by $p^{E(E-1)/2}$.

Next, we estimate the height $H(\Delta)$. We have $H(x_{ij}) \leqslant B$, $i = 1, \dots, E$, $j = 1, 2$. Denote by S_E the permutation group of E elements and for $\sigma \in S_E$, $\varepsilon(\sigma)$ the signature of σ. We have

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

For v an archimedean place,

$$\begin{aligned} |\Delta|_v &\leqslant E! \max_{1 \leqslant j \leqslant E} (|x_{j1}|_v^{e_{11}} |x_{j2}|_v^{e_{12}}) \times \cdots \times \max_{1 \leqslant j \leqslant E} (|x_{j1}|_v^{e_{E1}} |x_{j2}|_v^{e_{E2}}) \\ &\leqslant E!\, B^{e_{11}+e_{12}} \times \cdots \times B^{e_{E1}+e_{E2}}. \end{aligned}$$

We obtain, if $\Delta \neq 0$:

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

To summarize, $N_{K/\mathbb{Q}}(\Delta)$ is divisible by $p^{E(E-1)/2}$ but

$$|N_{K/\mathbb{Q}}(\Delta)| \leqslant H(\Delta)^{\rho} \leqslant (E^E B^{E'})^{\rho}.$$

We have then proved that under the condition $p^{E(E-1)/2} > (E^E B^{E'})^{\rho}$, we have $\Delta = 0$. As $p \geqslant \mathcal{P}$ and Δ is an arbitrary minor of M, we conclude that, under the assumption of the statement, the rank of M is $\leqslant E-1$. □

3.2.3. Technical conclusion of Theorem 3.4

In order to apply Proposition 3.7, $\mathcal{P}$ should satisfy the condition

$$(*) \qquad \mathcal{P} > (E^{M_1} B^{M_2})^{\rho}.$$

where $M_1 := \frac{2}{(E-1)}$ and $M_2 := \frac{2E'}{E(E-1)}$. We refer to [31, §1.3.5] for the following estimates of M_1 and M_2:

$$M_1 \leqslant \frac{2}{dD} + \frac{2}{D^2} \text{ and } M_2 \leqslant \frac{1}{d} + \frac{6}{D}.$$

This leads to this sufficient condition for $(*)$:

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

Note that $E \leqslant 2dD$ and, by an elementary study of function, we have $(2dD)^{2(dD)^{-1}+2D^{-2}} \leqslant e^8$.

Choose

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

The number $\mathcal{P}$ satisfies $(**)$ and we have $\mathcal{P} \leqslant (2e^8 B^{d^{-1}+6D^{-1}})^{\rho}$.

To finish the proof of Theorem 3.4, it remains to estimate the number k. We have $\mathcal{P} > B^{d^{-1}}$ thus we assume that B is suitably large so that $\mathcal{P}$ is large enough to apply Lemma 3.6.

From Lemma 3.6 and Proposition 3.7, $k = 1 + k' = 1 + \sum_{i=1}^{r} k''_{\mathfrak{p}_i}$ where $k''_{\mathfrak{p}}$ is the number of sets of type $S(\underline{t})$ in $S(P, B, \mathfrak{p})$. Using the Lang–Weil bound [20, Theorem 1], [13, Theorem 5.4.1], we obtain

$$k''_{\mathfrak{p}} \leqslant d(p + 1 + (d-1)(d-2)\sqrt{p}) \leqslant 2d^3 p.$$

Conjoining this with the upper bound for $p = N_{K/\mathbb{Q}}(\mathfrak{p})$ from Lemma 3.6, we obtain:

$$k \leqslant k_1 d^3 h(B)^3 \frac{\mathcal{P}}{\log \mathcal{P}} \log\left(\frac{\mathcal{P}}{\log \mathcal{P}}\right)$$

where k_1 is a constant depending on K.

As $\log \mathcal{P} \geqslant \log(\mathcal{P}/\log \mathcal{P})$, we have,

$$\begin{aligned} k &\leqslant k_1 d^3 h(B)^3 \mathcal{P} \\ &\leqslant c_2 d^3 \log_2^3(2d^3 H(P) B^{d-1})(B^{d^{-1}+6D^{-1}})^{\rho} \end{aligned}$$

where c_2 is a constant depending on K.

3.3. Proof of Theorem C

Let $P(X_1, X_2)$ monic in X_2 and B as in Theorem C. We keep the notation of Section 3.1.1.

3.3.1. Non absolutely irreducible case

If P is not absolutely irreducible, the following statement directly provides a bound for $N(P,B)$.

