EFFECTIVE HILBERT'S IRREDUCIBILITY THEOREM FOR GLOBAL FIELDS

MARCELO PAREDES [2] and ROMÁN SASYK [1,2]

Abstract. We prove an effective form of Hilbert's irreducibility theorem for polynomials over a global field K. More precisely, we give effective bounds for the number of specializations $t \in \mathcal{O}_K$ that do not preserve the irreducibility or the Galois group of a given irreducible polynomial $F(T,Y) \in K[T,Y]$. The bounds are explicit in the height and degree of the polynomial $F(T,Y)$, and are optimal in terms of the size of the parameter $t \in \mathcal{O}_K$. Our proofs deal with the function field and number field cases in a unified way.

1. Introduction

A cornerstone in diophantine geometry and Galois theory is Hilbert's irreducibility theorem, which in its original form proved in [14] states that for any polynomial $F(T,Y) \in \mathbb{Z}[T,Y]$ of degree at least one in Y, irreducible in $\mathbb{Q}[T,Y]$ there exist infinitely many integers $n \in \mathbb{Z}$ such that the specialized polynomial $F(n,Y) \in \mathbb{Z}[Y]$ is irreducible in $\mathbb{Q}[Y]$. This was then used by Hilbert to study the inverse Galois problem, more precisely, he showed that in order to prove that a finite group G is the Galois group of a finite extension of $\mathbb{Q}$ it is enough to show that G is the Galois group of some finite extension of the function field $\mathbb{Q}(T)$. Furthermore he constructed polynomials with rational coefficients with Galois group S_n and A_n for all n.

Since then, there have been numerous proofs, improvements and generalizations of Hilbert's irreducibility theorem. Of special interest are those variants which are quantitative. For instance, let K be a global field and let $\mathcal{O}_K$ be its ring of integers. Let us consider a polynomial $F \in \mathcal{O}_K[T_1,\dots,T_s,Y_1,\dots,Y_r]$ which is irreducible as a polynomial in $K(T_1,\dots,T_s)[Y_1,\dots,Y_r]$. We want to mesure how likely is it that a specialization $F(\boldsymbol{t},Y_1,\dots,Y_r)$ with $\boldsymbol{t} := (t_1,\dots,t_s) \in \mathcal{O}_K^s$ remains irreducible. In the case when $K = \mathbb{Q}$ it is natural to consider the quantity

$$N_{F,\mathbb{Q}}(B) := \left|\left\{\boldsymbol{t} \in \mathbb{Z}^s : \max_i |t_i| \le B \text{ and } F(\boldsymbol{t},X_1,\dots,X_r) \text{ is not irreducible in } \mathbb{Q}[X_1,\dots,X_r]\right\}\right|,$$

whereas for global fields a natural generalization of this quantity is

$$N_{F,K}(B) := \left|\left\{\boldsymbol{t} \in [B]^s_{\mathcal{O}_K} : F(\boldsymbol{t},Y_1,\dots,Y_r) \text{ is not irreducible in } K[Y_1,\dots,Y_r]\right\}\right|,$$

where $[B]^s_{\mathcal{O}_K}$ is the global field analogue of the integer box $[-B,B]^s \cap \mathbb{Z}$, which will be defined in Section 2.

We also want to mesure how likely is that a specialization of F on $\boldsymbol{t}$ preserves the Galois group of F. Specifically, for a global field K and $F \in \mathcal{O}_K[T_1,\dots,T_s,Y]$ an irreducible polynomial, let L be the splitting field of F over $K(T_1,\dots,T_s)$. Let G be the Galois group of $L/K(T_1,\dots,T_s)$. For a given $\boldsymbol{t} \in \mathcal{O}_K^s$ let $L_{\boldsymbol{t}}$ be the splitting field of $F(t_1,\dots,t_s,Y)$, and let $G_{\boldsymbol{t}}$ be the Galois group of $L_{\boldsymbol{t}}/K$. Then one wants to estimate the quantity

$$E_{F,K}(B) := \left|\left\{\boldsymbol{t} \in [B]^s_{\mathcal{O}_K} : G_{\boldsymbol{t}} \neq G\right\}\right|.$$

We will use the asymptotic notation $X \lesssim_{C_1,\dots,C_n} Y$ to mean $|X| \le c|Y|$ for some constant c depending on the parameters $C_1,\dots,C_n$. With this notation at hand, we record some of the known estimates for $|E_{F,K}(B)|$. When K is a number field, in [10, Theorem 2.1 and Theorem 2.5] Cohen used the large sieve to prove that the quantities $N_{F,K}(B)$ and $E_{F,K}(B)$ are both bounded by $\lesssim_{r,s,K,F} B^{s-\frac{1}{2}}\log(B)$ with the implicit constant depending polynomially on the height of the polynomial F. Furthermore in [22, Section 13, Theorem 1] Serre showed that the bounds can be improved to $\lesssim_{r,s,K,F} B^{s-\frac{1}{2}}(\log(B))^{\gamma}$ with $\gamma < 1$. In the case when $K = \mathbb{Q}$ and $s = r = 1$, in [21] by

2010 *Mathematics Subject Classification.* 11C08, 11D45, 11G50, 11R09, 11R32, 12E25.

Key words and phrases. Hilbert's irreducibility theorem, global fields, number of rational solutions of diophantine equations, determinant method, distribution of Galois groups.

means of the determinant method of Bombieri and Pila [4], Schinzel and Zannier obtained effective estimates for $N_{F,\mathbb{Q}}(B)$. Improving upon this work, in [24, § 3.2] Walkowiak used the p-adic determinant method of Heath-Brown [13] to prove the bound $N_{F,\mathbb{Q}}(B) \leq c(\log(H(F)))^{19} B^{\frac{1}{2}} (\log(B))^5$ with an explicit c depending on the degree of F, and with $H(F)$ the height of F. Recently, when $K = \mathbb{F}_q(T)$, [2, Theorem 1.1] Bary-Soroker and Entin used the large sieve for function fields to prove that Cohen's bound also holds in this case.

One may further sharpen the counting function $E_{F,K}(B)$ to take into consideration the algebraic structure of G. In this direction, in [26, Theorem 1.4] Zywina used the larger sieve of Gallagher to prove that for any number field K, if $L/K(T_1,\dots,T_s)$ is geometric (i.e. if $L \cap \overline{K} = K$) it holds the bound $E_{F,K}(B) \lesssim_{r,s,K,F} B^{s-1+\beta_G} \log(B)$ where $\beta_G := \max_{M \leq G} \frac{|\cup_{g\in G} gMg^{-1}|}{|G|}$ and M runs over the maximal subgroups of G. In [8, Corollary 1], Castillo and Dietman used Galois resolvents, and bounds obtained in [6] by means of the p-adic determinant method, to show that for $K = \mathbb{Q}$, for any subgroup H of G, and for all $\varepsilon > 0$ it holds that

$$\left|\left\{\boldsymbol{t} \in [B]^s_{\mathcal{O}_K} : G_{\boldsymbol{t}} = H\right\}\right| \lesssim_{F,\varepsilon} B^{s-1+|G/H|^{-1}+\varepsilon}.$$

Among other applications, the p-adic determinant method was used in [7, 13] by Browning, Heath-Brown, and Salberger to prove the uniform dimension growth conjecture of Heath-Brown and Serre for varieties over $\mathbb{Q}$ of degree $d \geq 6$. Specifically, they proved that for any integral projective variety X defined over $\mathbb{Q}$ of degree $d \geq 6$, it holds

$$|\{\boldsymbol{x} \in X(\mathbb{Q}) : H(\boldsymbol{x}) \leq B\}| \lesssim_{\dim(X),d,\varepsilon} B^{\dim(X)+\varepsilon},$$

where $H(\boldsymbol{x})$ is the projective height of $\boldsymbol{x}$. The conjecture for degree $d \geq 4$ was solved by Salberger in [20]. In order to do so, in that article Salberger introduced the global determinant method. This method was refined by Walsh in [25] in his solution of a conjecture of Heath-Brown posed in [13] on bounds for rational points of integral curves. All this was further explored in [9] by Castrick, Cluckers, Dittmann, and Nguyen to prove that the dimension growth conjecture holds without the ε factor when $d \geq 5$ and with a polynomial dependency in d. In [23] Vermeulen adapted [9] to prove the uniform dimension growth conjecture for integral projective varieties defined over $\mathbb{F}_q(T)$ of degree $d \geq 64$. Finally, in [19] we extended [9, 20, 23] and proved the uniform dimension growth conjecture for integral projective varieties over global fields of degree $d \geq 4$.

In the present article we apply some techniques and results of [19] to extend and improve the aforementioned results on effective Hilbert's irreducibility theorem to global fields. Specifically, in [19] we proved a Bombieri-Pila type of bound for curves over global fields, which depends polynomially on the degree of the curve (the cases $K = \mathbb{Q}$ and $K = \mathbb{F}_q(T)$ were already covered in [9, 23]). This, together with a technique we elaborated in [19] that allows us to suppose that a polynomial with coefficients in a global field has coefficients in $\mathcal{O}_K$ and it is almost primitive in the case when $\mathcal{O}_K$ is not a principal ideal domain, are the main novelties in our approach. It seems pertinent to emphasize that our proofs deal simultaneously with the number field and the function field cases. Because of that, for any $a_1, a_2 \in \mathbb{R}$ we will use the notation $[a_1, a_2] := \begin{cases} a_1 & \text{if } \operatorname{char}(K) = 0 \\ a_2 & \text{if } \operatorname{char}(K) > 0 \end{cases}$. We are now in position to state the first result of this article.

Theorem 1.1. *Let K be a global field, and let $F \in K[T,Y]$ be an irreducible polynomial of degree d_T in T and d_Y in Y. Then*

$$N_{F,K}(B) \lesssim_K 2^{[25d_Y,36d_Y]} d_Y^{[26,35]} d_T^{[21,26]} (\log(H_K(F)) + 1)^{[6,10]} B^{\frac{1}{2}},$$

where $H_K(F)$ denotes the K-relative height of F defined in Section 2.

