ON THE MALLE CONJECTURE AND THE GRUNWALD PROBLEM

François Emmanuel Motte

ON THE MALLE CONJECTURE
AND THE GRUNWALD PROBLEM

FRANÇOIS MOTTE

ABSTRACT. We contribute to the Malle conjecture on the number $N(K, G, y)$ of finite Galois extensions E of some number field K of finite group G and of discriminant of norm $|N_{K/\mathbb{Q}}(d_E)| \leq y$. For every group G and every number field K containing a certain number field K_0, we establish this lower bound : $N(K, G, y) \geq y^{\alpha(G)}$ for $y \gg 1$ and some specific exponent $\alpha(G)$ depending on G. 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 F_{t_0}/K and not only the specialization points t_0, and which provides some control of $|N_{K/\mathbb{Q}}(d_{F_{t_0}})|$. 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 G.

1. INTRODUCTION

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 discriminant $d_{E/K}$ of norm $N_K(d_{E/K})$ bounded by y. It is well-known that this number is finite. There is the following conjecture [Mal02] :

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

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

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 in his conjecture :
$a(G) = (|G|(1 - 1/l))^{-1}$ 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 [Wri89]. Malle worked on the resoluble case [Mal02], [Mal04], 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 [KM04]. Klüners also proved the lower bound part for dihedral groups of order $2p$ where p is an odd prime [Klü06]. 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

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

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 ($n \geq 1$) and many simple groups : A_n ($n \geq 5$), 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 also be given explicitly. It is smaller than $a(G)$. We explain why in §2.3.

Theorem A generalizes a previous result of Dèbes [Dèb17] who proved the special case $K = \mathbb{Q}$ and when G is supposed to be a regular Galois group over $\mathbb{Q}$.

There is a more general conjecture for not necessarily Galois extensions which we discuss in §2.5. The same lower bound holds for this general form of the conjecture (theorem 2.6).

1.2. The Grunwald problem. Furthermore, our approach makes it possible to impose some local constraints to the extensions E/K that we count. This relates to the famous Grunwald problem.

For every prime $\mathfrak{p}$ of 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* $\left(G, (L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p} \in S}\right)$.

The case of abelian, and more generaly solvable groups, has been studied by Grunwald, Wang and Neukirch [Wan48] [Neu79] : in particular, the answer is positive if G is of odd order. 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 [Wan48]. 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 [Har07], [DG12], [DLAN17]. It was recently established for hypersolvable groups (e.g. nilpotent) over any number field [HW18]. For non solvable groups, a result due to Dèbes and Ghazi [DG12] shows that any Grunwald problem $(L^{\mathfrak{p}}/K_{\mathfrak{p}})_{\mathfrak{p} \in S}$ (with $S \cap S_{exc} = \emptyset$), 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 [DG12]. 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 a *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. 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 $S \cap S_{exc} = \emptyset$, 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 $(G, (L^{\mathfrak{p}} / K_{\mathfrak{p}})_{\mathfrak{p} \in S})$. Furthermore, one can take $M = K$ if G is a regular Galois group over K.*

In particular, for all non solvable groups known to be regular groups over $\mathbb{Q}$, any unramified Grunwald problem has infinitely many solutions over $\mathbb{Q}$.

1.3. Diophantine results. Both theorem A and theorem B are special cases of a more general result, theorem AB, which will be stated in §2.2. 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, for theorem A, to count the number of these specialized extensions and for theorem B, to show that some local conditions can be prescribed to these extensions. We will follow a method developed in [DG12] and [Dèb17] over $\mathbb{Q}$ and which has an important diophantine part. A major tool will be an estimate of the number $N(F, B)$ of rational points on a curve of height bounded by a number B. This is a classical problem, for which Heath-Brown introduced a method in 2002 [HB02], which was refined for curves by Walkowiak [Wal05], both over $\mathbb{Q}$. In this context we will prove the following result, which extends Walkowiak's result to any number field and may be interesting for its own sake.

Denote by O_K the ring of integers of K. We will use the following height for number $x \in O_K$, sometimes called the *house* of x :
$$H(x) = \max(|x_1|, \cdots, |x_d|)$$
where $x_1, \cdots, x_d$ are the $\mathbb{Q}$-conjugates of x (see §3 for more on heights).

Consider a polynomial $F(X_1, X_2) \in O_K[X_1, X_2]$, irreducible in $K[X_1, X_2]$, monic in X_2.

For $B > 0$, define
$$N(F, B) = \#\{(x_1, x_2) \in O_K^2 \ : \ F(x_1, x_2) = 0, \ H(x_1) \leq B, \ H(x_2) \leq B\}.$$

Theorem C. *If B is suitably large (depending on K), we have*
$$N(F, B) \leq c \deg(F)^{14} (\log B)^4 B^{[K:\mathbb{Q}] / \deg(F)}$$
where c is a constant depending on K.

Having such an estimate available for any number field is crucial for our applications. Proof of theorem C is inspired by Walkowiak's work over $\mathbb{Q}$ but has to deal with several new phenomena occuring on an arbitrary number field.

---

1. Definition of specialized extensions is recalled in §2.

Theorem C has the following consequence more in the spirit of *Hilbert's Irreducibility Theorem* and which we will use for our results.

Corollary C. *Let $F(T,Y) \in O_K[T,Y]$ irreducible and monic in Y. There exist some positive constants $a_1, ..., a_4$ depending on K such that for all suitably large B, the number $N_T(F,B)$ of $t \in O_K$ with $H(t) \leq B$ and such that $F(t,Y)$ has a root in K satisfies*

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

where $H(F)$ is the height of F.[2]

Recall that the total number of $t \in O_K^2$ with $H(t) \leq B$ is asymptotic to $B^{[K:\mathbb{Q}]}$ (up to some multiplicative constant and a $\log B$ factor) [Sch79] [Bar14].