PROPOSITION 3.9. — *Let $P(X_1,X_2) \in \mathcal{O}_K[X_1,X_2]$ of degree d, irreducible in $K[X_1,X_2]$ and not absolutely irreducible. Then $N(P,B) \leqslant 4d^4$.*

Proof. — We will count the number of $x_1 \in \mathcal{O}_K$ such that there exists $x_2 \in \mathcal{O}_K$ with $P(x_1,x_2)=0$. The same argument for x_2 will allow us to conclude.

Let (x_1,x_2) be a zero of P. Consider the factorization of P in $\overline{K}[X_1,X_2]$. If $P(x_1,x_2)=0$ for $(x_1,x_2) \in \mathcal{O}_K^2$ then $\varphi(x_1,x_2)=0$ for some irreducible factor φ in $\overline{K}[X_1,X_2]$, also monic in X_2 and of degree $< d$ (as P is not irreducible in $\overline{K}[X_1,X_2]$). We deduce that $\psi(x_1,x_2)=0$ for a K-conjugate ψ of φ over K distinct from φ (or else $P(X_1,X_2)$ would not be irreducible in $K[X_1,X_2]$). Furthermore, φ and ψ are not associated: if they were, as they are monic in X_2, they would be equal.

Conclude that the product $\varphi\psi$ divide P. Thus x_1 is a double root of the polynomial $P(X_1,x_2)$. The number of such x_1 is bounded by the number of roots of the polynomial $\mathrm{disc}_{X_2}(P)$ which is of degree $\leqslant (2d-1)d \leqslant 2d^2$.

With the same argument for x_2, we can say that the total number of points $(x_1,x_2) \in \mathcal{O}_K^2$ such that $P(x_1,x_2)=0$ is at most $2d^2.2d^2 = 4d^4$. Hence $N(P,B) \leqslant 4d^4$. □

3.3.2. The absolutely irreducible case

We assume $P(X_1,X_2)$ is irreducible in $\overline{K}[X_1,X_2]$ and is monic in X_2. For our applications, we need a bound for $N(P,B)$ which does not depend on the height $H(P)$ of P. We will use the following Siegel lemma for which we refer to [24, Chapter 6].

LEMMA 3.10 (Siegel lemma). — *Let K be a number field and N, M two integers such that $1 \leqslant M < N$. Let H_0 be a positive number and $a_{ij} \in K$, $1 \leqslant i \leqslant N$, $1 \leqslant j \leqslant M$, some algebraic numbers, not all zero, with height at most H_0. Then there exists a vector $\underline{x} \in \mathcal{O}_K^N \backslash \{0\}$ such that:*

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

and with $\max_{1\leqslant i\leqslant N} H(x_i) \leqslant C(CNH_0)^{M/(N-M)}$, where C is a constant depending only on K.

The constant C that appears below is the constant that appears in Lemma 3.10.

PROPOSITION 3.11. — *Let $P(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$ be an irreducible polynomial in $\overline{K}[X_1, X_2]$ of degree d and monic in X_2. Then*

$$N(P, B) \leqslant d^2 + 3 \text{ or } H(P) \leqslant C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}.$$

Proof. — Assume that $N(P, B) > d^2 + 3$. Set $R = d^2 + 4$, $N = (d+1)(d+2)/2$ and let $\underline{x_1}, \ldots, \underline{x_R}$ be R zeroes of P such that $H(x_{ij}) \leqslant B$ $(i = 1, \ldots, R,\ j = 1, 2)$.

The total number of monomials of degree $\leqslant d$ in the indeterminates X_1, X_2 is N. Let $A = (a_{i,j})$ be the $R \times N$ matrix of which the i-th line is composed of these N monomials evaluated at x_{i1}, x_{i2} $i = 1, \ldots, R$. The one column matrix $c \in \mathcal{O}_K^N$, consisting of the coefficients of P is a non trivial solution of the system $AX = 0$.

As $Ac = 0$, the rank of A, say M, is $< N$. Up to re-numbering the lines, we may assume that the system $AX = 0$ is equivalent to its M first lines.

It follows from Lemma 3.10 that the system has a non-zero solution $c' \in \mathcal{O}_K^N$ satisfying

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

(note that $H(a_{i,j})$ is bounded by B^d, $1 \leqslant i \leqslant R$, $1 \leqslant j \leqslant N$).

Let $Q(X_1, X_2)$ be the polynomial whose coefficients are the elements of c'. Q is a non-zero polynomial of degree $\leqslant d$, its coefficients are in $\mathcal{O}_K$, and it satisfies $Q(x_{i1}, x_{i2}) = 0$ $(i = 1, \ldots, R)$.