Theorem 1.1 gives the best possible bound in terms of the magnitude of B, as it can be seen by the example $F(T,Y) = Y^2 - T^2$. Furthermore the dependence on F in the bound is completely explicit. When $K = \mathbb{Q}$ this result improves upon the bounds given in [24]. We remark that for number fields $K \neq \mathbb{Q}$ and for function fields this is the first effective bound of this type (the non effective bound $N_{F,K}(B) \lesssim_{F,K} B^{\frac{1}{2}}$ for number fields is a consequence of Siegel's finiteness theorem).

In order to prove Theorem 1.1 we follow the classical approach that reduces the problem of bounding $N_{F,K}(B)$ to that of bounding the number of $\mathcal{O}_K$-roots of any specialization of a certain irreducible polynomial $P(T,Y) \in \mathcal{O}_K[T,Y]$. In that sense, we prove the following result.

Theorem 1.2. *Let K be a global field, and let $P \in \mathcal{O}_K[T,Y]$ be an irreducible polynomial. Let d_T and d_Y be the degrees in T and Y of P, respectively, and let d be the total degree of P. Then the number of $t \in [B]_{\mathcal{O}_K}$ such that $P(t,Y)$ has a solution $y \in \mathcal{O}_K$ is*

$$|\{t \in [B]_{\mathcal{O}_K} : P(t,Y) \text{ has a solution } y \in \mathcal{O}_K\}| \lesssim_K d_Y^{[12,16]} d_T^{[5,9]} (\log(H_K(P))+1)^{[6,10]} B^{\frac{1}{d_Y}}.$$

For number fields, Theorem 1.2 improves upon [24, § 2.2] and [18, Corollary C] by removing the $\log(B)$ factor, and lowering the exponents in the degree and the height of P. For function fields, Theorem 1.2 seems to be new, even for $K = \mathbb{F}_q(T)$. As a consequence of Theorem 1.2, we give the following bound for $E_{F,K}(B)$.

Theorem 1.3. *Let K be a global field and let $F \in K[T,Y]$ be an irreducible polynomial of degrees d_T in T and d_Y in Y. Let G be the Galois group of F and let $\mathcal{H}$ be the family of subgroups of G. Let us suppose that F is separable and monic as a polynomial in $K(T)[Y]$. Then*

$$\begin{aligned} E_{F,K}(B) &\lesssim_K \sum_{H \in \mathcal{H}} 2^{[25|G/H|,36|G/H|]} |G/H|^{[26,35]} d_T^{[28,37]} d_Y^{[7,11]} |H|^{[27,36]} |G|^{[28,37]} (\log(H_K(F))+1)^{[6,10]} B^{\frac{1}{2}} \\ &\lesssim_{K,d_T,d_Y} (\log(H_K(F))+1)^{[6,10]} B^{\frac{1}{2}}. \end{aligned}$$

Moreover, in the case when F is non monic, the second inequality still holds true.

In the case of number fields, Theorem 1.3 improves upon the result of [10] when $s = 1$, whereas, in the case where $K = \mathbb{F}_q(T)$, Theorem 1.3 improves the result of [2] when $s = 1$ by removing the $\log(B)$ factor, and making explicit the dependence on the degree and the height of F. Once again, the novelty in the number field case lies in the effective dependence on the height of F, since it was shown in [22, § 9.2, Proposition 2] that the set of specializations for which $G_t \neq G$ is an affine thin subset, and then by means of Siegel's finiteness theorem, in [22, § 9.7] it was shown that for number fields the number of $t \in [B]_{\mathcal{O}_K}$ lying in an affine thin subset Ω is $\lesssim_{K,\Omega} B^{\frac{1}{2}}$.

While the order of magnitude on B of the bound of Theorem 1.3 is in general sharp as can be seen by considering the polynomial $F(T,Y) = Y^2 - T$, in some cases one may obtain better bounds. Indeed, when $K = \mathbb{Q}$ in [8] Castillo and Dietmann used Galois resolvents to find an adequate primitive element for the splitting field L of F, and use [6, Theorem 1] (which is a Bombieri-Pila type of bound over $\mathbb{Q}$ for lopsided boxes) to deduce a variant of Hilbert's irreducibility theorem for Galois groups that takes into consideration the subgroup structure of the Galois group of the specialized polynomial. By means of Theorem 1.2 and a lemma about Galois resolvents in [8], we improve and generalize [8, Theorem 1] to number fields, and we improve upon Theorem 1.3 in the case when K is a number field. Our result reads as follows.

Theorem 1.4. *Let K be a number field. Let $F(T,Y) \in \mathcal{O}_K[T,Y]$ be an irreducible polynomial of degrees d_T in T and d_Y in Y. Let G be the Galois group of F over $K(T)$, and let H be a subgroup of G. Then*

$$|\{t \in [B]_{\mathcal{O}_K} : \text{ the splitting field of } F(t,Y) \text{ over } K \text{ has Galois group } H\}| \lesssim_{K,d_Y,d_T} (\log(H_K(F))+1)^{[6,10]} B^{|G/H|^{-1}}.$$

As a corollary of Theorem 1.4 we also obtain the following result.

Theorem 1.5. *Let K be a number field, and let $F(T,Y) \in \mathcal{O}_K[T,Y]$ be an irreducible polynomial of degrees d_T in T and d_Y in Y. Let G be the Galois group of $F(T,Y)$ over $K(T)$. If $\delta_G := \max\{|G/H|^{-1} : H \text{ is a proper subgroup of } G\}$ and $\gamma_G := \max\{|G/H|^{-1} : H \text{ is an intransitive subgroup of } G\}$, then*

$$E_{F,K}(B) \lesssim_{K,d_Y,d_T} (\log(H_K(F))+1)^{[6,10]} B^{\delta_G},$$

and

$$N_{F,K}(B) \lesssim_{K,d_Y,d_T} (\log(H_K(F))+1)^{[6,10]} B^{\gamma_G}.$$

This bound is new in the case when $K \neq \mathbb{Q}$, whereas when $K = \mathbb{Q}$, this improves the bound given in [8].

Before ending this introduction, we must mention that the dependence on K of the implicit constants when K is a function field can be made explicit in the degree and genus of the field in all of the bounds, whereas for number fields this dependence is explicit in the degree and the discriminant only if one assumes the Generalized Riemann Hypothesis. This is because the dependence on K in this article relies on the dependence on K in the bounds obtained in [19], which in turn depend on estimates for the number of primes ideals of bounded norm. In the function field case this is covered by the Riemann Hypothesis for curves over finite fields, while in the number field case this is covered by the Landau prime ideal theorem, for which explicit versions are only known under the Generalized Riemann Hypothesis (see [19, Remark 2.7]).

Acknowledgments. M. Paredes was supported in part by a CONICET Postdoctoral Fellowship. R. Sasyk was supported in part through the grant PICT 2017-0883. We thank the anonymous referee for the careful reading of the manuscript and his or her many suggestions.

2. Heights in global fields

We use the asymptotic notation $X = O(Y)$ or $X \lesssim Y$ to mean $|X| \leq C|Y|$ for some constant C. We also use $O_{K,n,d}(Y)$ or $\lesssim_{K,n,d} Y$ to mean that the implicit constants depend on K, n and d.

Throughout this paper, K denotes a global field, i.e. a finite separable extension of $\mathbb{Q}$ or $\mathbb{F}_q(T)$, in which case we further assume that the field of constants is $\mathbb{F}_q$. We will denote by d_K the degree of the extension $K/\Bbbk$, where $\Bbbk$ indistinctively denotes the base fields $\mathbb{Q}$ or $\mathbb{F}_q(T)$.

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Then each embedding $\sigma : K \hookrightarrow \mathbb{C}$ induces a place v, by means of the equation

$$|x|_v := |\sigma(x)|_\infty^{\frac{n_v}{d_K}}, \tag{2.1}$$

where $|\cdot|_\infty$ denotes the absolute value of $\mathbb{R}$ or $\mathbb{C}$ and $n_v = 1$ or 2, respectively. Such places will be called the places at infinity, and will be denoted by $M_{K,\infty}$. Note that $\sum_{v \in M_{K,\infty}} n_v = d_K$. They are all the archimedean places of K. Since the complex embeddings come in pairs that differ by complex conjugation, we have $|M_{K,\infty}| \leq d_K$.

Now, let us suppose that K is a function field over $\mathbb{F}_q$, such that $\mathbb{F}_q$ is algebraically closed in K (in other words, the constant field of K is $\mathbb{F}_q$). A prime in K is, by definition, a discrete valuation ring $\mathcal{O}_{(\mathfrak{p})}$ with maximal ideal $\mathfrak{p}$ such that $\mathbb{F}_q \subseteq \mathfrak{p}$ and the quotient field of $\mathcal{O}_{(\mathfrak{p})}$ equals to K. By abuse of notation, when we refer to a prime in K, we will refer to the maximal ideal $\mathfrak{p}$. Associated to $\mathfrak{p}$, we have the usual $\mathfrak{p}$-adic valuation, that we will denote by $\mathrm{ord}_\mathfrak{p}$. The degree of $\mathfrak{p}$, denoted by $\deg(\mathfrak{p})$ will be the dimension of $\mathcal{O}_{(\mathfrak{p})}/\mathfrak{p}$ as an $\mathbb{F}_q$-vector space, which is finite. Then the norm of $\mathfrak{p}$ is defined as $\mathcal{N}_K(\mathfrak{p}) := q^{\deg(\mathfrak{p})}$. Any prime $\mathfrak{p}$ of K induces a place v in K by the equation

$$|x|_v := |x|_\mathfrak{p} := \mathcal{N}_K(\mathfrak{p})^{-\frac{\mathrm{ord}_\mathfrak{p}(x)}{d_K}}.$$

They are all the places in K. The set of all places in K is denoted by M_K. Now we fix an arbitrary place v_∞ in M_K above the place in $\mathbb{F}_q(T)$ defined by $\left|\frac{f}{g}\right|_\infty := q^{\deg(f)-\deg(g)}$. Its corresponding prime will be denoted $\mathfrak{p}_\infty$; it has degree at most d_K. The ring of integers of K is the subset

$$\mathcal{O}_K := \{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K, v \neq v_\infty\}.$$