The paper is organized as follows. In §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 §2. In §2.2, theorem AB is stated. In §2.3, theorem AB is shown to imply theorems A and theorem B. In §2.4, theorem AB is proved assuming theorems 2.1 and 2.2. §3 is dedicated to the proof of theorem C and corollary C. Finally, theorems 2.1 and 2.2 are proved in §4.

The following figure summarizes the structure of our approach.

---
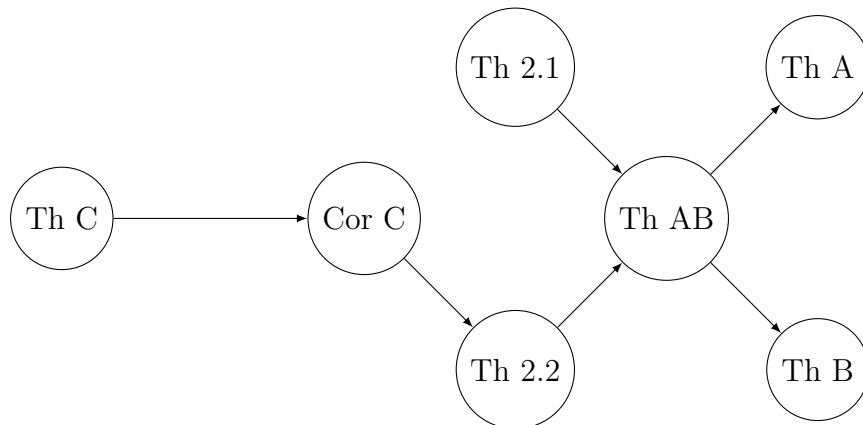
2. see §3 for more details on the height $H(F)$.

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 §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 $P(T, Y) \in O_K[T, Y]$ 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 $K[T]$, 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 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 $p_{-1} \geq r^2 g^2$ and such that every prime number p which is ramified in $K/\mathbb{Q}$ is $\leq p_{-1}$ 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 $B > 0$, 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 $t_0 \in O_K$ of height $H(t_0) \leq B$ such that*
— *the specialized extension F_{t_0}/K is of group G,*
— $\mathrm{Frob}_\mathfrak{p}(F_{t_0}/K) \in \mathcal{F}_\mathfrak{p}$ *for every $\mathfrak{p} \in S_B$.*

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

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 in [Dèb17]. We generalize it to arbitrary number fields.

Theorem 2.2 (*Hilbert-Malle type*)**.** *Let $B > 0$ be a real number. Let $\mathcal{H} \subset O_K$ be a subset consisting of t_0 such that $\operatorname{Gal}(F_{t_0}/K) = G$ and $H(t_0) \leq B$. 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 $E, \gamma \geq 0$ depending on $F/K(T)$ such that if B is suitably large (depending on $F/K(T)$), we have*

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

2.2. A unified version of theorem A and theorem B. Retain the notation and assumptions of §2. Fix an affine model $P(T, Y) \in O_K[T, Y]$ 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 [Dèb17], 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 $|N_{K/\mathbb{Q}}(d_{F_{t_0}/K})| \leq y$ and such that for every $\mathfrak{p} \in S$, F_{t_0}/K is unramified in $\mathfrak{p}$ and $\operatorname{Frob}_{\mathfrak{p}}(F_{t_0}/K) \in \mathcal{F}_{\mathfrak{p}}$.

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 $\mathbf{t} = \{t_1, \cdots, t_r\}$ 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 [DG12] and [Leg16] 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 $p \in [p_0, \dfrac{\log y}{2\rho\delta}]$ 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*

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

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

Set $\delta^- = \dfrac{\delta + \delta_P}{2}$ (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 $t_0 \in O_K$ such that $\Delta_P(t_0) \neq 0$, $H(t_0) \leq B$ and F_{t_0}/K is Galois of group G satisfy $|N_{K/\mathbb{Q}}(d_{F_{t_0}/K})| \leq y$.*

Proof. The polynomial $P(t_0, Y)$ is in $O_K[Y]$ (as $t_0 \in O_K$), 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 $1, y_0, \cdots, y_0^{|G|-1}$ is a K-basis of F_{t_0}/K consisting of elements in $O_{F_{t_0}}$. Thus

$$d_{F_{t_0}/K} \mid \operatorname{disc}(1, y_0, \cdots, y_0^{|G|-1}) = \operatorname{disc}(P(t_0, Y)) = \operatorname{disc}_Y(P(T, Y))_{T=t_0} = \Delta_P(t_0)$$

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

Straightforward estimates involving norms and height show next that
$$|N_{K/\mathbb{Q}}(\Delta_P(t_0))| \leq CB^{\rho\delta_P}$$
for some constant $C > 0$ depending on P and K; these estimates are detailed in §3.1. Hence we obtain :
$$|N_{K/\mathbb{Q}}(d_{F_{t_0}/K})| \leq CB^{\rho\delta_P},$$

The log of this last term is
$$\log[CB^{\delta_P\rho}] \sim \frac{\rho\delta_P}{\rho\delta^-} \log y.$$

As $\delta_P < \delta^-$, conclude that for y suitably large in terms of $F/K(T)$ and δ, we have
$$|N_{K/\mathbb{Q}}(d_{F_{t_0}/K})| \leq y.$$

$\square$

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 $t_0 \in O_K$ 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 $[p_0, \frac{\log y}{2\rho\delta}] \subset [p_0, \log B/2]$. 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 $[p_0, \log B/2]$.

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

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

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

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

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 $\alpha(G) = \dfrac{1 - 1/|G|}{\delta}$ is smaller than the Malle constant $a(G)$ (see [Dèb17, lemma 4.1]).

2.4. Proof of theorems A and B assuming theorem AB. Concerning theorem A, one proceeds as follows. Classically, every finite group G is known to be a regular Galois group over some number field, say K_0. If K is a number field containing K_0, G is still a regular Galois group over K. Clearly $N(K, G, y)$ from §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.