By construction, the polynomials P and Q have at least $d^2 + 4$ zeroes in common and are both of degree $\leqslant d$. By the Bezout theorem, these two polynomials are not relatively prime in $\overline{K}[X_1, X_2]$. As P is irreducible and of degree d, we have $Q = aP$ for some $a \in K$. Furthermore, as P is monic in X_2, then $a \in \mathcal{O}_K$ and $H(P) \leqslant H(Q)$. Thus we have

$$H(P) \leqslant H(Q) \leqslant \max_{1 \leqslant i \leqslant N} H(c_i') \leqslant C(CNB^d)^{M/(N-M)} \leqslant C(CNB^d)^N.$$

Note finally that $N \leqslant 4d^2$. Hence

$$H(P) \leqslant C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}. \qquad \square$$

We can now finish the proof of Theorem C. We deduce from Theorem 3.4, combined with the Bezout theorem that

$$N(P,B) \leqslant \sum_{i=1}^{k} \deg(P)\deg(P_i) \leqslant kdD$$
$$\leqslant c_2 d^4 D \log^3(d^3 H(P) B^{d-1})(B^{d^{-1}+6D^{-1}})^{\rho}.$$

We recall that D has to be chosen $\geqslant d$. We take $D = [d\log(B)+1]$. We have $B^{6(d\log(B))^{-1}} \leqslant 2^9$. We obtain:

$$N(P,B) \leqslant k_1 d^5 \log^3(2d^3 H(P) B^{d-1}) B^{\rho/d}\log(B)$$

where k_1 depends on K.

The bound $H(P) \leqslant C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}$ from Proposition 3.11 gives:

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

Finally we obtain:

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

3.4. Proof of Corollary C

We work now with a polynomial $P(T,Y) \in \mathcal{O}_K[T,Y]$ monic in Y and irreducible in $K[T,Y]$. We will estimate the number $N_T(P,B)$ of $t \in \mathcal{O}_K$ such that $H(t) \leqslant B$ and the specialized polynomial $P(t,Y)$ has a root y in K (or, equivalently, in $\mathcal{O}_K$ as $P(T,Y)$ is monic in Y). We recall that m, n and d are respectively the degree in T, Y and the total degree of P.

The following lemma based on the Liouville inequality, shows how to bound $H(y)$.

LEMMA 3.12. — *For all $t \in \mathcal{O}_K$, the height of any $y \in \mathcal{O}_K$ such that $P(t,y) = 0$ is bounded by $2(m+1)H(P)H(t)^m$.*

Proof. — We will use the Liouville inequality given in this form: if $Q \in \mathcal{O}_K[X]$ is monic and $x \in \mathcal{O}_K$ with $Q(x) = 0$, then $H(x) \leqslant 2H(Q)$. Indeed, the result is trivial if $x = 0$. For $x \neq 0$, we will show that for every archimedean place v, $|x|_v \leqslant 2H_v(Q)$. Fix v an archimedean place. If $|x|_v = 1$ it is trivial, else we write $Q(X) = X^n + a_1 X^{n-1} + \cdots + a_0$ and we deduce from $x^n + a_1 x^{n-1} + \cdots + a_0 = 0$ that

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

As $|x|_v > 1$ and $H_v(Q) \geqslant 1$, we deduce

$$1 \leqslant H_v(Q)\left(\frac{1}{|x|_v} + \cdots + \frac{1}{|x|_v^n}\right) < \frac{H_v(Q)}{|x|_v - 1}.$$

This yields $|x|_v \leqslant H_v(Q) + 1 \leqslant 2H_v(Q)$ and thus $H(x) \leqslant 2H(Q)$.

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

$$\deg(a_i(T)) \leqslant m \text{ and } H(a_i(T)) \leqslant H(P),\ i = 1, \ldots, n.$$

For $t \in \mathcal{O}_K$, the height of every solution $y \in \mathcal{O}_K$ of the equation $P(t,Y) = 0$ satisfies:

$$H(y) \leqslant 2H(P(t,Y)).$$

We have $H(P(t,Y)) = H(a_0(t), \ldots, a_n(t)) = \max_{1\leqslant i\leqslant n} \max_{v/\infty} |a_i(t)|_v$ and for an archimedean place v,

$$\begin{aligned} |a_i(t)|_v &\leqslant (m+1) \max_{1\leqslant j\leqslant n} (|a_{ij}|_v)|t|_v^m \\ &\leqslant (m+1)H_v(P)|t|_v^m. \end{aligned}$$

This yields

$$\begin{aligned} \max_{1\leqslant i\leqslant n} \max_{v/\infty} |a_i(t)|_v &\leqslant (m+1) \max_{v/\infty} H_v(P) \max_{v/\infty} |t|_v^m \\ &\leqslant (m+1)H(P)H(t)^m. \end{aligned}$$

This concludes the proof. □

Lemma 3.12 gives $N_T(P,B) \leqslant N(P,B')$ with $B' = 2(m+1)H(P)B^m$. However, in order to obtain the right conclusion, we will apply this inequality, not to P, but to some polynomial Q deduced from P by some change of variables. More precisely, we proceed as follows.

