manuscripta math. 89, 107 - 137 (1996)

manuscripta mathematica

Hilbert Subsets and s-Integral Points

PIERRE DÈBES (*)

Received November 14, 1995

A classical tool for studying Hilbert's irreducibility theorem is Siegel's finiteness theorem for S-integral points on algebraic curves. We present a different approach based on s-integral points rather than S-integral points. Given an integer $s > 0$, an element t of a field K is said to be s-integral if the set of places $v \in M_K$ for which $|t|_v > 1$ is of cardinality $\leq s$ (instead of contained in S for "S-integral"). We prove a general diophantine result for s-integral points (Th.1.4). This result, unlike Siegel's theorem, is effective and is valid more generally for fields with the product formula. The main application to Hilbert's irreducibility theorem is a general criterion for a given Hilbert subset to contain values of given rational functions (Th.2.1). This criterion gives rise to very concrete applications : several examples are given (§2.5). Taking advantage of the effectiveness of our method, we can also produce elements of a given Hilbert subset of a number field with explicitely bounded height (Cor.3.7). Other applications, including the case that K is of characteristic $p > 0$, will be given in forthcoming papers ([8],[9]).

Hilbert subsets of a field K are classically defined to be the sets of the form

$$H_{P_1,\dots,P_n} = \{t \in K | P_i(t,Y) \text{ is irreducible in } K[Y], i = 1,\dots,n\},$$

where $P_i(T,Y)$ is an irreducible polynomial in $K(T)[Y]$, $i = 1,\dots,n$. Hilbert's irreducibility theorem asserts that Hilbert subsets of $\mathbb{Q}$ are infinite [14 ;Ch.9]. More generally, a field K with the same property is called *hilbertian*. Most of the applications of this paper are explicit forms of Hilbert's theorem. Furthermore, the base field K will only be assumed to be a field with the product formula [14 ;Ch.2]. From results of Weissauer and Uchida, such fields are known to be hilbertian if they are of characteristic 0 or, of characteristic

(*) Univ. Lille, 59655 Villeneuve d'Ascq, France. E-mail : pde@ccr.jussieu.fr

$p > 0$ and imperfect [12 ;Ch.11,14]. Number fields, regular function fields over a constant field k are typical examples.

A classical tool for studying the Hilbert property is Siegel's finiteness theorem for S-integral points on algebraic curves [14 ;Ch.8]. We follow a different approach based on *s-integral points* rather than S-integral points. Given an integer $s \geq 0$, an element $t \in K$ is said to be s-integral if the set of places $v \in M_K$ for which $|t|_v > 1$ is of cardinality $\leq s$. That is, the condition "of cardinality $\leq s$" replaces the condition "contained in S" in the usual definition of "S-integral point". For example, usual integers are 1-integral in $\mathbb{Q}$. In §1 we establish a general diophantine result for s-integral points (Th.1.4 below), which will play the role of Siegel's theorem. Th.1.4 uses a basic result due to Sprindzuk [20]. The main theorems of [5], which are more precise and more general variants of Sprindzuk's result, are recalled briefly in §1.1.

Let $\mathbf{P} = \{P_1, \ldots, P_m\}$ be a family of m polynomials in $K(T)[Y]$. For each $t \in K$, define $D_t(\mathbf{P})$ (resp. $D_t^+(\mathbf{P})$) to be the minimal (resp. maximal) degree over K of a field generated by m distinct elements $y_1(t), \ldots, y_m(t) \in \overline{K}$ such that $y_i(t)$ is a root of $P_i(t, Y)$, $i = 1, \ldots, m$. These definitions extend naturally to the points $t = \infty$ and $t = \text{gen}$, *i.e.*, respectively, the point at infinity and the generic point of $\mathbb{P}^1$ (see §1.3).