If K is a number field with ring of integers $\mathcal{O}_K$, we define

$$[B]_{\mathcal{O}_K} := \{x \in \mathcal{O}_K : \max_{\sigma : K \hookrightarrow \mathbb{C}} |\sigma(x)|_\infty \leq B^{\frac{1}{d_K}}\} = \{x \in \mathcal{O}_K : \max_{v \in M_{K,\infty}} |x|_v \leq B^{\frac{n_v}{d_K}}\}.$$

When K is a function field, we define

$$[B]_{\mathcal{O}_K} := \{x \in \mathcal{O}_K : |x|_{v_\infty} \leq B^{\frac{1}{d_K}}\}.$$

We will use a notion of height for a polynomial that is defined in [3, § 1.6]. Specifically, given a global field K of degree d_K and a place $v \in M_K$, for $F = \sum_I a_I \boldsymbol{Y}^I \in K[Y_1, \dots, Y_n]$, we define

$$|F|_v := \max_I |a_I|_v.$$

Following [3, § 1.6], the K-relative height of $F \in K[Y_1, \dots, Y_n]$ is defined as

$$H_K(F) := \left(\prod_{v \in M_K} |F|_v \right)^{d_K}.$$

We will also use the K-affine relative height

$$H_{K,\mathrm{aff}}(F) := \left(\prod_{v \in M_K} \max\{1, |F|_v\} \right)^{d_K}.$$

In particular,

$$H_K(F) \le H_{K,\mathrm{aff}}(F).$$

We will use the following property concerning the height of polynomials, which is a consequence of [19, Proposition 2.2], that will allow us to deal with polynomials defined in global fields with non-principal ring of integers.

Lemma 2.1. *Let K be a global field. There exists a positive constant $c_1 = c_1(K)$ with the property that for any $F \in K[Y_1, \dots, Y_n]$ there is $\lambda \in K^\times$ such that $\lambda F \in \mathcal{O}_K[Y_1, \dots, Y_n]$, and for all $v \in M_{K,\infty}$ it holds*

$$|\lambda F|_v \le \begin{cases} c_1 H_K(F)^{\frac{n_v}{d_K^2}} & \text{if } K \text{ is a number field,} \\ c_1 H_K(F)^{\frac{1}{d_K}} & \text{if } K \text{ is a function field.} \end{cases} \tag{2.2}$$

In particular, $H_{K,\mathrm{aff}}(\lambda F) \lesssim_K H_K(F)$.

We will use the following standard estimate of Liouville (or perhaps Cauchy). Let K be a field with an absolute value $|\cdot|$. Let $P = a_0 + a_1 Y + \cdots + a_d Y^d \in K[Y]$. of degree $d \ge 0$. Let y be a root of P over an algebraic closure $\overline{K}$ of K. Let us suppose that $|\cdot|$ also denotes an extension of the absolute value to $K(y)$. Then

$$|y| \le \begin{cases} 1 + \frac{\max_i |a_i|}{|a_d|} & \text{if } |\cdot| \text{ is archimedean} \\ \frac{\max_i |a_i|}{|a_d|} & \text{if } |\cdot| \text{ is non-archimedean} \end{cases}. \tag{2.3}$$

Indeed, If $|\cdot|$ is archimedean, then for any $|y| \ge 1$ it holds the inequality

$$|a_d||y|^d = \left| \sum_{i=0}^{d-1} a_i y^i \right| \le \sum_{i=0}^{d-1} |a_i||y|^i \le \max|a_i| \sum_{i=0}^{d-1} |y|^i = \max|a_i| \frac{|y|^d - 1}{|y| - 1} \le \max|a_i| \frac{|y|^d}{|y| - 1},$$

from where the bound follows at once. On the other hand, If $|\cdot|$ is non-archimedean, (3.2) follows by replacing the triangle inequality by the ultrametric inequality.

3. Bounds for the number of integral roots of the specialized polynomial

As with many proofs of Hilbert's irreducibility theorem, we are going to reduce the problem to that of bounding the number of $t \in [B]_{\mathcal{O}_K}$ for which $P(t, Y)$ has an $\mathcal{O}_K$-root, with $P(T, Y) \in \mathcal{O}_K[T, Y]$ an adequate irreducible polynomial of degree d_T in T. In order to bound these specializations, we note that for any such t we can bound the size of any root $y \in \mathcal{O}_K$ of $P(t, y) = 0$. More precisely, Liouville's inequality (3.2) gives $y \in [cB^{d_T}]_{\mathcal{O}_K}$ for some constant c depending on the degree and height of P. Thus, the number of t's for which $P(t, Y)$ has an $\mathcal{O}_K$-root is contained in the subset of $(t, y) \in [cB^{d_T}]^2_{\mathcal{O}_K}$. Then, as in [21, 24] we bound the cardinal of this subset by means of a Bombieri-Pila type of bound. The difference in our proof is that we are going to use a Bombieri-Pila type of bound that we obtained in [19], which is valid for global fields and gives bounds with the $\log(B)$ term removed, and that we are going to use Lemma 2.1 which allows us to deal with polynomials defined in global fields with non-principal ring of integers.

As in [19, Definition 3.22], if c_1 is the constant in Lemma 2.1 we let

$$\beta := \begin{cases} 27d^4 & \text{if } \mathrm{char}(K) = 0, \\ d^{\frac{14}{3}} & \text{if } 0 < \mathrm{char}(K) \leq \max\{27d^4, c_1\}, \\ 1 & \text{if } \mathrm{char}(K) > \max\{27d^4, c_1\}. \end{cases}$$

Given $P \in \mathcal{O}_K[T,Y]$ of total degree d we define $b(P) := 0$ if P is not absolutely irreducible, otherwise we let

$$b(P) := \prod_{\mathfrak{p} \in \mathcal{P}_P} \exp\left(\frac{\log(\mathcal{N}_K(\mathfrak{p}))}{\mathcal{N}_K(\mathfrak{p})}\right),$$

where

$$\mathcal{P}_P := \{\mathfrak{p} \notin M_{K,\infty} : \mathcal{N}_K(\mathfrak{p}) > \max\{\beta, c_1\} \text{ and } P \bmod \mathfrak{p} \text{ is not absolutely irreducible}\}.$$

When P is absolutely irreducible, [19, Lemma 3.23] gives the bound

$$b(P) \lesssim_{K,n} \max\left\{d^{[-2,2]} \log(H_{K,\mathrm{aff}}(P)), 1\right\}. \tag{3.1}$$

We are now in position to state the Bombieri-Pila type of bound that we have obtained in [19].

Theorem 3.1 ([19, Corollary 5.15])**.** *Let K be a global field of degree d_K. Let $P \in \mathcal{O}_K[T,Y]$ of total degree d be irreducible, and let P_d be its homogeneous part of total degree d. Then for any $B \geq 1$, it holds*

$$\begin{aligned} \left|\left\{(t,y) \in [B]^2_{\mathcal{O}_K} : P(t,y) = 0\right\}\right| &\lesssim_K B^{\frac{1}{d}} \frac{\min\{d^{[2,6]} \log(H_K(P_d)) + d^{[3,7]} \log(B) + d^{[4,8]}, d^{[4,\frac{14}{3}]} b(P)\}}{H_K(P_d)^{\frac{1}{d^2}}} + d \log(B) + d^{[4,8]} \\ &\lesssim_K d^{[4,8]} (\log(H_{K,\mathrm{aff}}(P)) + 1) B^{\frac{1}{d}}. \end{aligned}$$

With this at hand we can now prove Theorem 1.2 of the Introduction.

Proof of Theorem 1.2. By Lemma 2.1, after multiplying by an adequate non-zero constant, we may suppose that P verifies the bound (2.2) with $\lambda = 1$. Let us write $P(T,Y) = a_0(T)Y^{d_Y} + \cdots + a_{d_Y}(T)$. Let $t \in [B]_{\mathcal{O}_K}$ and let $y \in \mathcal{O}_K$ be a root of $P(t,Y)$. By Liouville's inequality (3.2), $|y|_v \leq 2 \max_i |a_i(t)|_v$ for all $v \in M_{K,\infty}$. Then (2.2) implies that

$$|y|_v \leq 2 \max_i |a_i(t)|_v \leq 2|d_T+1|_v^{[1,0]} |P|_v |t|_v^{d_T} \leq 2c_1 |d_T+1|_v^{[1,0]} H_K(P)^{\left[\frac{n_v}{d_K^2}, \frac{1}{d_K}\right]} |t|_v^{d_T} \text{ for all } v \in M_{K,\infty}. \tag{3.2}$$

It follows that $y \in [(2c_1)^{d_K^2} (d_T+1)^{[d_K,0]} H_K(P) B^{d_T}]_{\mathcal{O}_K}$. Thus, its enough to bound the number of 2-tuples (t,y) lying in the box $[(2c_1)^{d_K^2} (d_T+1)^{[d_K,0]} H_K(P) B^{d_T}]^2_{\mathcal{O}_K}$ which are zeroes of $P(T,Y)$. Since Theorem 3.1 gives a bound of size $O_{K,P}(B^{\frac{d_T}{d}})$, we will distinguish between the cases when d is large and when d is small as in [21]. To that end, let $H := \max\{e^e, H_{K,\mathrm{aff}}(P)\}$, let $L_1 := \log(H)$ and let $L_2 := \log(\log(H))$. Since $H \geq e^e$, it holds $L_2 \geq 1$.