Proof of Corollary C. — Recall that $H = \max(e^e, H(P))$. Let $L_1 = \log(H)$ and $L_2 = \log(\log(H)) \geqslant 1$. We have $L_2 \geqslant 1$. As $P(T,Y)$ is monic in Y, we have $d \leqslant n + m - 1$. We may and will assume that $m \geqslant 1$ and $n \geqslant 1$. In particular $d \leqslant mn < mnL_1/L_2$.

Consider the polynomial

$$Q(T,Y) = P(T, T^E + Y)$$

where $E = [mn\frac{L_1}{L_2}] + 1 \leqslant 2mnL_1$. This polynomial is of degree $d' \in [nE, nE+m]$ and we have $N_T(P,B) = N_T(Q,B)$.

Using the inequality

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

for every zero (t,y') of Q such that $H(t) \leqslant B$, we have for suitably large B,

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

Thus, defining $B'' = 3(m+1)HB^E$, we have

$$N_T(Q,B) \leqslant N(Q,B'').$$

Now use Theorem C with Q and B'':

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

We have $E \leqslant 2d^2 \log H \log B$, and as $1/nE \leqslant L_2/L_1$, we have $H^{1/nE} \leqslant log(H)$. Thus

$$\begin{aligned} &N(Q,B'') \\ &\quad\leqslant c_5(3d^3\log H\log B)^{14}(4d^3\log H\ \log B)^4(3^\rho d^\rho \log^\rho H)\log^\rho BB^{\rho/n}. \end{aligned}$$

Finally, we obtain

$$N_T(P,B) \leqslant c_6 d^{54+\rho}(\log H)^{18+\rho}B^{\rho/n}\,(\log B)^{18+\rho}. \qquad \square$$

4. Proof of Theorem 2.1 and Theorem 2.2

4.1. Proof of Theorem 2.1

Return to the situation of Section 2.1: a regular Galois extension $F/K(T)$ of group G is given. Fix a good prime $\mathfrak{p}$ for $F/K(T)$ and an associated union $\mathcal{F}_\mathfrak{p}$ of conjugacy classes of G. The following result generalizes [8, Proposition 5.1], proved in the case $K=\mathbb{Q}$. We say that $t_0 \notin \mathfrak{t}$ modulo $\mathfrak{p}$ if t_0 does not meet any of the branch point of F_{t_0}/K modulo $\mathfrak{p}$.

Proposition 4.1. — *The set*

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

is a union of cosets modulo $\mathfrak{p}$ *and the number* $\nu(\mathcal{F}_\mathfrak{p})$ *of these cosets satisfies*

$$\begin{aligned} \nu(\mathcal{F}_\mathfrak{p}) &\geqslant \frac{|\mathcal{F}_\mathfrak{p}|}{|G|} \times (q+1-2g\sqrt{q}-|G|(r+1)) \\ \nu(\mathcal{F}_\mathfrak{p}) &\leqslant \frac{|\mathcal{F}_\mathfrak{p}|}{|G|} \times (q+1+2g\sqrt{q}) \end{aligned}$$

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

We omit the proof which merely consists in changing the prime number p to the prime ideal $\mathfrak{p}$ in the proof of [8, Proposition 5.1]. From classical results due to Grothendieck–Beckmann (e.g using the form given in [21]), if $t_0 \notin \mathfrak{t} \mod \mathfrak{p}$ then $\mathfrak{p}$ is unramified in F_{t_0}/K. This last statement is needed to prove Theorem 2.1 and is also used in the proof of Proposition 4.1.

Consider the prime numbers p_0 and p_{-1} given in Section 2. Let $x > 0$ be a real number. Let $S_{[p_0,x]}$ be the set of all primes of K over the interval $[p_0, x]$ and let $\mathcal{F}_{[p_0,x]}$ be a Frobenius data on $S_{[p_0,x]}$. Next, with $S_{]p_{-1},p_0[}$ consisting of the prime ideals over the interval $]p_{-1}, p_0[$, set $S_x = S_{[p_0,x]} \cup S_{]p_{-1},p_0[}$.

Consider the Frobenius data $\mathcal{F}_x$ on S_x obtained by adding to the Frobenius data $\mathcal{F}_{[p_0,x]}$ some local conditions over the primes of K over the interval $]p_{-1}, p_0[$ in this manner: to every conjugacy class of G, we associate a prime $\mathfrak{p} \in S_{]p_{-1},p_0[}$ in such a way that every conjugacy class of G appears in the Frobenius data $\mathcal{F}_x$; for the other ideals in $S_{]p_{-1},p_0[}$, we take $\mathcal{F}_\mathfrak{p} = G$ ($\mathcal{F}_\mathfrak{p}$ can be chosen arbitrary). Set $I = \prod_{\mathfrak{p}\in S_x} \mathfrak{p}$ and denote by $\{p_1, \dots, p_n\}$ the set of prime numbers in the interval $]p_{-1}, x]$.