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 (in this first case) 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 $p \in [2, p_0[$ [3] or $\mathfrak{p}$ is bad for $F/K(T)$. Here p_0 is the prime number defined in §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 $S \cap S_{exc} = \emptyset$, 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, i.e., G is not necessarily a regular Galois group over K. The definition of S_{exc} relies on results from [DG12]. A constant $c(G)$ is defined there, for which the following lemma is true.

Lemma 2.5. *Given a finite group G and a number field K, there exist non negative integers r and g such that with*
$$S_{exc} = \{\mathfrak{p} \text{ prime of } K \mid p_{\mathfrak{p}} \mid 6|G| \text{ or } p_{\mathfrak{p}} \leq \max(p_0, c(G))\}$$
the following holds. For every finite set S of primes of K with $S \cap S_{exc} = \emptyset$, there exists a finite Galois extension M/K totally split at each prime $\mathfrak{p} \in S$ and a 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 is the prime number defined in §2.1 from K, G and the integers r, g from the statement.

A proof of this lemma is given in §5 of [DG12].

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 $S \cap S_{exc} = \emptyset$. 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 $S \cap S_{exc} = \emptyset$) 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.

---

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

2.5. A generalization of theorem AB to not necessarily Galois extensions. Denote by S_n the permutation group on n letters $1, \cdots, n$. For an extension E/K of degree n, we denote by $\hat{E}/K$ its Galois closure. The Galois group $\mathrm{Gal}(\hat{E}/K)$ acts transitively on the n embeddings $E \hookrightarrow \overline{K}$. Let $G(1) \subset G$ be the stabilizing subgroup of the neutral 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

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

Theorem 2.6. *If G is a regular Galois group over K, then there exists $\alpha > 0$ such that*

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

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

Remark 2.7. The special case $G(1) = \{1\}$ corresponds to the case the action $G \subset S_n$ is free and transitive, equivalently the extension E/K is Galois of group G. As the proof below shows, we will deduce the general case from this special case.

Proof. 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 only point to be checked is that $\hat{E} = N$. Let H be the biggest normal subgroup of G that is contained in $G(1)$. The Galois closure of $N^{G(1)}$ is N^H. But as H is a normal subgroup, for every $g \in G$, we have $H = H^g \subset G(1)^g = G(i)$ (where $i = g(1)$). Thus, we have $H \subset \bigcap_{i=1}^{n} G(i)$ and H is then the trivial subgroup. Hence $N^H = N$.

The proof of theorem 2.6 easily follows : the Galois extensions N/K provided by theorem A (or by theorem AB) provide as many extensions E/K as requested in the general case. Note that the norm $N_{K/\mathbb{Q}}(d_{E/K})$ is less than $N_{K/\mathbb{Q}}(d_{N/K})$. $\qquad\square$

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 $x \in O_K$ is $H(x) = \max\limits_{\sigma : K \hookrightarrow \overline{K}} |\sigma(x)| = \max\limits_{\substack{v \in M_K \\ v/\infty}} |x|_v$.

Remark 3.1. If $x \neq 0$, then $H(x) = \max\limits_{\sigma : K \hookrightarrow \overline{K}} \max(1, |\sigma(x)|) = \max\limits_{\substack{v \in M_K \\ v/\infty}} (1, |x|_v)$.

Indeed, it is classical that if $x \in O_K$, $x \neq 0$ and $H(x) \leq 1$ then x is a k-th root of 1 for some $k \geq 1$.

We generalize the height to elements of K and to tuples as follows :

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

— for $\underline{a} = (a_1, \cdots, a_n) \in K^n$, $H(a) = \max\limits_{v \in M_K} H_v(\underline{a})$, where $H_v(\underline{a}) = \max(|a_1|_v, \cdots, |a_n|_v)$,

  and $H^+(\underline{a}) = \max\limits_{v \in M_K} H_v^+(\underline{a})$, where $H_v^+(\underline{a}) = \max(1, |a_1|_v, \cdots, |a_n|_v)$

Note that for $x \in O_K$, $H(x) = H(1, x) = H^+(x)$.

The height of a polynomial P with coefficients $a_1, \cdots, a_n$ in K is $H(P) = H(a_1, \cdots, a_n)$.

3.1.2. Preliminary lemmas. The following notation and properties are used all along this section. For theorem C, we consider a polynomial $F(X_1, X_2) \in O_K[X_1, X_2]$.

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 F in X_1 (or in T),
— n be the degree of F in X_2 (or in Y),
— d be the total degree of F (we may and will assume that $d \geq 2$).

The following statement collects different properties used in this paper.

Proposition 3.2. *Let $\underline{a} = (a_1, \cdots, a_m)$ be a m-tuple in K^m ($m \in \mathbb{N}$), let $P(\underline{X}) \in K[\underline{X}] = K[X_1, ..., X_n]$ be a polynomial in n variables with l non-zero coefficients and $(x_1, \cdots, x_n) \in K^n$. Let $t \in K$, $t \neq 0$, and $\sigma : K \to \overline{\mathbb{Q}}$ be a field morphism. Then we have*

(1) $H(\underline{a}) = H(\sigma(\underline{a}))$.

(2) $H(a_i) \leq H^+(\underline{a}) \leq H(a_1) \cdots H(a_m)$. $(i = 1, ..., m)$.

(3) $H(P(x_1, \ldots, x_n)) \leq l.H^+(P). \prod\limits_{i=1}^{n} H(x_i)^{\deg_{X_i}(P)}$.

Proof. 1. is clear.