Theorem (Th.1.4) — *Assume that the polynomials $P_1, \ldots, P_m$ are separable over $K(T)$ and unramified above $T = \infty$. Then if t is an s-integral point of K of sufficiently large height $h(t)$, we have the inequality*

$$s\, D_\infty^+(\mathbf{P})\, D_t(\mathbf{P}) \geq D_{\text{gen}}(\mathbf{P}) \tag{1}$$

Geometrically, the condition "$P_i(T, Y)$ unramified above $T = \infty$" merely means that the function T has only simple poles on a smooth projective model of the curve $P_i(t, y) = 0$. We also use the phrase "∞ is not a branch point of $P_i(T, Y)$". Equivalently, the polynomial $P_i(T, Y)$ is totally split in $\overline{K}((1/T))$. This condition is not really restrictive, at least when ramification above $T = \infty$ is tame : one can indeed reduce to the unramified situation by some "blowing-up" $T \to T^e$ ($e > 0$).

Several papers, in particular of Bombieri [1], Sprindzuk [20] and the author [5], were devoted to the case of a single polynomial, *i.e.*, $m = 1$, in the eighties. We now explain why passing to the case of *several* polynomials is the main point of Th.1.4.

The following example, due to J. Coates [1], is a nice illustration of the case of a single polynomial $P(T, Y)$. Take $K = \mathbb{Q}$ and $s = 1$. Assume that P is irreducible in $K(T)[Y]$ (which implies $D_{\text{gen}}(P) = \deg_Y(P)$) and that the function induced by T on the algebraic curve with affine equation $P(t, y) = 0$ has at least two poles that are not conjugate over $\mathbb{Q}$ (which implies $D_\infty^+(P) < \deg_Y(P)$). Then it follows from inequality (1) that $D_t(P) > 1$ for all but finitely

many integers t, *i.e.*, there are only finitely many solutions to the equation $P(t,y) = 0$ with $(t,y) \in \mathbb{Z} \times \mathbb{Q}$ — a classical diophantine result of Runge. This is not fully satisfactory though. Indeed the situation where all the poles of T are simple and conjugate over K may happen quite often : this is the spirit of Hilbert's irreducibility theorem. In this case, $D_\infty^+(P) = \deg_Y(P) = D_{\text{gen}}(P)$ and inequality (1) is trivial.

On the contrary, inequality (1) always yields interesting conclusions for large m in situations where m varies and this holds : $D_{\text{gen}}(\mathbf{P})$ is increasing with m whereas $D_\infty^+(\mathbf{P})$ is bounded by a constant not depending on m. We will reduce to such situations in applications. This strategy already appears in some form in papers of Fried and Weissauer ([11],[21]). These papers appeared approximately at the same period as those of Bombieri, Sprindzuk and the author. Although the methods may look somewhat different — for example Weissauer uses non-standard analysis —, they seem to rest on common basic principles. They certainly all did influence the author. This paper can be considered as an attempt to unify and develop these various works.

The main applications of Th.1.4 are concerned with Hilbert's irreducibility theorem. In §2 we prove a quite general criterion for a Hilbert subset to contain values of given rational functions. More precisely, given a Hilbert subset $H_{P_1,\dots,P_n}$ of K, an infinite set $\mathbf{f}$ of non constant polynomials $f(T) \in K[T]$ and an integer $s > 0$, we define two assumptions on $P_1, \dots, P_n$ and $\mathbf{f}$, labeled (A), (B) and show the following.

Theorem (Th.2.1) — *Under assumptions (A), (B), there exists a finite subset* $\mathbf{f}_0 \subset \mathbf{f}$ *with this property :*

(2) For all s-integral points $t \in K$ of sufficiently large height, at least one out of the values $f(t)$ with $f \in \mathbf{f}_0$ lies in the Hilbert subset $H_{P_1,\dots,P_n}$.