Let us suppose first that $d \geq d_K^2 d_T d_Y \frac{L_1}{L_2}$. Then $(d_T+1)^{\frac{d_K}{d}} \leq 2$, $H^{\frac{1}{d}} \leq \log(H)^{\frac{1}{d_K^2 d_T d_Y}}$ and $B^{\frac{d_T}{d}} \leq B^{\frac{1}{d_Y}}$. By Theorem 3.1 applied to P in the box $[(2c_1)^{d_K^2} (d_T+1)^{[d_K,0]} H B^{d_T}]^2_{\mathcal{O}_K}$ we conclude that the number of $t \in [B]_{\mathcal{O}_K}$ for which $P(t,Y) = 0$ has a solution in $\mathcal{O}_K$ is bounded by

$$\lesssim_K d^{[4,8]} (\log(H_{K,\mathrm{aff}}(P)) + 1) \left((2c_1)^{d_K^2} (d_T+1)^{[d_K,0]} H B^{d_T}\right)^{\frac{1}{d}} \lesssim_K d^{[4,8]} ((\log(H))^{\frac{1}{d_K^2 d_T d_Y}+1} + 1) B^{\frac{1}{d_Y}}. \tag{3.3}$$

Let us suppose now that $d < d_K^2 d_T d_Y \frac{L_1}{L_2}$ and let us consider the polynomial $G(T,Y) := P(T, T^E + Y)$ where $E = \left\lfloor d_K^2 d_T d_Y \frac{L_1}{L_2} \right\rfloor + 1 \in [d_K^2 d_T d_Y \frac{L_1}{L_2}, 2d_K^2 d_T d_Y L_1]$. Then

$$d_Y E \leq \deg(G) \leq d_Y E + d_T \leq 3 d_K^2 d_Y^2 d_T L_1, \text{ and } \log(H_{K,\mathrm{aff}}(G)) \lesssim_K [d_Y, 1] + \log(H_{K,\mathrm{aff}}(P)) \lesssim_K [d_Y, 1] + \log(H).$$

Note that every zero $(t,y) \in \mathcal{O}_K^2$ of G corresponds to a zero of P of the form $(t, y + t^E)$. Then (3.2) implies that any zero (t,y) of G with $t \in [B]_{\mathcal{O}_K}$ and $y \in \mathcal{O}_K$ verifies

$$|y|_v = |-t^E + (y + t^E)|_v \leq |t|_v^E + 2c_1 |d_T+1|_v^{[1,0]} H_K(P)^{\left[\frac{n_v}{d_K^2}, \frac{1}{d_K}\right]} |t|_v^{d_T} \text{ for all } v \in M_{K,\infty}.$$

Then it follows that $y \in [(3c_1)^{d_K^2}(d_T+1)^{[d_K,0]}H_K(P)B^E]_{\mathcal{O}_K}$. Hence, by Theorem 3.1 applied to G in the box $[(3c_1)^{d_K^2}(d_T+1)^{[d_K,0]}HB^E]^2_{\mathcal{O}_K}$ the number of $t \in [B]_{\mathcal{O}_K}$ for which $P(t,Y)=0$ has a solution in $\mathcal{O}_K$ is bounded by

$$\begin{aligned}
&\lesssim_K \deg(G)^{[4,8]}\left(\log(H_{K,\mathrm{aff}}(G))+1\right)\left((3c_1)^{d_K}(d_T+1)^{[d_K,0]}HB^E\right)^{\frac{1}{\deg(G)}}\\
&\lesssim_K d_Y^{[8,16]}d_T^{[4,8]}([d_Y,1]+\log(H))^{[4,8]+1}H^{\frac{L_2}{d_K^2 d_T d_Y L_1}}B^{\frac{1}{d_Y}}\\
&\lesssim_K d_Y^{[12,16]}d_T^{[4,8]}(\log(H))^{[5,9]}(\log(H))^{\frac{1}{d_K^2 d_T d_Y}}B^{\frac{1}{d_Y}} \lesssim_K d_Y^{[12,16]}d_T^{[4,8]}(\log(H))^{[5,9]+\frac{1}{d_K^2 d_T d_Y}}B^{\frac{1}{d_Y}} \qquad (3.4)
\end{aligned}$$

Since there are at most d_T values of t for which $a_0(t)=0$, from (3.3) and (3.4) we deduce the bound stated in Theorem 1.2 written in terms of $H_{K,\mathrm{aff}}(P)$. By Lemma 2.1 we recover Theorem 1.2 in terms of $H_K(P)$. □

4. Effective Hilbert's irreducibility theorem

The goal of this section is to prove Theorem 1.1 from the Introduction. The idea of the proof is as follows. The irreducibility of a polynomial $F \in K[T,Y]$ implies that for any $t \in \mathcal{O}_K$ such that $F(t,Y)$ is reducible over K, any non-trivial factorization of $F(t,Y)$ over K gives an irreducible polynomial over K which comes from specialization by t of a non-trivial factor $G(T,Y)$ of $F(T,Y)$ over $\overline{K(T)}$, an algebraic closure of $K(T)$. From the fact that G does not lie in $K[T]$ but $G(t,Y)$ does lie in $K[T]$ it follows that some coefficient of G does not lie in $K[T]$ but its specialization lies in K. Then the minimal polynomial $P(T,Y)$ of this coefficient will lie in $K[T,Y]$ and will have a root in $\mathcal{O}_K$, thus one is reduced to the problem of bounding the number of specializations of an irreducible polynomial which have $\mathcal{O}_K$-roots, and this is exactly the setting of Theorem 1.2 which was proved in Section 3. In order to carry out this strategy, it is required to bound the degree and height of the polynomial P. Obtaining such bounds will be the main technical aspect of this section. In order to prove Theorem 1.1 it will be convenient first to prove a variant of it for polynomials $F(T,Y) \in K[T,Y]$ that are monic on Y. This is the content of the following proposition.

Proposition 4.1. *Let K be a global field and let $F \in \mathcal{O}_K[T,Y]$ be a polynomial that is monic in Y and irreducible over K. Let d_T and d_Y denote the degrees in T and Y of F, respectively. Then*

$$|\{t \in [B]_{\mathcal{O}_K} : F(t,Y) \text{ is reducible over } K\}| \lesssim_K 2^{[25d_Y,36d_Y]}d_T^{[14,26]}\left(\log(H_K(F))+1\right)^{[6,10]}B^{\frac{1}{2}}.$$

Before proving Proposition 4.1, we will require a preliminary lemma, which generalizes [21, Lemma 3] and [24, Lemme 3.1] to global fields. In order to state it, let $\overline{K(T)}$ be an algebraic closure of $K(T)$, and let

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

be the factorization of F over $\overline{K(T)}[Y]$. Since for all i, y_i is integral over $\mathcal{O}_K[T]$,then for any non-empty subset $\omega \subseteq \{1,\dots,d_Y\}$ and for any nonnegative integer $j \le |\omega|$, $\tau_j(y_i : i \in \omega)$ is integral over $\mathcal{O}_K[T]$, where τ_j is the j^{th} fundamental symmetric function. Hence if $P_{\omega,j}(T,Y)$ denotes the minimal polynomial of $\tau_j(y_i : i \in \omega)$ over $K(T)$, it follows that $P_{\omega,j} \in \mathcal{O}_K[T,Y]$ and it is monic in Y.

Lemma 4.2. *Let K be a global field and let $F \in \mathcal{O}_K[T,Y]$ be a polynomial that is monic in Y and irreducible over K. Let d_T and d_Y denote the degrees in T and Y of F, respectively. Let us suppose that $d_Y \ge 2$. Let $t \in \mathcal{O}_K$ such that $F(t,Y)$ is reducible over K. Then there exists a non-empty subset $\omega \subseteq \{1,\dots,d_Y\}$ of cardinal $|\omega| \le \frac{d_Y}{2}$ and $j \le |\omega|$ such that*

1. $2 \le \deg_Y(P_{\omega,j}) \le 2^{d_Y}$;
2. *$P_{\omega,j}(t,Y)$ has a zero in $\mathcal{O}_K$;*
3. $\deg(P_{\omega,j}) \le d_T \deg_Y(P_{\omega,j}) \le d_T 2^{d_Y}$;
4. $H_K(P_{\omega,j}) \lesssim ([2^{d_Y+2}(d_T+1),1]^{d_K}H_K(F))^{\deg_Y(P_{\omega,j})}$.

Proof. Since $K[T, y_1, \dots, y_{d_Y}]$ is integral over $K[T]$, by [1, Exercise 2, Chap. 5], for any $t \in K$ the specialization morphism $T \to t$ extends to a morphism from $K[T, y_1, \dots, y_{d_Y}]$ to $\overline{K}$. For $y \in K[T, y_1, \dots, y_{d_Y}]$ we denote $y(t)$ the image of y under this morphism.

Let t be as in the statement of the lemma, namely, $t \in \mathcal{O}_K$ such that $F(t, Y)$ is reducible over K. Since F is monic on Y, by Gauss's lemma it is reducible over $\mathcal{O}_K$, so we have a decomposition

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

where $\omega \subseteq \{1, \dots, d_Y\}$, $|\omega| \leq \frac{d_Y}{2}$ and $R(Y) := \prod_{i \in \omega}(Y - y_i(t)) \in \mathcal{O}_K[Y]$. Up to a sign, the coefficients of $R(Y)$ are equal to $\tau_j(y_i(t) : i \in \omega)$, $j = 1, \dots, |\omega|$. Observe that at least one of the $\tau_j(y_i : i \in \omega)$ verifies that it is not in $K(T)$, otherwise $F(T, Y)$ would be reducible over K. Let $\theta_{\omega,j}$ be this element and let $P_{\omega,j}(T, Y)$ be its minimal polynomial over $K(T)$. By the discussion preceding the lemma, $P_{\omega,j}(T, Y) \in \mathcal{O}_K[T, Y]$ and is monic in Y. Note that $\theta_{\omega,j}(t) \in \mathcal{O}_K$, hence $P_{\omega,j}$ verifies condition (2).

It is clear that $\deg_Y(P_{\omega,j}) \geq 2$, since otherwise $\theta_{\omega,j}$ would lie in $K(T)$. Moreover, the polynomial

$$\prod_{\omega' \subseteq \{1, \dots, d_Y\} : |\omega'| = |\omega|} (Y - \tau_j(y_i : i \in \omega')) \tag{4.1}$$

has degree in Y equal to $\binom{d_Y}{|\omega|} \leq 2^{d_Y}$, it is invariant under the action of the Galois group of F so it has coefficients in $K(T)$ (and hence in $K[T]$ since $K[T]$ is integrally closed in $K(T)$) and vanishes on $\theta_{\omega,j}$. It follows that $P_{\omega,j}$ divides this polynomial, thus $\deg_Y(P_{\omega,j}) \leq 2^{d_Y}$. This proves condition (1).