2. Using the definition, we have

$$H(a_i) = \max\limits_{v \in M_K} \max(|a_i|_v) \leq \max\limits_{v \in M_K} \max(1, |a_1|_v, ..., |a_n|_v) \leq \prod\limits_{i=1}^{m} \max\limits_{v \in M_K} \max(1, |a_i|_v).$$

3. We write $P(\underline{X}) = \sum p_{\underline{a}} \underline{X}^{\underline{a}} = \sum p_{a_1, ... a_n} X_1^{a_1} ... X_n^{a_n}$ and set $d_i = \deg_{X_i}(P)$, $i = 1, \cdots n$.
— for every archimedean place v, we have

$$|P(\underline{x})|_v \leq l. \max\limits_{\underline{a}}(|p_{\underline{a}}|_v) \max(1, |x_1|_v)^{d_1} ... \max(1, |x_n|_v)^{d_n}.$$

— for every finite place v, we have

$$|P(\underline{x})|_v \leq \max\limits_{\underline{a}}(|p_{\underline{a}}|_v) \max(1, |x_1|_v)^{d_1} ... \max(1, |x_n|_v)^{d_n}.$$

Whence

$$H(P(\underline{x})) = \max\limits_{v \in M_K} \max(1, |P(\underline{x})|_v)$$

$$\leq l. \max\limits_{v \in M_K} \max\limits_{\underline{a}} \max(1, |p_{\underline{a}}|_v). \max\limits_{v \in M_K} \max(1, |x_1|_v)^{d_1} \cdots \times \max\limits_{v \in M_K} \max(1, |x_n|_v)^{d_n}$$

$\square$

10

Ideals in O_K and norm. The norm of an ideal $J \subset O_K$ is the cardinality of the quotient ring $N_{K/\mathbb{Q}}(J) = \#O_K/J$ (see [Sam67] for more details). For $a \in O_K$,

$$N_{K/\mathbb{Q}}(aO_K) = |N_{K/\mathbb{Q}}(a)| = \prod_{\sigma:K\to\overline{\mathbb{Q}}} |\sigma(a)| \le H(a)^\rho.$$

We can now prove the inequality

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

stated in the proof of proposition 2.3.

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

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

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

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

$\square$

We will also use the following result.

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

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

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

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

3.1.3. A generalized Heath-Brown result. For every real number $B > 0$, set

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

and

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

Our approach for bounding the number $N(F,B)$ follows an idea of Heath-Brown [HB02] 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 $R(F,B)$ in k subsets, each being the zero set of some polynomial $F_i \in O_K[X_1, X_2]$ relatively prime with F, $i = 1, \cdots, k$. The Bezout theorem then yields the desired bound for $N(F,B)$. An important point is to have a good upper bound for the number k of polynomials F_i. To this end, we prove the following effective generalized Heath-Brown result.

Theorem 3.4. *Let $F(X_1, X_2) \in O_K[X_1, X_2]$ be a polynomial, irreducible in $\overline{K}[X_1, X_2]$ of degree d, let $D \geq d$ be an integer and let B be a suitably large real number (depending on ρ, d, D). There exist a number $k \geq 1$ and some polynomials $F_1, ..., F_k \in O_K[X_1, X_2]$ relatively prime with F in $\overline{K}[X_1, X_2]$ and of degree $\deg(F_i) \leq D$, such that every point $(x_1, x_2) \in R(F, B)$ is a zero of at least one of $F_1, \ldots, F_k$. Furthermore, the integer k is bounded from above by :*

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

where c_2 is a constant depending only on K.

Remark 3.5. This theorem is true for all integers $D \geq d$. 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).

3.2. Proof of theorem 3.4 Fix $D \geq d$ and $B > 0$. The condition that B should be suitably large appears in §3.2.3. We explain below how to construct the polynomials $F_1, \cdots, F_k$, that appear in theorem 3.4.

We take one of the polynomials F_i, $i = 1, \cdots, k$ to be $\dfrac{\partial F}{\partial X_1}$; it is relatively prime to F and of degree $\leq d$. So we may next focus on the subset

$$S(F, B) = \{\underline{x} \in R(F, B) \mid \frac{\partial F}{\partial X_1}(\underline{x}) \neq 0\} \subset R(F, B),$$

and look for k' polynomials F_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 $S(F, B, \mathfrak{p}) \subset S(F, B)$. Let $\mathfrak{p}$ be a prime ideal of O_K and

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

We have

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

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

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

for a constant C_1 depending on K.

Proof. Fix $\underline{x} = (x_1, x_2) \in S(F, B)$; we have $\dfrac{\partial F}{\partial X_1}(\underline{x}) \neq 0$. The number of prime ideals $\mathfrak{p}$ of O_K such that $\dfrac{\partial F}{\partial X_j}(\underline{x}) \in \mathfrak{p}$ is at most $\rho \log_2(H(\dfrac{\partial F}{\partial X_1}(\underline{x})))$ from lemma 3.3. The height of

12

$\frac{\partial F}{\partial X_1}(\underline{x})$ can be estimated using proposition 3.2 : the number l of the non-zero monomials of $\frac{\partial F}{\partial X_1}$ is bounded by $d(d+1)/2 \le d^2$, its degree by $d-1$ and its height by $dH^+(F)$, whence

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

Consider the Galois closure $\widehat{K}/\mathbb{Q}$ of $K/\mathbb{Q}$ and its Galois group Γ. For a conjugacy class C of Γ and $x \ge 1$, denote by $\pi_C(x)$ the number of prime numbers $p \le x$, which do not ramify in $\widehat{K}/\mathbb{Q}$ and such that $\mathrm{Frob}_p(\widehat{K}/\mathbb{Q}) \in C$. For $C = \{1\}$, $\pi_{\{1\}}(x)$ is the number of primes $p \le x$, totally split in $O_{\widehat{K}}$.