LEMMA 4.2. — *We have* $I = \prod_{1\leqslant i\leqslant n}(p_i\mathcal{O}_K)$ *and* $I \cap \mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}$.

Proof. — The set S_x is the set of all prime ideals of K over $p_1, \dots, p_n$. Using that all primes $\mathfrak{p} \in S_x$ are unramified in K from the definition of p_{-1}, we obtain

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

For $i \in \{1, \dots, n\}$, we have $p_i\mathcal{O}_K \cap \mathbb{Z} = p_i\mathbb{Z}$. The next argument shows that

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

Inclusion $\supset$ is obvious: $p_1 \dots p_n \in (p_1\mathcal{O}_K) \dots (p_n\mathcal{O}_K) \cap \mathbb{Z}$. As $\mathbb{Z}$ is a P.I.D, the ideal $(p_1\mathcal{O}_K) \dots (p_n\mathcal{O}_K) \cap \mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$. From $(p_1\mathcal{O}_K) \dots (p_n\mathcal{O}_K) \cap \mathbb{Z} \subset p_i\mathcal{O}_K \cap \mathbb{Z}$, we deduce that $p_i \mid a$, $i = 1, \dots, n$. As $p_1, \dots, p_n$ are distinct, $p_1 \dots p_n \mid a$ whence the desired inequality. □

Denote the intersection $\bigcap_{\mathfrak{p}\in S_x} \tau(\mathcal{F}_\mathfrak{p})$ by $\tau(S_x, \mathcal{F}_x)$. It follows from the Chinese remainder Theorem that $\tau(S_x, \mathcal{F}_x)$ contains $\mathcal{N}(S_x, \mathcal{F}_x) = \prod_{\mathfrak{p}\in S_x} \nu(\mathcal{F}_\mathfrak{p})$ cosets modulo I. The following proposition is a more precise and more technical form of Theorem 2.1. It involves the following notation.

- for a Frobenius data $\mathcal{F}_S = (\mathcal{F}_\mathfrak{p})_{\mathfrak{p}\in S}$, as in Section 2.1, the density of $\mathcal{F}_S$, denoted by $\chi(\mathcal{F}_S)$, is the product of all $|\mathcal{F}_\mathfrak{p}|/|G|$ for $\mathfrak{p} \in S$,
- for a positive real number x, the number $\pi(x)$ is the number of primes $\leqslant x$ and $\Pi(x)$ is the product of all prime numbers $p \leqslant x$. Recall that $\pi(x) \sim x/\log x$ and $\log(\Pi(x)) \sim x$ when $x \to +\infty$.

- for a set S of prime ideals in K, the number $\Pi(S)$ is the product of all primes numbers p such that $p = p_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \in S$[(5)].

PROPOSITION 4.3.

(1) *If $t_0 \in \mathcal{O}_K$ is any representative of one of the cosets modulo I in $\tau(S_x, \mathcal{F}_x)$ then $\mathrm{Gal}(F_{t_0}/K) = G$ and $t_0 \in \tau(\mathcal{F}_{\mathfrak{p}})$ for each $\mathfrak{p} \in S_x$.*

(2) *If x is suitably large,*

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

(3) *Fix a $\mathbb{Z}$-basis $\underline{e} = (e_1, \dots, e_n)$ of $\mathcal{O}_K$ and denote by $H(\underline{e})$ the height of $\underline{e}$. For every coset modulo I in $\tau(S_x, \mathcal{F}_x)$, there exists a representative $t_0 \in \mathcal{O}_K$ of height $H(t_0) \leqslant \frac{\rho H(\underline{e})}{\Pi(p_{-1})}\Pi(x)$.*

Proof.

(1). — From the definition of $\tau(S_x, \mathcal{F}_x)$, we have that $\mathrm{Frob}_{\mathfrak{p}}(F_{t_0}/K) \in \mathcal{F}_{\mathfrak{p}}$ for every $\mathfrak{p} \in S_x$. From the Frobenius condition on the primes of $S_{]p_{-1},p_0[} \subset S_x$, the subgroup $\mathrm{Gal}(F_{t_0}/K) \subset G$ meets all conjugacy classes of G, so it is the whole group G by a lemma of Jordan [17].

(2). — Using Proposition 4.1, we have, for $q = N(\mathfrak{p})$ with $\mathfrak{p} \in S_x$.