Next, we will bound the height of $P_{\omega,j}$. Let $v \in M_{K,\infty}$. We denote by $\overline{K_v}$ the algebraic closure of the v-completion of K_v. Thus $|\cdot|_v$ extends in a unique way to $\overline{K_v}$. Let us write

$$P_{\omega,j} = \sum_{i=0}^{\deg_Y(P_{\omega,j})} P_i(T) Y^{\deg_Y(P_{\omega,j}) - i} \text{ with } P_i(T) = \sum_h p_{i,h} T^h. \tag{4.2}$$

Claim 4.3. *It holds that*

$$\max_h |p_{i,h}|_v \leq \sup_{z \in \overline{K_v} : |z|_v \leq 1} |p_i(z)|_v \leq \sup_{z \in \overline{K_v} : |z|_v \leq 1} |P_{\omega,j}(z, Y)|_v$$

Proof of Claim 4.3. If K is a number field, $\overline{K_v} = \mathbb{C}$, thus by Cauchy's integral formula it holds

$$|p_{i,h}|_v = \left| \frac{P_i^{(h)}(0)}{h!} \right|_v \leq \sup_{z \in \overline{K_v}, |z|_v \leq 1} |P_i(z)|_v \leq \sup_{z \in \overline{K_v} : |z|_v \leq 1} |P_{\omega,j}(z, Y)|_v.$$

Let us suppose now that K is a function field. By the maximum principle (e.g. see [5, §2.2, Proposition 5]), it holds that $\max_h |p_{i,h}|_v = \sup_{z \in \overline{K_v} : |z|_v \leq 1} |P_i(z)|_v$. □

Let $\alpha_l(z)$, $1 \leq l \leq \deg_Y(P_{\omega,j})$ denote the roots of $P_{\omega,j}(z, Y)$. By means of expressing the coefficients of $P_{\omega,j}$ in terms of symmetric functions of its roots, with an argument similar to the one in [3, Lemma 1.6.7] we will see that

$$|P_{\omega,j}(z, Y)|_v \leq \left|2^{\deg_Y(P_{\omega,j})}\right|_v \prod_{l=1}^{\deg_Y(P_{\omega,j})} \max\{1, |\alpha_l(z)|_v\}. \tag{4.3}$$

Indeed, if $P_{\omega,j}(z, Y) = \sum_{i=0}^{\deg_Y(P_{\omega,j})} P_i(z) Y^{\deg_Y(P_{\omega,j}) - i}$ with $P_0(T) = 1$, it holds that $P_i(z) = \sum_{j_1 < j_2 < \cdots < j_i} \alpha_{j_1}(z)\alpha_{j_2}(z) \cdots \alpha_{j_i}(z)$. Hence,

$$|P_i(z)|_v \leq \left| \binom{\deg_Y(P_{\omega,j})}{i} \right|_v \max_{j_1 < j_2 < \cdots < j_i} |\alpha_{j_1}(z)|_v |\alpha_{j_2}(z)|_v \cdots |\alpha_{j_i}(z)|_v \leq \left|2^{\deg_Y(P_{\omega,j})}\right|_v \prod_{l=1}^{\deg_Y(P_{\omega,j})} \max\{1, |\alpha_l(z)|_v\}.$$

Since $P_{\omega,j}$ divides the polynomial in (4.1), each $\alpha_l(z)$ is of the form $\tau_j(y_i(z) : i \in \omega')$ for some $\omega' \subseteq \{1, \dots, d_Y\}$ with $|\omega'| = |\omega|$, and hence

$$|\alpha_l(z)|_v \leq \left|\binom{|\omega|}{j}\right|_v \prod_{i\in\omega'} \max\{1, |y_i(z)|_v\} \leq |2^{|\omega|}|_v \prod_{i=1}^{d_Y} \max\{1, |y_i(z)|_v\}. \tag{4.4}$$

Claim 4.4. *Writing $F(T,Y)$ as $F(T,Y) = a_0(T)Y^{d_Y} + a_1(T)Y^{d_Y-1} + \cdots + a_{d_Y}(T)$ with $a_0(T) = 1$, it holds that*

$$\prod_{i=1}^{d_Y} \max\{1, |y_i(z)|_v\} \leq [|d_Y + 1|_v, 1] \max_i |a_i(z)|_v.$$

Proof of Claim 4.4. Let us suppose that K is a number field. Let $\sigma : K \hookrightarrow \mathbb{C}$ be the embedding corresponding to v. We denote by $\sigma(F)$ the usual action of σ on F. It follows that $\prod_{i=1}^{d_Y} \max\{1, |y_i(z)|_v\}$ is the Mahler measure of the polynomial $\sigma(F)(z,Y)$. Then [3, Lemma 1.6.7] implies the conclusion of the claim.

On the other hand, if K is a function field, we write $F_1(z,Y) = \prod_{i:|y_i(z)|_v \geq 1}(Y - y_i(z)) \in \overline{K_v}[Y]$ and $F_2(z,Y) = \prod_{i:|y_i(z)|_v<1}(Y - y_i(z)) \in \overline{K_v}[Y]$, thus $F(z,Y) = F_1(z,Y)F_2(z,Y)$. Observe that $|F_2(z,Y)|_v = 1$, since it is a monic polynomial on Y and its coefficients are symmetric functions on elements of absolute value at most 1. From this and the fact that $\prod_{i=1}^{d_Y} \max\{1, |y_i(z)|_v\}$ is the absolute value of one of the coefficients of $F_1(z,T)$, it follows that

$$\prod_{i=1}^{d_Y} \max\{1, |y_i(z)|_v\} \leq |F_1(z,Y)|_v = |F_1(z,Y)|_v |F_2(z,Y)|_v = |F(z,Y)|_v = \max_i |a_i(z)|_v,$$

where the identity $|F_1(z,Y)|_v|F_2(z,Y)|_v = |F_1(z,Y)F_2(z,Y)|_v$ is Gauss's lemma (e.g. see [3, Lemma 1.6.3]). □

By Claim 4.3, Claim 4.4, inequalities (4.3), (4.4), and the elementary bound

$$|a_i(z)|_v \leq |d_T + 1|_v |F|_v \max\{1, |z|_v^{d_T}\} \text{ for all } i, \tag{4.5}$$

we conclude the bound

$$|p_{i,h}|_v \leq \left(|2^{|\omega|+1}|_v [|d_Y + 1|_v, 1] |d_T + 1|_v |F|_v\right)^{\deg_Y(P_{\omega,j})}. \tag{4.6}$$

Since $|\omega| \leq \frac{d_Y}{2}$, inequality (4.6) gives the bound on $H_K(P_{\omega,j})$ in the item (4) statement of the lemma.

It remains to prove (3). To that end, first we will bound the degrees of the P_i's in (4.2). Since for each $z \in K$ $P_i(z)$ is up to a sign the i^{th} elementary symmetric function on the roots $\alpha_l(z)$, $1 \leq l \leq \deg_Y(P_{\omega,j})$ of $P_{\omega,j}(z,Y)$ and these roots can be bounded by combining (4.4), Claim 4.4 and (4.5), then

$$|P_i(z)|_v \leq \left|\binom{\deg_Y(P_{\omega,j})}{i}\right|_v \left([|d_Y + 1|_v, 1] |2^{\omega}|_v |d_T + 1|_v |F|_v \max\{1, |z|_v^{d_T}\}\right)^i = O_F(|z|_v^{d_T i}),$$

it follows that $\deg P_i \leq d_T i$. Then

$$\deg P_{\omega,j} = \max_{0 \leq i \leq \deg_Y(P_{\omega,j})} (\deg_Y(P_{\omega,j}) - i + \deg P_i) \leq d_T \deg_Y(P_{\omega,j}).$$

This ends the proof of the lemma. □

Proof of Proposition 4.1. We may suppose that $d_Y \geq 2$, otherwise the bound is trivial. Let $S(B)$ be the number of $t \in [B]_{\mathcal{O}_K}$ such that $F(t,Y)$ is reducible over K. Let $S_\omega(B)$ be the number of $t \in [B]_{\mathcal{O}_K}$ such that $P_{\omega,j}(t,Y)$ has a zero in $\mathcal{O}_K$. By Lemma 4.2(2) it holds

$$S(B) \leq \sum_\omega S_\omega(B) \leq 2^{d_Y} \max_\omega S_\omega(B).$$

Combining Theorem 1.2 and Lemma 4.2 it holds that

$$\begin{aligned} S_\omega(B) &\lesssim_K \deg(P_{\omega,j})^{[17,25]} \left(\log H_K(P_{\omega,j})+1\right)^{[6,10]} B^{\frac{1}{\deg_Y(P_{\omega,j})}} \\ &\lesssim_K 2^{[17d_Y,25d_Y]} d_T^{[17,25]} \left(2^{d_Y}[(d_Y+2)\log(2)+\log(d_T+1),0]+2^{d_Y}\log(H_K(F))+1\right)^{[6,10]} B^{\frac{1}{2}} \\ &\lesssim_K 2^{[24d_Y,35d_Y]} d_T^{[14,25]} \left(\log(H_K(F))+1\right)^{[6,10]} B^{\frac{1}{2}}. \end{aligned}$$

We conclude that

$$S(B) \lesssim_K 2^{[25d_Y,36d_Y]} d_T^{[14,25]} \left(\log(H_K(F))+1\right)^{[6,10]} B^{\frac{1}{2}}. \tag{4.7}$$

□

Having proved Proposition 4.1, which is valid for polynomials which are monic in Y, we will now proceed to give a proof of a quantitative variant of Hilbert's irreduciblity theorem for global fields, which is the content of Theorem 1.1 of the Introduction and the main result in this article.