Fix an integer $P > 0$ and let $x > 0$ such that

$$(*) \quad \pi_{\{1\}}(x) \ge h(B) + 1 + \pi_{\{1\}}(P).$$

More precisely, we take x as follows : $x = 2a \log a$ with $a = 6\,|\Gamma|\,h(B)\pi_{\{1\}}(P)$. For P suitably large, depending on K, B, it is easily checked that $\frac{x}{\log x} \ge a$ and so

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

which implies that $\pi_{\{1\}}(x) \ge h(B) + 1 + \pi_{\{1\}}(P)$ as from classical results on the Chebotarev theorem, we have $\pi_{\{1\}}(x) \ge \frac{x}{2|\Gamma| \log x}$, for x suitably large.

From $(*)$, there exist at least $[h(B)] + 1$ prime numbers $p \in]P, x]$ 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 $\le x$. Furthermore, this number $\rho[h(B)] + \rho$ is $\ge r$ as $r = [\rho h(B)] + 1$.

We choose r of these ideals which we denote by $\mathfrak{p}_1, ..., \mathfrak{p}_r$. By lemma 3.3, there exists an ideal, say $\mathfrak{p}_i$ $(i \in \{1, ..., r\})$, such that $\frac{\partial F}{\partial X_1}(x_1, x_2) \notin \mathfrak{p}_i$, which means that $(x_1, x_2) \in S(F, B, \mathfrak{p}_i)$. Thus we obtain $S(F, B) = \bigcup_{i=1}^{r} S(F, B, \mathfrak{p}_i)$.

Now $\pi_{\{1\}}(P) \le \frac{2P}{|\Gamma| \log P}$ for P suitably large depending on K, B. So for $i = 1, \cdots, r$,

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

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

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

$\square$

3.2.2. Working on $S(F, B, \mathfrak{p})$ for a fixed $\mathfrak{p} \in \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$. For the next steps, we choose a monomial $X_1^{m_1} X_2^{m_2}$ such that the corresponding coefficient in F is non-zero and such that $m_1 + m_2 = d$. We let then $\mathcal{E}$ be the following set of monomials

$$\mathcal{E} = \{X_1^{e_1} X_2^{e_2} \mid 0 \le e_i \le m_i, \ i = 1, 2, \ e_1 + e_2 \le D\}.$$

Fix $\mathfrak{p} \in \{\mathfrak{p}_1, \cdots \mathfrak{p}_r\}$. Recall from lemma 3.6 that $N_{K/\mathbb{Q}}(\mathfrak{p}) = p \geq P$ and $D \geq d$. Let $\mathbb{F}_p = O_K/\mathfrak{p}$ be the residue field of $\mathfrak{p}$. For every point $\underline{t} = (t_1, t_2) \in \mathbb{F}_p^2$ of F modulo $\mathfrak{p}$ such that $\dfrac{\partial F}{\partial X_1}(\underline{t}) \not\equiv 0 \mod \mathfrak{p}$, consider then the following subset of $S(F, B, \mathfrak{p})$:

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

We have $S(F, B, \mathfrak{p}) = \bigcup_{\underline{t}} S(\underline{t})$ where $\underline{t}$ ranges over the all non-singular points of F modulo p. Fix such a $\underline{t}$. We have $\frac{\partial F}{\partial X_1}(\underline{t}) \neq 0 \mod \mathfrak{p}$. 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 $\underline{x_i} = (x_{i1}, x_{i2})$, $i = 1, \cdots, L$, 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

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

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

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

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

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

(1) The rank of M is $\leq E - 1$,

(2) There exists a non-zero polynomial $F_{\underline{t}}$ of degree $\leq D$ such that
   — $F_{\underline{t}}(\underline{x}) = 0$ for all $\underline{x} \in S(\underline{t})$,
   — $F_{\underline{t}}$ and F are relatively prime.

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 [Wal05] lemma 1.2 for a proof (mod p^m there just has to be replaced by mod $\mathfrak{p}^m$).

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

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

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

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

Furthermore, an argument using Newton polygons shows that for our choice of the set $\mathcal{E}$ of monomials, the polynomials F and $F_{\underline{t}}$ are relatively prime. We refer to [Wal05, §1.3.4] where this argument is detailed.

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

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

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 $N(a) \leq H(a)^\rho$ for every $a \in O_K$.

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

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

We apply Lemma 3.8 with F, $\underline{u} \in \widetilde{O_K}^2$ taken to be a lift of $\underline{t}$, and with $\underline{x}$ taken to be $\underline{x_i}$ $(i = 1, \cdots, E)$. 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 $m \geq 1$ and $i = 1, \cdots, E$).

Set $\underline{w_i} = (w_{i1}, w_{i2}) = (f_m(x_{i2}), x_{i2})$, consider the matrix $M_0 = (\underline{w_i}^{\underline{e}})_{1 \leq i \leq E, \, \underline{e} \in \mathcal{E}}$ and set $\Delta_0 = \det(M_0)$. For every $m \geq 1$, we have

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

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

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

$$\underline{w_i}^{\underline{e}} = f_m(t_2 + y_{i2})^{e_1}(t_2 + y_{i2})^{e_2} = g_{\underline{e}}(y_{i2})$$

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

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 linear operations on the columns, without changing the determinant of M_0, in such a way to organize the columns by strictly growing degree. If a is the smallest degree of some monomial, in first column, the degree a monomial can be removed in every other column; iterating this process proves the claim.