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

As in [8], using that $g < r|G|/2 - 1$ (if $|G| > 1$; from the Riemann–Hurwitz formula) and that $q \geqslant r^2|G|^2$ for each $\mathfrak{p} \in S_x$ (from the choice of p_{-1}), we have

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

As all primes $p \in]p_{-1}, x]$ are unramified, we have $\prod_{\mathfrak{p}\in S_x} N(\mathfrak{p}) = \Pi(S_x)^{\rho} = \left(\frac{\Pi(x)}{\Pi(p_{-1})}\right)^{\rho}$ and $\mathrm{card}(S_x) \leqslant \rho\pi(x)$. Hence, we obtain

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

(5) Recall that $p_{\mathfrak{p}}$ denote the prime number such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

(3). — We have $\mathcal{O}_K = \{\sum_{i=1}^{\rho} m_i \cdot e_i \mid m_i \in \mathbb{Z}\ i = 1, \dots, \rho\}$ and so

$$\mathcal{O}_K/I = \left\{ \sum_{i=1}^{\rho} \overline{m_i} \cdot \overline{e_i} \,\middle|\, \overline{m_i} \in \mathbb{Z}/\mathbb{Z} \cap I \ i = 1, \dots, \rho \right\}.$$

From Lemma 4.2, $\mathbb{Z}/\mathbb{Z}\cap I = \mathbb{Z}/\Pi(S_x)\mathbb{Z}$. Every coset modulo I in $\tau(S_x, \mathcal{F}_x)$ has a representative $t = \sum_{i=1}^{\rho} m_i.e_i$ in $\mathcal{O}_K$ such that $1 \leqslant m_i \leqslant \Pi(S_x)$, $i = 1, \dots, \rho$.

Next we have for each archimedean place v,

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

Whence $H(t) \leqslant \rho\Pi(S_x)H(e_1, \dots, e_\rho) = \frac{\rho H(\underline{e})}{\Pi(p_{-1})}\Pi(x)$. □

Proof of Theorem 2.1. — For a positive number B, we let $x = p_B$ be the biggest prime number such that $\Pi(p_B) \cdot p_B \leqslant B$. Denote by q_B the next prime number. As $\Pi(q_B) = \Pi(p_B) \cdot q_B$, we have

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

the last inequality uses the classical estimate $q_B \leqslant 2p_B$.

Taking the log of these terms yields

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

which shows that

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

Take a number B which satisfies the following conditions:

- $\frac{\log B}{2} \leqslant p_B \leqslant 2\log B$,
- $p_B \geqslant \frac{\rho H(\underline{e})}{\Pi(p_{-1})}$,
- $\pi(p_B) \leqslant 2\log B/\log\log B$,
- p_B is large enough so that Proposition 4.3 can be applied with $x = p_B$.

It suffices to take B suitably large depending on K, $H(\underline{e})$, $\Pi(p_{-1})$.

As in Theorem 2.1, let S_B be the set of primes of K over the interval $[p_0, \log B/2]$. The interval $[p_0, \frac{\log B}{2}]$ is contained in the interval $[p_0, p_B]$ of Proposition 4.3. Let $\mathcal{F}_B$ be a Frobenius data on S_B. Extend it to a Frobenius data $\mathcal{F}_x = \mathcal{F}_{p_B}$ on the set $S_x = S_{p_B}$ of primes over the interval $[p_{-1}, p_B]$ (by defining $\mathcal{F}_\mathfrak{p}$ arbitrarily for every $\mathfrak{p}$ over some prime in $[\frac{\log B}{2}, p_B]$). The Frobenius data is extended to primes over $]p_{-1}, p_0]$ as explained above Lemma 4.2.

Next, use Proposition 4.3 with $x = p_B$, the set S_{p_B} and the Frobenius data $\mathcal{F}_{p_B}$. Note that the upper bound for $H(t_0)$ in Proposition 4.3(3) is $\leqslant p_B\Pi(p_B)$ and so $\leqslant B$. Conclude from Proposition 4.3 (2) that the number $\mathcal{N}$ of $t_0 \in \mathcal{O}_K$ such that $\mathrm{Gal}(F_{t_0}/K) = G$, $H(t_0) \leqslant B$ and for all $\mathfrak{p} \in S_B$, $\mathrm{Frob}_{\mathfrak{p}}(\mathrm{F_{t_0}/K}) \in \mathcal{F}_{\mathfrak{p}}$ satisfies

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

Furthermore, we have

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

and

- $\Pi(p_B)^\rho = \frac{(4p_B^2\Pi(p_B))^\rho}{(2p_B)^{2\rho}} \geqslant \frac{B^\rho}{(2p_B)^{2\rho}}$,
- $(2p_B)^{2\rho} \leqslant c_1^{\log B/\log\log B}$ for a constant c_1 depending on $F/K(T)$.