Proof of Theorem 1.1. By Lemma 2.1, after multiplying by an adequate non-zero constant, we may suppose that F verifies the bound (2.2) with $\lambda = 1$. Let us write $F(T,Y) = a_0(T)Y^{d_Y} + a_1(T)Y^{d_Y-1} + \cdots + a_{d_Y}(T)$ and let

$$G(T,Y) := a_0(T)^{d_Y-1} F\left(\frac{Y}{a_0(T)}, T\right) = Y^{d_Y} + a_1(T)Y^{d_Y-1} + a_0(T)a_2(T)Y^{d_Y-2} + \cdots + (a_0(T))^{d_Y-1}a_{d_Y}(T).$$

Then G is monic in Y, it belongs to $\mathcal{O}_K[T,Y]$, $\deg_T(G) \le d_T d_Y$, $\deg_Y(G) = d_Y$ and if F is irreducible, then G is irreducible. Let us now bound $H_K(G)$ in terms of $H_K(F)$. To that end, note that for any $v \in M_{K,\infty}$ it holds

$$\begin{aligned} |G|_v &= \max\{1, |a_1(T)|_v, |a_0(T)a_2(T)|_v, \ldots, |a_0(T)^{d_Y-1}a_{d_Y}(T)|_v\} \\ &\le [|2^{d_T(\frac{(d_Y+1)d_Y}{2}-1)}|_v, 1] \max\{1, |a_1(T)|_v, |a_0(T)|_v|a_2(T)|_v, \ldots, |a_0(T)|_v^{d_Y-1}|a_{d_Y}(T)|_v\} \\ &\le [|2^{d_T d_Y^2}|_v, 1] \max\{1, |F|_v^{d_Y}\} \le c_1^{d_Y}[|2^{d_T d_Y^2}|_v, 1] H_K(F)^{[\frac{n_v}{d_K^2}, \frac{1}{d_K}]d_Y}, \end{aligned}$$

where in the second inequality we have used that $|fg|_v \le 2^{\deg(f)+\deg(g)}|f|_v|g|_v$ if v is archimedean (e.g see [3, Lemma 1.6.11]) and $|fg|_v = |f|_v|g|_v$ by Gauss's lemma (e.g. see [3, Lemma 1.6.3]) if v is non-archimedean, and in the fourth inequality we have used (2.2). Then

$$H_{K,\mathrm{aff}}(G) = \prod_{v\in M_{K,\infty}} \max\{1,|G|_v\} \le \begin{cases} c_1^{d_Y d_K^2} 2^{d_T d_Y^2 d_K} H_K(F)^{d_Y} & \text{if } K \text{ is a number field,} \\ c_1^{d_Y d_K} H_K(F)^{d_Y} & \text{if } K \text{ is a function field.} \end{cases}$$

By Proposition 4.1 it holds that the number of $t \in [B]_{\mathcal{O}_K}$ with $a_0(t) \neq 0$ and $F(t,Y)$ reducible over K is bounded by

$$\begin{aligned} |\{t \in [B]_{\mathcal{O}_K} : G(t,Y) \text{ is reducible over } K\}| &\lesssim_K 2^{[25\deg_Y(G), 36\deg_Y(G)]} \deg_T(G)^{[14,25]} \left(\log(H_{K,\mathrm{aff}}(G))+1\right)^{[6,10]} B^{\frac{1}{2}} \\ &\lesssim_K 2^{[25d_Y,36d_Y]} d_Y^{[26,35]} d_T^{[20,25]} \left(\log(H_K(F))+1\right)^{[6,10]} B^{\frac{1}{2}}. \end{aligned} \tag{4.8}$$

Taking into account that there are at most d_T values of t for which $a_0(t) = 0$ we see that (4.8) implies the bound in the statement of Theorem 1.1 . □

Remark 4.5. In some cases by the same method of the proof of Theorem 1.1 one can derive a polynomial bound in d_Y and d_T. Specifically, if the polynomial F in Theorem 1.1 is also assumed to be separable, combining our techniques with [11, § 3] would yield the bound

$$|\{t \in [B]_{\mathcal{O}_K} : F(t,Y) \text{ is reducible over } K\}| \lesssim_K d_Y^{c(F)} d_T^{[21,26]} \left(\log(H_K(F))+1\right)^{[6,10]} B^{\frac{1}{2}},$$

where $c(F)$ is, modulo an absolute constant, the Hilbert index defined in [11, § 3.2], which in some cases, e.g. when the Galois group of F is bounded by d_Y^α for some $\alpha > 0$, can be bounded by an absolute constant (see [11, Theorem 4.1]).

From Theorem 1.1 it follows easily the next quantitative variant of Hilbert's irreducibility theorem which improves upon [21, Theorem] and [24, Théorème 3] when $K = \mathbb{Q}$.

Corollary 4.6. *Let $s \in \mathbb{N}$ and let $F(T,Y) \in \mathcal{O}_K[T,Y]$ be an irreducible polynomial of degrees d_T in T and d_Y in Y. Let $C := 2^{[25d_Y,36d_Y]} d_Y^{[26,35]} d_T^{[21,26]} (\log(H_K(F))+1)^{[6,10]}$. Then there exist a constant $c_K \lesssim_K 1$ and s algebraic integers $t_1,\dots,t_s \in [s + c_K C^2]_{\mathcal{O}_K}$ such that the polynomials $F(t_i,Y)$ are irreducible over K for all $i = 1,\dots,s$.*

5. Distribution of Galois groups

The goal of this section is to prove Theorem 1.3, Theorem 1.4, and Theorem 1.5 of the Introduction. As with many instances of Hilbert's irreducibility theorem, it is possible to adapt the strategy of Section 4 to bound the subset of specializations that have a Galois group different from the Galois group of a given irreducible polynomial $F \in K[T,Y]$. More precisely, let $F \in K[T,Y]$ be an irreducible polynomial, monic in Y. Let us denote by L the splitting field of the polynomial F over $K(T)$. Let G be the Galois group of $L/K(T)$. Given $t \in K$ we let L_t be the splitting field of the polynomial $F(t,Y) \in K[Y]$. Let G_t be the Galois group of L_t/K. Let us suppose that F is separable as a polynomial in $K(T)[Y]$ and let $\Delta(T)$ be the discriminant of F, which we regard as a polynomial in $K[T]$. Let $A = K[T]$ and let C be the integral closure of A in L. Let $\mathfrak{p} = (T-t)K[T]$ and let $\mathfrak{P}$ be a prime in C lying over $\mathfrak{p}$. Let $t \in K$ such that $\Delta(t) \neq 0$, i.e. the polynomial $F(t,Y)$ does not have multiple roots in $K = A/\mathfrak{p}$. Since $L_t = C/\mathfrak{P}$ and the Galois group G_t of L_t/K is naturally identified with the Galois group of $(C/\mathfrak{P})/(A/\mathfrak{p})$, by [15, Chapter VII, Section 2, Theorem 2.9] there is an isomorphism of groups $\iota : G_t \to G_{\mathfrak{P}}$, where $G_{\mathfrak{P}}$ is the decomposition group of $\mathfrak{P}$, which is a subgroup of G. If ρ denotes the natural embedding of G in the permutation group $S_{\deg_Y(F)}$, it follows that there are injective morphisms ι, ρ_t such that the following is a commutative diagram

$$\begin{array}{ccc} G_t & \xrightarrow{\ \iota\ } & G \\ & \searrow^{\rho_t} & \downarrow \rho \\ & & S_{\deg_Y(F)} \end{array}$$

With all this at hand we are able to prove Theorem 1.3 and Theorem 1.4 of the Introduction.

Proof of Theorem 1.3. The strategy of the proof of Theorem 1.3 consists of making effective [22, Chapter 9, Section 9.2, Proposition 2] and then using Theorem 1.1. More precisely, let us suppose that F is monic on Y. By Lemma 2.1, after multiplying by an adequate non-zero constant, we may suppose that F verifies the bound (2.2) with $\lambda = 1$. Since $L/K(T)$ is a Galois extension, all its subextensions are of the form L^H for some subgroup $H \leq G$. By the separability assumption, they are of the form $K(T)(\alpha_H)$ for some $\alpha_H \in L$, which we may suppose it is integral over $K[T]$. Let $P_H \in K[T,Y]$ be an irreducible polynomial of minimal degree which has α_H as a root.

Claim 5.1. *Let $\mathcal{H}$ be the subset of subgroups of G. It holds that*

$$\{t \in [B]_{\mathcal{O}_K} : G_t \neq G \text{ and } \Delta(t) \neq 0\} \subseteq \bigcup_{H \in \mathcal{H}} \{t \in [B]_{\mathcal{O}_K} : P_H(t,Y) \text{ is reducible over } K\}.$$

Proof of Claim 5.1. Let $A = K[T]$ and let C be the integral closure of A in L. Let $t \in [B]_{\mathcal{O}_K}$ such that $\Delta(t) \neq 0$. Let $\mathfrak{P}$ be any prime lying over $\mathfrak{p} = (T-t)A$. Since F is monic in Y, G_t is identified with the decomposition group of $\mathfrak{P}$. Let us assume that $G_t \neq G$. Then there are $\sigma \in G$, $f \in \mathfrak{P} \subseteq C$ such that $\sigma(f) \notin \mathfrak{P}$. Moreover, there is $H \in \mathcal{H}$ such that $f \in K(T)(\alpha_H)$. Since f is integral over A, it lies in the integral closure of A over $K(T)(\alpha_H)$. Since α_H is integral and separable, by the proof of [12, Proposition 13.14] it follows that $f \in K[T][\{\frac{\alpha_H^i}{\Delta(T)^2}\}_i]$. Then, by cleaning denominators, there are $N \in \mathbb{N}_0$ and $P \in K[T,Y]$ such that $\Delta(T)^N f = P(T,\alpha_H)$. By assumption, $f \in \mathfrak{P}$, thus $P(t,\alpha_H(t)) = 0$. Arguing by contradiction, let us suppose that $P_H(t,Y)$ is irreducible over K. Since $P_H(t,\alpha_H(t)) = 0$ it follows that there is some $Q(Y) \in K[Y]$ verifying $P(t,Y) = Q(Y)P_H(t,Y)$. Since $P_H(T,Y)$ has as a root the element $\sigma(\alpha_H)$, it follows that $P_H(t,\sigma(\alpha_H)(t)) = 0$. Then $P(t,\sigma(\alpha_H)(t)) = 0$. But $\Delta(T)^N f = P(T,\alpha_H)$ implies that $\sigma(\Delta(T)^N f) = \Delta(T)^N \sigma(f) = P(T,\sigma(\alpha_H))$. The assumption that $\sigma(f)(t) \notin \mathfrak{P}$

implies that $\sigma(f)(t) \neq 0$. This, together with the fact that $\Delta(t) \neq 0$, implies that $P(t, \sigma(\alpha_H)(t)) \neq 0$, which is a contradiction. □

By Claim 5.1, Theorem 1.3 will follow from Theorem 1.1 if one can bound the heights and the degrees of the polynomials $P_H(T,Y)$. For this purpose, we will require to choose an adequate α_H for each $H \in \mathcal{H}$. This will be achieved in the next two claims.