In the end, 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 $\geq l - 1$ 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 $m \geq E(E-1)/2$, 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 $H(x_{ij}) \leq B$, $i = 1, \cdots, E$, $j = 1, 2$. Denote by S_E the permutation group of E elements and for $\sigma \in S_E$, $\varepsilon(\sigma)$ the signature of σ. We

15

have

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

For v an archimedean place,

$$|\Delta|_v \leq E! \max_{1 \leq j \leq E} (|x_{j1}|_v^{e_{11}} |x_{j2}|_v^{e_{12}}) \times \cdots \times \max_{1 \leq j \leq E} (|x_{j1}|_v^{e_{E1}} |x_{j2}|_v^{e_{E2}})$$

$$\leq E! \, B^{e_{11}+e_{12}} \times \cdots \times B^{e_{E1}+e_{E2}}$$

We obtain :

$$H(\Delta) = \max_{v/\infty}(1, |\Delta|_v)$$

$$\leq E! \, B^{e_{11}+e_{12}} \times \cdots \times B^{e_{E1}+e_{E2}}$$

To summarize, $N_{K/\mathbb{Q}}(\Delta)$ is divisible by $p^{E(E-1)/2}$ but $|N_{K/\mathbb{Q}}(\Delta)| \leq H(\Delta)^\rho \leq (E^E B^{E'})^\rho$. We have then proved that under the condition $p^{E(E-1)/2} > (E^E B^{E'})^\rho$, we have $\Delta = 0$. As $p \geq P$ and Δ is an arbitrary minor of M, we conclude that, under the assumption of the statement, the rank of M is $\leq E - 1$. $\qquad\square$

3.2.3. Technical conclusion of theorem 3.4. In order to apply proposition 3.7, P should satisfy the condition

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

where $M_1 := \dfrac{2}{(E-1)}$ and $M_2 := \dfrac{2E'}{E(E-1)}$. We refer to [Wal05] for the following estimates of M_1 and M_2 :

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

This leads to this condition

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

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

$$P = 1 + [(e^8 B^{d^{-1}+6D^{-1}})^\rho] \leq (2^{13} B^{d^{-1}+6D^{-1}})^\rho,$$

and take B large enough so that P satisfies the required condition of proposition 3.7.

To finish the proof of theorem 3.4, it remains to estimate the number k.

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 $S(F, B, \mathfrak{p})$. Using the Lang-Weil bound [FJ86], we obtain

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

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

$$k \leq k_1 d^3 h(B)^3 \frac{P}{\ln P} \ln(\frac{P}{\ln P}).$$

where k_1 is a constant depending on K.

As $\log P \geq \log(P/\log P)$, we have,

$$k \leq k_1 d^3 h(B)^3 P$$

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

where c_2 is a constant depending on K.

3.3. Proof of theorem C. Let $F(X_1, X_2)$ monic in x_2 and B as in theorem C. We keep the notation of §3.1.1.

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

Proposition 3.9. *Let* $F(X_1, X_2) \in O_K[X_1, X_2]$ *of degree d, irreducible in $K[X_1, X_2]$ and not absolutely irreducible. Then $N(F, B) \leq 4d^4$.*

Proof. We will count the number of $x_1 \in O_K$ such that there exists $x_2 \in O_K$ with $F(x_1, x_2) = 0$. The same argument for x_2 will allow us to conclude.

Let (x_1, x_2) be a zero of F. Consider the factorization of F in $\overline{K}[X_1, X_2]$. If $F(x_1, x_2) = 0$ for $(x_1, x_2) \in O_K^2$ 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 F 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 $F(X_1, X_2)$ 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 F. Thus x_1 is a double root of the polynomial $F(X_1, x_2)$. The number of such x_1 is bounded by the number of roots of the polynomial $\text{disc}_{x_2}(F)$ which is of degree $\leq (2d-1)d \leq 2d^2$.

With the same argument for x_2, we can say that the total number of points $(x_1, x_2) \in O_K^2$ such that $F(x_1, x_2) = 0$ is at most $2d^2.2d^2 = 4d^4$. Hence $N(F, B) \leq 4d^4$. □

3.3.2. The absolutely irreducible case. We assume $F(X_1, X_2)$ is irreducible in $\overline{K}[X_1, X_2]$ and is monic in X_2. For our applications, we need a bound for $N(F, B)$ which does not depend on the height $H(F)$ of F. We will use the following Siegel lemma for which we refer to [MR14].

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

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

and with $\max_{1 \leq i \leq N} H(x_i) \leq C(CNH_0)^{M/(N-M)}$, 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 $F(X_1, X_2) \in O_K[X_1, X_2]$ be an irreducible polynomial in $\overline{K}[X_1, X_2]$ of degree d and monic in X_2. Then*

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

17

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

The total number of monomials of degree $\leq d$ 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} $i = 1, \cdots, R$. The one column matrix $f \in O_K^N$, consisting of the coefficients of F is a non trivial solution of the system $AX = 0$.

As $Af = 0$, 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 $g \in O_K^N$ satisfying

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

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

Let $G(X_1, X_2)$ be the polynomial whose coefficients are the elements of g. G is a non-zero polynomial of degree $\leq d$, its coefficients are in O_K, and it satisfies $G(x_{i1}, x_{i2}) = 0$ ($i = 1, \cdots, R$).

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

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

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

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

$\square$

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

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

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

$$N(F, B) \leq k_1 d^5 \log^3(d^3 H^+(F) B^{d-1}) B^{\rho/d} \log(B)$$

where k_1 depends on K.

The bound $H(F) \leq C^{5d^2} 2^{8d^2} d^{8d^2} B^{4d^3}$ from proposition 3.11 gives :

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

Finally we obtain :

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

18

3.4. Proof of corollary C. We work now with a polynomial $F(T, Y) \in O_K[T, Y]$ monic in Y and irreducible in $K[T, Y]$. We will estimate the number $N_T(F, B)$ of $t \in O_K$ such that $H(t) \leq B$ and the specialized polynomial $F(t, Y)$ has a root y in K (or, equivalently, in O_K as $F(T, Y)$ is monic in Y). We recall that m, n and d are respectively the degree in T, Y and the total degree of F.

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

Lemma 3.12. *For all $t \in O_K$ but at most m of them, the height of any $y \in O_K$ such that $F(t, y) = 0$ is bounded by $2(m + 1)H(F)H(t)^m$.*

Proof. We will use the Liouville inequality given in this form : if $P \in K[X]$ and $x \in \overline{K}$ such that $P(x) = 0$, then $H(x) \leq 2H(P)$.