Assumption (A) is that ∞ is not a branch point of $\mathbf{P}$, *i.e.*, that all polynomials $P_1, \dots, P_n$ are unramified over $T = \infty$. In characteristic 0, assumption (B) is that no more than one point $x \in \mathbb{P}^1(\overline{K})$ has the property that $f(x)$ is in the branch point set of $\mathbf{P}$ for infinitely many $f \in \mathbf{f}$. (There is an extra "tameness condition" in positive characteristic). §2.5 gives a first series of concrete applications of this general criterion. For example Cor.2.7 is an effective form of Weissauer's result (reproved by Fried with standard methods) that fields with the product formula are separably hilbertian. Here is another example. If the polynomials $P_1, \dots, P_n$ are unramified above $T = 1$ and $T = \infty$ and tamely ramified above $T = 0$, then there exists an integer M_o with the following property : there always is at least one element of $H_{P_1,\dots,P_n}$ among M_o consecutive powers $t, t^2, \dots, t^{M_o}$ of suitably large s-integers t (Cor.2.9). Over the rationals and for usual integers t, the same result is shown to hold with $M_o = 2$ (Prop.2.11). But Prop.2.11 uses Siegel's theorem. Cor.2.9 and Th.2.1 are more general : the base field K is any field with the product formula, possibly of characteristic p. This will be developed in [8]. Also "s-integral' is more

general than "S-integral" : for example, our method provides results on prime powers p^m (Cor.2.10).

Furthermore, unlike Siegel's theorem, our results are effective : for number fields, the constants involved are explicitely computable from the data. In §3 we prove this effective version of Hilbert's irreducibility theorem.

Theorem (Cor.3.7) — *Let $P_1, \dots, P_n$ be n irreducible polynomials in $\mathbb{Q}[T, Y] \setminus \mathbb{Q}[T]$. Then there exists in the Hilbert subset $H_{P_1,\dots,P_n}$ a rational number $x = u/v \in \mathbb{Q}$ of height*

$$h(x) = \max(\mathrm{Log}\,|u|, \mathrm{Log}\,|v|) \leq 10^{10} D^{100nD^2 \mathrm{Log}(D)} (H^2 + 1) \tag{3}$$

where $\deg(P_i) \leq D$ and $h(P_i) \leq H$, $i = 1, \dots, n$.

To our knowledge, no such result was known before. Furthermore, the underlying proof of Hilbert's theorem avoids several usual reductions, which turn out to be fairly expensive in terms of constants (Cf. Remark 3 of §2). A more precise algorithm is also given in §3 which, together with some results on the factorization of polynomials in one variable ([16], [15]), leads to the following result.

Theorem (Cor.3.8) — *Let $P_1, \dots, P_n$ be n irreducible polynomials in $\mathbb{Q}[T, Y] \setminus \mathbb{Q}[T]$, with degree $\leq D$ and logarithmic height $\leq H$. Then one can find a specific specialization $x \in H_{P_1,\dots,P_n}$ in time $H^{O(1)} \exp(nD^{O(1)})$.*

Using a different method, Schinzel and Zannier recently improved the bound in Cor.3.7 [18]. Their method however does not allow to improve Cor.3.8. Getting polynomial time in Cor.3.8, *i.e.*, replacing $\exp(D^{O(1)})$ by $D^{O(1)}$, seems to be a difficult problem. More general versions of Cor.3.7 (arbitrary number field as base field, several variables, etc.) are given in §3, which is the "effective" part of this paper. Some results of the first sections are followed by an "Addition to Th." which is concerned with the values of the constants involved in the number field case. These additions are systematically proved in §3.

We will devote a forthcoming paper [8] to further applications of Th.1.4. In particular, we will investigate more closely the case of a field K of characteristic $p > 0$, which, due to the possibility of unseparability and wild ramification, is more delicate and requires additional techniques. We only announce here two results of [8].

Theorem [8 ;Th.2.2] — *Let K be a field with the product formula. Let $P(T, Y) \in K(T)[Y]$ be a polynomial, absolutely irreducible and separable over $K(T)$. Assume further that $P(T, Y)$ is tamely ramified above $T = \infty$. Let b be an element of K of height $h(b) > 0$ such that*

(*) $b \notin K^\ell$ (i.e, b is not a ℓth power in K) for all primes ℓ and $-b \notin K^2$.

Then $P(b^m, Y)$ is irreducible for infinitely integers $m > 0$.