Finally, using that $\pi(p_B) \leqslant 2\rho \log B/\log\log B$, we obtain

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

for a constant c depending on $F/K(T)$. □

4.2. Proof of Theorem 2.2

The proof combines the diophantine results of Section 3 with the following result.

THEOREM 4.4. — *Let $F/K(T)$ be a regular Galois extension of group G. There exists an integer $N \leqslant |\mathrm{Aut}(G)|$ and some polynomials $\widetilde{P}_1, \dots, \widetilde{P}_N \in \mathcal{O}_K[U,T,Y]$, irreducible in $\overline{K(U)}(T)[Y]$, of degree $\deg_Y(\widetilde{P}_i) = |G|$, monic in Y and a finite set $\varepsilon \subset K$ such that the following holds:*

- *all the affine curves $\widetilde{P}_i(U,t,y) = 0$ (over $\overline{K(U)}$) are of the same genus g_F,*
- *for every $u_0 \in \mathcal{O}_K\backslash\varepsilon$, $\widetilde{P}_i(u_0,T,Y)$ is irreducible in $\overline{K}(T)[Y]$ and the affine curve $\widetilde{P}_i(u_0,t,y)$ is of genus g_F, $i = 1,\dots,N$,*
- *for every $t_0 \in \mathcal{O}_K$ which is not a branch point of $F/K(T)$,*

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

This result is the special case of [9, Theorem 2.16] for which $F/K(T) = L/K(T)$. Each polynomial $\widetilde{P}_i$ is an affine model of the $K(U)$-regular cover $\widetilde{f}_i : \widetilde{X}_i \to \mathbb{P}^1_{K(U)}$ that appears there and is obtained somehow by twisting

f_i by itself ($i = 1, \dots, N$). Except for a finite number of them, the K-points on $\widetilde{X}_i|_{u_0}$ that appear in [9] correspond to the zeroes (t_0, y_0) of the polynomial $\widetilde{P}_i(u_0, T, Y)$, $i = 1, \cdots N$. That $N \leqslant |\mathrm{Aut}(G)|$ is explained in the proof of [9, Theorem 2.16].

Diophantine estimates. — *The constants c_i below, $i = 1, 2, 3$ depend only on the extension $F/K(T)$. We have for $u_0 \in \mathcal{O}_K$ such that $H(u_0) \leqslant B$ and for $i = 1, \dots, N$:*

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

For real numbers $g, D, H, B \geqslant 0$ and $d_Y \geqslant 2$, consider all polynomials $Q \in \mathcal{O}_K[T, Y]$ monic in Y and irreducible in $\overline{K}(T)[Y]$ such that

- $\deg_Y(Q) = d_Y$
- $\deg(Q) \leqslant D$
- $H(Q) \leqslant H$
- the curve $Q(t, y) = 0$ is of genus $\leqslant g$.

For each such polynomial Q, the number of $t \in \mathcal{O}_K$ of height $H(t) \leqslant B$ and such that $Q(t, y) = 0$ for some $y \in \mathcal{O}_K$ is finite. Denote by $Z(g, D, d_Y, H, B)$ the maximal cardinality of all these finite sets when Q ranges over all polynomials satisfying the above conditions.

As in Theorem 2.2, let B be a positive number and $\mathcal{H} \subset \mathcal{O}_K$ be a subset consisting of t_0 such that $\mathrm{Gal}(F_{t_0}/K) = G$ and $H(t_0) \leqslant B$. From Theorem 4.4, for every $u_0 \in \mathcal{H}$, the number of $t_0 \in \mathcal{H}$ such that $F_{t_0}/K = F_{u_0}/K$ is $\leqslant N\, Z(g_F, c_1, |G|, c_2 B^{c_3}, B)$. Let E be the cardinality of ε of Theorem 4.4, we obtain

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

From Corollary C, we have for suitably large B

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

and so finally, we obtain

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

BIBLIOGRAPHY

[1] F. Barroero, "Counting algebraic integers of fixed degree and bounded height", *Monatsh. Math.* **175** (2014), no. 1, p. 25-41.

[2] Y. Bilu, "Counting number fields in fibers (with an appendix by Jean Gillibert)", *Math. Z.* **288** (2018), no. 1-2, p. 541-563.

[3] E. Bombieri & J. Pila, "The number of integral points on arcs and ovals", *Duke Math. J.* **59** (1989), no. 2, p. 337-357.

[4] N. Broberg, "A note on a paper by R. Heath-Brown: "The density of rational points on curves and surfaces" [*Ann. Math. (2)* **155** (2002), no. 2, p. 553–595; MR1906595]", *J. Reine Angew. Math.* **571** (2004), p. 159-178.

[5] H. Chen, "Explicit uniform estimation of rational points II. Hypersurface coverings", *J. Reine Angew. Math.* **668** (2012), p. 89-108.