Claim 5.2. *Let $F(T,Y) = \prod_{i=1}^{d_Y}(Y - y_i)$ with y_i lying in an algebraic closure of $K(T)$. There exists $\alpha_G = y_1 + \gamma_1 y_2 + \cdots + \gamma_{d_Y-1} y_{d_Y}$ with $\gamma_i \in [d_Y^{i+1}]_{\mathcal{O}_\Bbbk}$ for all $1 \leq i \leq d_Y - 1$, such that $L = K(T)(\alpha_G)$.*

Proof of Claim 5.2. Recall that $\Bbbk = \mathbb{Q}$ if K is a number field, and $\Bbbk = \mathbb{F}_q[T]$ if K is a function field. By examining the proof of the primitive element theorem as in [17, Theorem 5.1] we see that $y_1 + \gamma y_2$ is a primitive element for $K(T)(y_1, y_2)$ for any $\gamma \in L$ which is not of the form $\frac{y_i - y_1}{y_2 - y_j}, j \neq 2$. Since there are at most d_Y^2 such possible elements in L and $[d_Y^2]_{\mathcal{O}_\Bbbk}$ has more that d_Y^2 elements, it follows that we may take $\gamma \in [d_Y^2]_{\mathcal{O}_\Bbbk}$. Arguing by induction it follows that there are $\gamma_1, \ldots \gamma_{d_Y-1}$ such that $\alpha_G = y_1 + \gamma_1 y_2 + \ldots + \gamma_{d_Y-1} y_{d_Y}$ is a primitive element for $L/K(T)$, and $\gamma_i \in [d_Y^{i+1}]_{\mathcal{O}_\Bbbk}$ for all i. □

Claim 5.3. *There exists $\alpha_H \in L$ integral over $K[T]$ for which there exists a polynomial $P_H(T,Y) \in \mathcal{O}_K[T,Y]$ that is a multiple of the minimal polynomial of α_H over $K(T)$, such that $\deg(P_H) \leq d_T |H||G|$ and*

$$H_{K,\mathrm{aff}}(P_H) \leq c_1^{d_K|H||G|+d_K^2} 2^{(|G|+|H||G|+|H||G|d_K+d_T|H||G|)d_K} |G|^{(|H|+1)|G|d_K} (d_Y^{d_Y+1})^{|H||G|d_K} (d_T+1)^{|H||G|d_K} H_K(F)^{|H||G|}.$$

Proof of Claim 5.3. It holds that L^H is the field extension of $K(T)$ generated by the coefficients of the polynomial $\prod_{\rho \in H}(Y - \rho(\alpha_G))$, which are of the form $\tau_j(\rho(\alpha_G) : \rho \in H), 1 \leq j \leq |H|$. Note that the coefficients of this polynomial are integral over $K[T]$, since by construction α_G is integral over $K[T]$. Let $\tau_j := \tau_j(\rho(\alpha_G) : \rho \in H), 1 \leq j \leq |H|$. Since all the τ_j lie in L, they are elements of degree at most $|G|$. Then repeating the argument of Claim 5.2 we may take $\alpha_H = \tau_1 + \delta_1 \tau_2 + \cdots + \delta_{|H|-1}\tau_{|H|}$ with $\delta_i \in [|G|^{i+1}]_{\mathcal{O}_\Bbbk}$ for all $1 \leq i \leq |H| - 1$.

Let $P_H(T,Y)$ be the minimal polynomial of α_H over $K[T]$. By construction of α_H, it is monic in Y, thus $H_K(P_H) = H_{K,\mathrm{aff}}(P_H)$, and $\deg_Y(P_H(T,Y)) = |G/H|$. Let $P(T,Y) := \prod_{\rho \in G}(Y - \rho(\alpha_H))$. Since P is invariant under the action of the Galois group G and α_H is integral over $K[T]$, it holds that $P(T,Y) \in K[T,Y]$. Furthermore, $P_H(T,Y)$ divides $P(T,Y)$ in $K(T)[Y]$ because it has α_H as a root. Since the principal term of $P_H(T,Y)$ as a polynomial in Y is a scalar, we conclude that there is some $Q(T,Y) \in K[T,Y]$ such that $P(T,Y) = Q(T,Y)P_H(T,Y)$. Then, for all $v \in M_K$ it follows that

$$|P(T,Y)|_v \begin{cases} = |Q(T,Y)|_v |P_H(T,Y)|_v & \text{if } v \text{ is non-archimedean} \\ \geq \left|2^{-(\deg(P(T,Y))}\right|_v |Q(T,Y)|_v |P_H(T,Y)|_v & \text{if } v \text{ is archimedean} \end{cases}, \tag{5.1}$$

where we have used Gauss's lemma $|fg|_v = |f|_v |g|_v$ if v is non-archimedean, and the inequality $|fg|_v \geq 2^{-(\deg(f)+\deg(g))}|f|_v|g|_v$ if v is archimedean (e.g. see [3, Lemma 1.6.11]). From (5.1) and the fact that the height of any non-zero polynomial is at least 1, it follows that

$$\begin{aligned} H_{K,\mathrm{aff}}(P_H(T,Y)) = H_K(P_H(T,Y)) \leq H_K(P_H(T,Y))H_K(Q(T,Y)) &\leq 2^{\deg(P(T,Y))d_K} H_K(P(T,Y)) \\ &\leq 2^{\deg(P(T,Y))d_K} H_{K,\mathrm{aff}}(P(T,Y)). \end{aligned}$$

Thus, in order to bound $H_{K,\mathrm{aff}}(P_H(T,Y))$ it is enough to bound the height and degree of $P(T,Y)$.

Let us first bound the height of $P(T,Y)$. Note that for any $\rho \in G$, $\rho(\tau_j) = \tau_j((\rho\sigma)(\alpha_G) : \sigma \in H), 1 \leq j \leq |H|$. Furthermore, since G acts by permutation on the roots of F, from the construction of α_G it follows that for all $\rho \in G$, for all $v \in M_{K,\infty}$, and for all $z \in \overline{K}_v$ it holds the bound

$$|\rho(\alpha_G)(z)|_v = \left|y_{\rho(1)}(z) + \gamma_1 y_{\rho(2)}(z) + \cdots + \gamma_{d_Y-1} y_{\rho(d_Y)}(z)\right|_v \leq |d_Y^{d_Y+1}|_v \max_{1 \leq i \leq d_Y} \{|y_i(z)|_v\}. \tag{5.2}$$

Then, for all $\rho \in G$, for all $v \in M_{K,\infty}$, and for all $z \in \overline{K}_v$ it follows that

$$|\rho(\tau_j)(z)|_v \leq \left|\binom{|H|}{j}\right|_v \max_{I\subseteq H:|I|=j} \prod_{\sigma\in I} |(\rho\sigma)(\alpha_G)(z)|_v \leq |2^{|H|}|_v |d_Y^{d_Y+1}|_v^j \max_i\{|y_i(z)|_v^j\} \text{ for all } 1 \leq j \leq |H|,$$

and hence

$$\begin{aligned} |\rho(\alpha_H)(z)|_v = \left|\rho(\tau_1)(z) + \delta_1\rho(\tau_2)(z) + \cdots + \delta_{|H|-1}\rho(\tau_{|H|})(z)\right|_v &\leq \left||H||G|^{|H|}\right|_v \max_j\{|\rho(\tau_j)(z)|_v\} \\ &\leq \left||G|^{|H|+1}\right|_v |2^{|H|}|_v |d_Y^{d_Y+1}|_v^{|H|} \max\{1, |y_i(z)|_v\}^{|H|}. \end{aligned} \tag{5.3}$$

By Liouville's inequality (3.2), $|y_i(z)|_v \leq 2\max_{1\leq i\leq d_Y}\{|a_i(z)|_v\}$. Then, arguing as in the proof of inequality (4.3), from inequalities (4.5) and (5.3), it follows that for all $v \in M_{K,\infty}$ and for all $z \in \overline{K_v}$ with $|z|_v \leq 1$ it holds the bound

$$\begin{aligned} |P(z,Y)|_v &\leq \left|2^{|G|}\right|_v \prod_{\rho\in G} \max\{1, |\rho(\alpha_H)(z)|_v\} \leq \left|2^{|G|}\right|_v \left(\left||G|^{|H|+1}\right|_v |2^{|H|}|_v |d_Y^{d_Y+1}|_v^{|H|}\right)^{|G|} \left(\max_{1\leq i\leq d_Y}\{1, |y_i(z)|_v\}\right)^{|H||G|} \\ &\leq \left|2^{|G|}\right|_v \left(\left||G|^{|H|+1}\right|_v |2^{|H|}|_v |d_Y^{d_Y+1}|_v^{|H|}\right)^{|G|} 2^{|H||G|} \left(\max_{1\leq i\leq d_Y}\{1, |a_i(z)|_v\}\right)^{|H||G|} \\ &\leq \left|2^{|G|}\right|_v \left(\left||G|^{|H|+1}\right|_v |2^{|H|}|_v |d_Y^{d_Y+1}|_v^{|H|}\right)^{|G|} 2^{|H||G|} |d_T+1|_v^{|H||G|} \max\{1, |F|_v\}^{|H||G|}. \end{aligned} \tag{5.4}$$

By the same argument as in the proof of Claim 4.3, and by inequality (5.4), we conclude that for all $v \in M_{K,\infty}$,

$$|P(T,Y)|_v \leq \left|2^{|G|}\right|_v \left(\left||G|^{|H|+1}\right|_v |2^{|H|}|_v |d_Y^{d_Y+1}|_v^{|H|}\right)^{|G|} 2^{|H||G|} |d_T+1|_v^{|H||G|} \max\{1, |F|_v\}^{|H||G|}. \tag{5.5}$$