Theorem [8 ;Th.3.4] — *Let K be a global field. Let v_o be a place of K. Then every Hilbert subset of K is dense in $\prod_{v \neq v_o} K_v$ for the "strong approximation topology", i.e., the topology involved in the strong approximation theorem for global fields [2].*

These results were only known for number fields as a consequence of Siegel's theorem ([7] for the first one; [19 ;Ch.9.7], [17], [5] for the second one). In characteristic $p > 0$, the second result answers a question of B. Kunyavsky.

I wish to thank M. Chardin and M. Giusti for useful hints concerning the use of resultants in the last section and M. Fried for a thorough reading of the manuscript and many valuable suggestions.

NOTATION

Heights. We adhere to the notation of [14]. Let F be a field with a proper set M_F of absolute values satisfying the product formula with multiplicities 1. For each finite extension K of F, the set of absolute values of K extending those of M_F is a proper set M_K, satisfying the product formula with multiplicities $[K_v : F_v]$ for $v \in M_K$. For each integer $n \geq 1$, the (absolute logarithmic) height of points $(x_o, \ldots, x_n) \in \mathbb{P}^n(\overline{F})$ is then defined by

$$(4) \qquad h(x_o, \ldots, x_n) = \frac{1}{[K : F]} \sum_{v \in M_K} [K_v : F_v] \ \mathrm{Log}(\max(|x_o|_v, \ldots, |x_n|_v))$$

where K is any field containing $x_o, \ldots, x_n$. One defines the height of an element $x \in \overline{F}$ to be the height in $\mathbb{P}^1(\overline{F})$ of $(1, x)$. By height of a family of polynomials $P_1, \ldots, P_m$ we mean the height of the collection of the coefficients of $P_1, \ldots, P_m$. For a rational function $f \in \overline{K}(T)$, "$h(f) \leq h$" (respectively "$\deg(f) \leq d$") means that f can be written $f = A/B$ with $A, B \in \overline{K}(T)$ such that $h(A, B) \leq h$ (respectively $\max(\deg(A), \deg(B)) \leq d$). In the sequel, a field with the product formula is a finite extension K of a field F with the product formula with multiplicities 1 and the associated height is the one defined above.

Algebraic curves and function fields. Throughout this paper, by algebraic curve we mean a smooth projective geometrically irreducible curve defined over $\overline{K}$. There is a classical dictionnary between algebraic curves and irreducible polynomials in $\overline{K}[T, Y]$ or, equivalently, function fields in one variable over $\overline{K}$: points on curves correspond to places of fields and nonconstant morphisms between curves to field homomorphisms. In particular, if C is the algebraic curve associated to a polynomial $P(T, Y) \in K[T, Y]$, then each non constant rational function φ in the function field $K(T)[Y]/(P)$ induces a finite morphism $\varphi : C \to \mathbb{P}^1$ defined over K. This applies in particular to $\varphi = T$. Then we have $\deg(\varphi) = [\overline{K}(C) : \overline{K}(\varphi)] = \deg_Y P$.