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

$$\deg(a_i(T)) \leq m \text{ and } H(a_i(T)) \leq H(F), \ i = 1, \cdots, n.$$

For $t \in O_K$ such that $a_0(t) \neq 0$ (the number of such t is $\leq m$), the height of every solution $y \in O_K$ of the equation $F(t, Y) = 0$ satisfies :

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

We have $H(F(t, Y)) = H(a_0(t), \cdots, a_n(t)) = \max\limits_{1 \leq i \leq n} \max\limits_{v \in M_K} |a_i(t)|_v$ and

— for an archimedean place v,

$$|a_i(t)|_v \leq (m + 1) \max\limits_{1 \leq i \leq n} (|a_{ij}|_v) \max(1, |t|_v)^m$$
$$\leq (m + 1)H_v(F) \max(1, |t|_v)^m,$$

— for a finite place v, $|a_i(t)|_v \leq H_v(F) \max(1, |t|_v)^m$.

This yields

$$\max\limits_{1 \leq i \leq n} \max\limits_{v \in M_K} |a_i|_v \leq (m + 1) \max\limits_{v \in M_K} H_v(F) \max\limits_{v \in M_K} \max(1, |t|_v)^m$$
$$\leq (m + 1)H(F)H(t)^m$$

This concludes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

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

Proof of Corollary C. We work with the $t \in O_K$ such that lemma 3.12 can be applied. Adding the number of exceptional t will only change the constant that appears in the final bound.

Let $H = \max(e^e, H(F))$, $L_1 := \log(H)$ and $L_2 := \log(\log(H))$. We have $L_2 \geq 1$. As $F(T, Y)$ is monic in Y, we have $d \leq n + m - 1$. We may and will assume that $m \geq 1$ and $n \geq 1$. In particular $d \leq mn < mnL_1/L_2$.

Consider the polynomial

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

19

where $E = [mn\frac{L_1}{L_2}] + 1 \leq 2mnL_1$. This polynomial is of degree $d' \in [nE, nE + m]$ and every zero $(t, y) \in O_K^2$ of F corresponds to a zero $(t, y') = (t, y - t^E) \in O_K^2$ of G. Using the inequality

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

for every zero (t, y') of G such that $H(t) \leq B$, we have

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

Thus, defining $B'' = 2(m + 1)HB^E$, we have

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

Now use theorem C with G and B'':

$$N(G, B'') \leq c_5 d'^{14} \log^4(B'')(B'')^{\rho/d'}$$
$$\leq c_5(nE + m)^{14} \log^4(2(m + 1)HB^E)(2(m + 1)HB^E)^{\rho/nE}$$
$$\leq c_5(nE + m)^{14} \log^4(2(m + 1)HB^E)(2(m + 1)H)^{\rho/nE}B^{\rho/n}$$

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

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

Finally, we obtain

$$N_T(F, B) \leq c_6 d^{54+\rho}(\log H)^{18+\rho}B^{\rho/n}(\log B)^{3+\rho}.$$

$\square$

4. PROOF OF THEOREM 2.1 AND THEOREM 2.2.

4.1. Proof of theorem 2.1 Return to the situation of §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 [Dèb17, proposition 5.1], proved in the case $K = \mathbb{Q}$.

Proposition 4.1. *The set*

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

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

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

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

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 [Dèb17, proposition 5.1].

Consider the prime numbers p_0 and p_{-1} given in §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 $\{p_1, \cdots, p_n\}$ the set of prime numbers in the interval $]p_{-1}, x]$.

Lemma 4.2. *We have* $I = \prod_{1 \le i \le n} (p_i O_K)$ *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 $p_1, \cdots, p_n$. Using that all primes $\mathfrak{p} \in S_x$ are unramified in K from the definition of p_{-1}, we obtain

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

For $i \in \{1, \cdots, n\}$, we have $p_i O_K \cap \mathbb{Z} = p_i \mathbb{Z}$. The next argument shows that

$$(p_1 O_K) \cdots (p_n O_K) \cap \mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

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

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 §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 $\le x$ and $\Pi(x)$ is the product of all prime numbers $p \le x$. 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 $\mathfrak{p} \in S$[4].

Proposition 4.3. *1. If $t_0 \in O_K$ 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,

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

3. Fix a $\mathbb{Z}$-basis $\underline{e} = (e_1, \cdots, e_n)$ of 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 $t_0 \in O_K$ of height $H(t_0) \le \dfrac{\rho H(\underline{e})}{\Pi(p_{-1})}\Pi(x)$.

---

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

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 [Jor72].

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

$$\mathcal{N}(S_x, \mathcal{F}_x) = \prod_{\mathfrak{p} \in S_x} \nu(\mathcal{F}_{\mathfrak{p}})$$

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

$$\geq \chi(\mathcal{F}_x) \times \prod_{\mathfrak{p} \in S_x} q \times \prod_{\mathfrak{p} \in S_x} (1 + \frac{1}{q} - \frac{2g}{\sqrt{q}} - \frac{(r+1)|G|}{q})$$

As in [Dèb17], using that $g < r|G|/2 - 1$ (if $|G| > 1$; from the Riemann-Hurwitz formula) and that $q \geq r^2|G|^2$ for each $\mathfrak{p} \in S_x$ (from the choice of p_{-1}), we have

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

As all primes in S_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 $\mathrm{card}(S_x) \leq \rho\pi(x)$. Hence, we obtain

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

3. We have $O_K = \{\sum_{i=1}^{\rho} m_i.e_i \mid m_i \in \mathbb{Z} \ \ i = 1, \cdots, \rho\}$ and so

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

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 O_K such that $1 \leq m_i \leq \Pi(S_x)$, $i = 1, \cdots, \rho$. Next we have

— for each finite place v, $|t|_v = \left|\sum_{i=1}^{\rho} m_i.e_i\right| \leq \max_{1 \leq i \leq \rho}(|e_1|_v, \cdots, |e_{\rho}|_v)$.