Then

$$\begin{aligned} H_{K,\mathrm{aff}}(P(T,Y)) &= \left(\prod_{v\in M_{K,\infty}} \max\{1, |P(T,Y)|_v\}\right)^{d_K} \\ &\leq \left(\prod_{v\in M_{K,\infty}} (2c_1)^{|H||G|} \left|2^{|G|+|H||G|} |G|^{(|H|+1)|G|} (d_Y^{(d_Y+1)|H||G|}) (d_T+1)^{|H||G|}\right|_v H_K(F)^{[\frac{n_v}{d_K^2}, \frac{1}{d_K}]|H||G|}\right)^{d_K} \\ &= c_1^{d_K|H||G|} 2^{(|G|+|H||G|+|H||G|d_K)d_K} |G|^{(|H|+1)|G|d_K} (d_Y^{d_Y+1})^{|H||G|d_K} (d_T+1)^{|H||G|d_K} H_K(F)^{|H||G|}. \end{aligned} \tag{5.6}$$

Let us now bound the degree of $P(T,Y)$. Note that the coefficients of $P(z,Y)$ as a polynomial in $K[Y]$ are, up to a sign, symmetric functions on the roots $\rho(\alpha_H), \rho \in G$. Then, arguing as in the proof of Lemma 4.2(3), it follows that $\deg(P) \leq d_T|H||G|$. □

By Theorem 1.1 and Claim 5.3, it follows that

$$\begin{aligned} &|\{t \in [B]_{\mathcal{O}_K} : P_H(t,Y) \text{ is reducible over } K\}| \\ &\qquad \lesssim_K 2^{[25\deg_Y(P_H), 36\deg_Y(P_H)]} \deg_Y(P_H)^{[26,35]} \deg_T(P_H)^{[21,26]} (\log(H_{K,\mathrm{aff}}(P_H))+1)^{[6,10]} B^{\frac{1}{2}} \\ &\qquad \lesssim_K 2^{[25|G/H|, 36|G/H|]} |G/H|^{[26,35]} d_T^{[28,37]} d_Y^{[7,11]} |H|^{[27,36]} |G|^{[28,37]} (\log(H_K(F))+1)^{[6,10]} B^{\frac{1}{2}}. \end{aligned} \tag{5.7}$$

Theorem 1.3 follows from Claim 5.1, inequality (5.7), and by taking into account that $|\mathcal{H}| \lesssim_{|G|} 1 \lesssim_{d_Y} 1$ and that the contribution of the t's with $\Delta(t) = 0$ only changes the implicit constant.

The case when F is non monic is dealt as in the proof of Theorem 1.1. □

Remark 5.4. In some cases the argument in the proof of Theorem 1.3 can give polynomial dependence on d_Y and d_T. More specifically, the bounds in d_Y in general are not polynomial because both proofs reduce the problem of bounding the exceptional specializations to that of bounding the number of specializations of some polynomials that depend on the Galois group G of $L/K(T)$. In general, the group G can be as large as $d_Y!$. Nonetheless, if $|G| \leq d_Y^\alpha$ for some absolute constant α, the degree of the minimal polynomial P_H can be bounded polynomially on d_Y, d_T. Furthermore, instead of considering $\mathcal{H}$ as all subgroups of G, one may just consider those maximal subgroups of

G. In this case, there are results that give polynomial bounds for $\mathcal{H}$, e.g. by [16, Theorem 1.3], $|\mathcal{H}| \lesssim |G|^{\frac{3}{2}}$. Taking these observations in consideration, by Remark 4.5 one can prove Theorem 1.3 with a polynomial bound in d_Y.

We now give a proof of Theorem 1.4 of the Introduction.

Proof of Theorem 1.4. As in the proof of Theorem 1.1 we may suppose that F is monic, with $F(T,Y) = Y^{d_Y} + g_1(T)Y^{d_Y-1} + \cdots + g_{d_Y}(T) \in \mathcal{O}_K[T,Y]$. It is easy to see that [8, Lemma 4] is also valid for number fields, so let $\Phi_{F,K}(Z,T)$ be the Galois resolvent constructed in that lemma. Then, if $t \in [B]_{\mathcal{O}_K}$ is such that $F(t,Y)$ has Galois group H over K, then $\Phi_{F,H}(Z,t)$ has a root $z \in \mathcal{O}_K$. Factoring $\Phi_{F,H}(Z,T)$ over K, by Gauss lemma each irreducible factor can be assumed to have $\mathcal{O}_K$-coefficients, monic on Z, and having degree at least $|G/H|$ and at most $|S_{d_Y}/H|$. Moreover, there are at most $\frac{|H|}{|G|}|S_{d_Y}|$ such factors. We conclude the proof by applying Theorem 1.2 to each such irreducible factor of $\Phi_{F,H}(Z,T)$. □

As a corollary, we deduce Theorem 1.5 of the Introduction.

Proof of Theorem 1.5. The bounds follow from Theorem 1.4 and from the fact that if $F(T,Y) = g_0(T)Y^{d_Y} + g_1(T)X^{d_Y-1} + \cdots + g_{d_Y}(T)$, then $g_0(T) \neq 0$ and $\Delta(T) \neq 0$ and the number of exceptional $t \in [B]_{\mathcal{O}_K}$ for which $f(t,Y)$ has degree less than d_Y or becomes inseperable are those t for which $g_0(t) = 0$ or $\Delta(t) = 0$ is bounded by $\lesssim_{K,\deg(F)} 1$. □

As a concluding remark, we mention that, arguing by induction on the number of parameters and using Kronecker's substitution (see for instance [10, Lemma 7.1]), one may extend Theorem 1.2 and then Theorem 1.1, Theorem 1.3, Theorem 1.4 and Theorem 1.5 to polynomials $F \in K[T_1,\dots,T_s,Y]$. However, by the nature of the induction and the fact that Theorem 1.2 depends on $H_K(F)$, the bound has a factor $(\log(B))^\nu$ for some ν. Thus, in the higher dimensional case the bounds one would obtain are not optimal in B. For the sake of completeness we state without the proof the bound that would be obtained by this procedure that extends Theorem 1.2 to the case of several parameters.

Theorem 5.5. *Let K be a global field. Let $P(T_1,\dots,T_s,Y) \in \mathcal{O}_K[T_1,\dots,T_s,Y]$ be irreducible of degree d_Y in Y, and let us suppose that P is monic of degree d_Y. Then there are positive constants $\mu,\nu \lesssim_s 1$ such that*

$$\left|\left\{(t_1,\dots,t_s) \in [B]^s_{\mathcal{O}_K} : P(t_1,\dots,t_s,Y) = 0 \text{ has a solution } y \in \mathcal{O}_K\right\}\right| \lesssim_{K,s} (\log(H_K(P))+1)^\mu B^{s-1+\frac{1}{d_Y}}(\log(B))^\nu.$$

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] L. Bary-Soroker and A. Entin. Explicit Hilbert's irreducibility theorem in function fields. In *Abelian varieties and number theory*, volume 767 of *Contemp. Math.*, pages 125–134. Amer. Math. Soc., Providence, RI, 2021.

[3] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

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

[5] S. Bosch. *Lectures on formal and rigid geometry*, volume 2105 of *Lecture Notes in Mathematics*. Springer, Cham, 2014.

[6] T. D. Browning and D. R. Heath-Brown. Plane curves in boxes and equal sums of two powers. *Math. Z.*, 251(2):233–247, 2005.

[7] T. D. Browning, D. R. Heath-Brown, and P. Salberger. Counting rational points on algebraic varieties. *Duke Math. J.*, 132(3):545–578, 2006.

[8] A. Castillo and R. Dietmann. On Hilbert's irreducibility theorem. *Acta Arith.*, 180(1):1–14, 2017.

[9] W. Castryck, R. Cluckers, P. Dittmann, and K. H. Nguyen. The dimension growth conjecture, polynomial in the degree and without logarithmic factors. *Algebra Number Theory*, 14(8):2261–2294, 2020.

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

[11] P. Dèbes and Y. Walkowiak. Bounds for Hilbert's irreducibility theorem. *Pure Appl. Math. Q.*, 4(4, Special Issue: In honor of Jean-Pierre Serre. Part 1):1059–1083, 2008.

[12] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

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

[14] D. Hilbert. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 110:104–129, 1892.
[15] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
[16] M. W. Liebeck, L. Pyber, and A. Shalev. On a conjecture of G. E. Wall. *J. Algebra*, 317(1):184–197, 2007.
[17] J. Milne. *Fields and Galois Theory. https://www.jmilne.org/math/CourseNotes/FT.pdf*, 2021.
[18] F. Motte. On the Malle conjecture and the Grunwald problem. *arXiv e-prints*, page arXiv:1812.11376, Dec. 2018.
[19] M. Paredes and R. Sasyk. Uniform bounds for the number of rational points on varieties over global fields. *To appear in Algebra Number Theory*, page arXiv:2101.12174, Jan. 2021.
[20] P. Salberger. Counting rational point on projective varieties. *Preprint*, 2009.
[21] A. Schinzel and U. Zannier. The least admissible value of the parameter in Hilbert's irreducibility theorem. *Acta Arith.*, 69(3):293–302, 1995.
[22] J. P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.
[23] F. Vermeulen. Points of bounded height on curves and the dimension growth conjecture over $\mathbb{F}_q[t]$. *Bull. Lond. Math. Soc.*, 54(2):635–654, 2022.
[24] Y. Walkowiak. Théorème d'irréductibilité de Hilbert effectif. *Acta Arith.*, 116(4):343–362, 2005.
[25] M. N. Walsh. Bounded rational points on curves. *Int. Math. Res. Not. IMRN*, (14):5644–5658, 2015.
[26] D. Zywina. Hilbert's irreducibility theorem and the larger sieve. *arXiv e-prints*, page arXiv:1011.6465, Nov 2010.

[1]Instituto Argentino de Matemáticas Alberto P. Calderón-CONICET, Saavedra 15, Piso 3 (1083), Buenos Aires, Argentina;

[2]Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina.
Email address: mparedes@dm.uba.ar
Email address: rsasyk@dm.uba.ar