[6] P. Dèbes, "Hilbert subsets and S-integral points", *Manuscr. Math.* **89** (1996), no. 1, p. 107-137.

[7] ———, "Méthodes topologiques et analytiques en théorie inverse de Galois: théorème d'existence de Riemann", in *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, Sémin. Congr., vol. 5, Soc. Math. France, Paris, 2001, p. 27-41.

[8] ———, "On the Malle conjecture and the self-twisted cover", *Israel J. Math.* **218** (2017), no. 1, p. 101-131.

[9] ———, "Groups with no parametric Galois realizations", *Ann. Sci. Éc. Norm. Supér. (4)* **51** (2018), no. 1, p. 143-179.

[10] P. Dèbes & N. Ghazi, "Galois covers and the Hilbert–Grunwald property", *Ann. Inst. Fourier* **62** (2012), no. 3, p. 989-1013.

[11] C. Demarche, G. Lucchini Arteche & D. Neftin, "The Grunwald problem and approximation properties for homogeneous spaces", *Ann. Inst. Fourier* **67** (2017), no. 3, p. 1009-1033.

[12] R. Dvornicich & U. Zannier, "Fields containing values of algebraic functions", *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **21** (1994), no. 3, p. 421-443.

[13] M. D. Fried & M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 11, Springer-Verlag, Berlin, 1986, xviii+458 pages.

[14] D. Harari, "Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini", *Bull. Soc. Math. France* **135** (2007), no. 4, p. 549-564.

[15] Y. Harpaz & O. Wittenberg, "Zéro-cycles sur les espaces homogènes et problème de Galois inverse", `https://arxiv.org/abs/1802.09605`, 2018.

[16] D. R. Heath-Brown, "The density of rational points on curves and surfaces", *Ann. Math. (2)* **155** (2002), no. 2, p. 553-595.

[17] C. Jordan, "Recherches sur les substitutions", *J. Liouville* **17** (1872), p. 351-367.

[18] J. Klüners, "Asymptotics of number fields and the Cohen–Lenstra heuristics", *Jux* **18** (2006), no. 3, p. 607-615.

[19] J. Klüners & G. Malle, "Counting nilpotent Galois extensions", *J. Reine Angew. Math.* **572** (2004), p. 1-26.

[20] S. Lang & A. Weil, "Number of points of varieties in finite fields", *Amer. J. Math.* **76** (1954), p. 819-827.

[21] F. Legrand, "Specialization results and ramification conditions", *Israel J. Math.* **214** (2016), no. 2, p. 621-650.

[22] G. Malle, "On the distribution of Galois groups", *J. Number Theory* **92** (2002), no. 2, p. 315-329.

[23] ———, "On the distribution of Galois groups. II", *Experiment. Math.* **13** (2004), no. 2, p. 129-135.

[24] M. R. Murty & P. Rath, *Transcendental numbers*, Springer, New York, 2014, xiv+217 pages.

[25] J. Neukirch, "On solvable number fields", *Invent. Math.* **53** (1979), no. 2, p. 135-164.

[26] D. J. Saltman, "Generic Galois extensions and problems in field theory", *Adv. in Math.* **43** (1982), no. 3, p. 250-283.

[27] P. Samuel, *Théorie algébrique des nombres*, Hermann, 1967, 130 pages.

[28] S. H. Schanuel, "Heights in number fields", *Bull. Soc. Math. France* **107** (1979), no. 4, p. 433-449.

[29] A. Schinzel & U. Zannier, "The least admissible value of the parameter in Hilbert's irreducibility theorem", *Acta Arith.* **69** (1995), no. 3, p. 293-302.

[30] J.-P. Serre, *Topics in Galois theory*, second ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., 2008, with notes by Henri Darmon, xvi+120 pages.

[31] Y. Walkowiak, "Théorème d'irréductibilité de Hilbert effectif", *Acta Arith.* **116** (2005), no. 4, p. 343-362.

[32] S. Wang, "A counter-example to Grunwald's theorem", *Ann. Math. (2)* **49** (1948), p. 1008-1009.

[33] D. J. Wright, "Distribution of discriminants of abelian extensions", *Proc. London Math. Soc. (3)* **58** (1989), no. 1, p. 17-50.

[34] U. Zannier, "On the number of times of root of $f(n,x) = 0$ generates a field containing a given number field", *J. Number Theory* **72** (1998), no. 1, p. 1-12.

Manuscrit reçu le 13 avril 2021,
révisé le 18 novembre 2021,
accepté le 16 février 2022.

François MOTTE
f.e.motte@gmail.com
Laboratoire Paul Painlevé
Mathématiques
Université Lille
59655 Villeneuve d'Ascq Cedex (France)