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

Whence $H(t) \leq \rho\Pi(S_x)H(e_1, \cdots, e_{\rho}) = \frac{\rho H(e)}{\Pi(p_{-1})}\Pi(x)$. $\qquad\square$

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

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

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

Taking the log of these terms yields
$$\frac{\log(\Pi(p_B))}{p_B} + \frac{\log p_B}{p_B} \leq \frac{\log B}{p_B} \leq \frac{\log(\Pi(p_B))}{p_B} + \frac{2\log 2p_B}{p_B}$$

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

Take a number B which satisfies the following conditions :
— $\frac{\log B}{2} \leq p_B \leq 2\log B$,
— $p_B \geq \dfrac{\rho H(\underline{e})}{H(p_{-1})}$,
— $\pi(p_B) \leq 2\log B/\log\log B$.
It suffices to take B suitably large depending on K, $H(\underline{e})$, $H(p_{-1})$.

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 $[p_0, \log B/2]$ 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 $[\log B/2, p_B]$).

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 $\leq p_B\Pi(p_B)$ and so $\leq B$. Conclude from proposition 4.3 (2) that the number $\mathcal{N}$ of $t_0 \in O_K$ such that $\mathrm{Gal}(F_{t_0}/K) = G$, $H(t_0) \leq B$ and for all $\mathfrak{p} \in S_B$, $\mathrm{Frob}_{\mathfrak{p}}(\mathrm{F}_{t_0}/\mathrm{K}) \in \mathcal{F}_{\mathfrak{p}}$ satisfies
$$\mathcal{N} \geq \chi(\mathcal{F}_{p_B}) \times \frac{\Pi(p_B)^{\rho}}{(\Pi(p_{-1}))^{\rho}} \times \left(\frac{1}{2r|G|}\right)^{\rho\pi(p_B)}.$$

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

and
— $\Pi(p_B)^{\rho} = \dfrac{(4p_B^2\Pi(p_B))^{\rho}}{(2p_B)^{2\rho}} \geq \dfrac{B^{\rho}}{(2p_B)^{2\rho}}$,
— $(2p_B)^{2\rho} \leq c_1^{\log B/\log\log B}$ for a constant c_1 depending on $F/K(T)$.
Finally, using that $\pi(p_B) \leq 2\rho\log B/\log\log B$, we obtain
$$\mathcal{N} \geq \frac{B^{\rho}}{c^{\log B/\log\log B}}$$

for a constant c depending on $F/K(T)$. $\qquad\square$

4.2. Proof of theorem 2.2. The proof combines the diophantine results of §3 with the following result.

Theorem 4.4. *Let $F/K(T)$ be a regular Galois extension of group G. There exists an integer $N \leq |Aut(G)|$ and some polynomials $\widetilde{P}_1, \cdots, \widetilde{P}_N \in O_K[U, T, Y]$, 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,*

23

— *for every* $u_0 \in O_K \backslash \varepsilon$, $\widetilde{P}_i(u_0, T, Y)$ *is irreducible in* $\overline{K}(T)[Y]$ *and the affine curve* $\widetilde{P}_i(u_0, t, y)$ *is of genus* g_F, $i = 1, \cdots, N$,
— *for every* $t_0 \in O_K$ *which is not a branch point of* $F/K(T)$,

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

This result is the special case of [Dèb18, 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 $(i = 1, \cdots, N)$. Except for a finite number of them, the K-points on $\widetilde{X}_i|_{u_0}$ that appear in [Dèb18] correspond to the zeroes (t_0, y_0) of the polynomial $\widetilde{P}_i(u_0, T, Y)$, $i = 1, \cdots N$.

Diophantine estimates. The constants c_i below, $i = 1, 2, 3$ depend only on the extension $F/K(T)$. We have :
— $\deg(\widetilde{P}(u_0, T, Y)) \leq \deg(\widetilde{P}) = c_1$
— $\deg_Y(\widetilde{P}(u_0, T, Y)) = \deg_Y(\widetilde{P}) = |G|$
— $H(\widetilde{P}(u_0, T, Y)) \leq c_2 H(u_0)^{c_3} \leq c_2 B^{c_3}$

For real numbers $g, D, H, B \geq 0$ and $d_Y \geq 2$, consider all polynomials $Q \in O_K[T, Y]$ monic in Y and irreducible in $\overline{K}(T)[Y]$ such that
— $\deg_Y(Q) = d_Y$
— $\deg(Q) \leq D$
— $H(Q) \leq H$
— the curve $Q(t, y) = 0$ is of genus $\leq g$.
For each such polynomial Q, the number of $t \in O_K$ of height $H(t) \leq B$ and such that $Q(t, y) = 0$ for some $y \in O_K$ 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 $\mathcal{H} \subset O_K$ be a subset consisting of t_0 such that $\mathrm{Gal}(F_{t_0}/K) = G$ and $H(t_0) \leq B$. 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 $\leq N Z(g_F, c_1, |G|, c_2 B^{c_3}, B)$. Let E be the cardinality of ε of theorem 4.4, we obtain

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

From corollary C, we have

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

Finally we obtain

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

REFERENCES

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

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

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

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

[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.

[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.

[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.

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

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

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

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

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

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

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

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

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

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

[Sam67]   Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[Sch79]   Stephen Hoel Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[Wal05]   Yann Walkowiak. Théorème d'irréductibilité de Hilbert effectif. *Acta Arith.*, 116(4):343–362, 2005.

[Wan48]   Shianghaw Wang. A counter-example to Grunwald's theorem. *Ann. of Math. (2)*, 49:1008–1009, 1948.

[Wri89]   David J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1):17–50, 1989.

E-mail address: francois.motte@univ-lille.fr

Laboratoire Paul Painlevé, Mathématiques, Université Lille, 59655 Villeneuve d'Ascq Cedex, France