Unramified fibers. A polynomial $P(T,Y) \in K(T)[Y]$ is said to be separable over $K(T)$ if it has no multiple roots in $\overline{K(T)}$. In that case, we say that a point $t_o \in \mathbb{P}^1(\overline{K})$ is not a branch point of $P(T,Y)$, or that $P(T,Y)$ is unramified above $T = t_o$, if $P(T,Y)$ is totally split in $\overline{K}((T-t_o))$ (as a polynomial in Y), *i.e.*, has $d = \deg_Y P$ distinct roots $y_1, \ldots, y_d$ in $\overline{K}((T-t_o))$. Then the field generated by the coefficients of y_i will be denoted by $K(y_i(t_o))$, $i = 1, \ldots, d$. When the polynomial $P(t_o,Y)$ has d distinct roots in $\overline{K}$, *i.e.*, when t_o is not a root of the discriminant $\Delta(T)$ of $P(T,Y)$ relative to Y, then y_i is a power series in $T - t_o$ and the field $K(y_i(t_o))$ is the field generated by the constant term of y_i, $i = 1, \ldots, d$. When $t_o = \infty$, $T - t_o$ should be replaced by $1/T$. For convenience, we note that these definitions can be generalized to include the case that $t_o = T$ is the generic point of $\mathbb{P}^1$: only replace in the above $\overline{K}((T-t_o))$ by $\overline{K(t_o)}((T-t_o))$. Then the generic point $t_o = T$ is not a branch point of $P(T,Y)$ and each of the Laurent series y solution of $P(t,y) = 0$ consists of a single constant term in $\overline{K(T)}$. If $P(T,Y)$ is absolutely irreducible (*i.e.*, irreducible in $\overline{K}(T)[Y]$) and $\varphi : C \longrightarrow \mathbb{P}^1$ is the finite morphism induced by T on the algebraic curve associated with $P(T,Y)$, then the points of C in the fiber $\varphi^{-1}(t_o)$ correspond to the distinct irreducible factors of $P(T,Y)$ in $\overline{K}((T-t_o))[Y]$. Thus, if t_o is not a branch point of $P(T,Y)$, then the fiber $\varphi^{-1}(t_o)$ consists of $d = \deg_Y P$ distinct points $Q_1, \ldots, Q_d$, which correspond to the distinct Laurent series $y_1, \ldots, y_d$ in $\overline{K}((T-t_o))$ solution of $P(T,y_i) = 0$. The field $K(y_i(t_o))$ corresponds to the field of definition $K(Q_i)$ of the point Q_i on C, $i = 1, \ldots, d$.

1 s-INTEGRAL POINTS

1.1 Sprindzuk's inequalities

In 1979, Sprindzuk proved a general result on the values of algebraic functions [20]. There were several variants of Sprindzuk's theorem in the eighties ([1], [5], [11]). To our knowledge, the most precise and most general ones were given in [5]. Th.1.1 below can be regarded as a slightly weakened but more practical form of these results. Several proofs of Sprindzuk's result were given. The most general one corresponds to an algebraic approach due to Bombieri [1]. His quite conceptual proof rests on Weil's decomposition theorem and the quadraticity of the canonical height on abelian varieties. Although Bombieri restricts to number fields, his proof is valid for any field K with the product formula. However there is a slight error in Bombieri's original paper. Correct statements and proofs can be found in [4] and [5]. Also, the constants involved in Bombieri's method can't seem to be easily computed. The effective part of Th.1.1 comes from another proof of Sprindzuk's result given in [5]. Like Sprindzuk's original one, this alternate proof involves analytical methods from the transcendental number theory.

Let K be a field with the product formula. Let $P(T,Y)$ be a polynomial, irreducible in $K(T)[Y]$, separable over $K(T)$ and unramified above $T = \infty$.

Denote the $d = \deg_Y(P)$ roots in $\overline{K}((1/T))$ of the polynomial $P(T,Y)$ by $y_1, \ldots, y_d$.

Theorem 1.1 — *There exist two constants A and B with the following property. Let $t \in K$ and $v \in M_K$. Then for any non constant divisor $D(Y) \in K[Y]$ of $P(t,Y)$, we have :*

$$(1) \qquad \frac{[K_v : F_v]\ \mathrm{Log}\,|t|_v}{\max\limits_{1\le i\le d}[K(y_i(\infty)) : F]} \le \frac{\deg(D)}{\deg_Y P} h(t) + A + B\sqrt{h(t)}$$

Addition to Th.1.1. *Assume further that K is a number field and that the polynomial $P(T,Y)$ is irreducible in $K[T,Y]$ and totally split in $\overline{K}[[1/T]]$. Then the constants A and B can be taken to be*

$$(2) \qquad \begin{cases} A = 15\deg(P)^2 h(P) + 136\deg(P)^3 + 3\deg(P)\,\mathrm{Log}(E) \\ B = 3\deg(P)^3 h(P) + 25\deg(P)^4 + \deg(P)^2\,\mathrm{Log}(E) \end{cases}$$

where E is the Eisenstein constant of the polynomial P, i.e., the l.c.m. of the Eisenstein constants of the Laurent series $y_1, \ldots, y_d \in \overline{K}((1/T))$ satisfying $P(T, y_i) = 0$, $i = 1, \ldots, d$.

Proof. We give two proofs corresponding to the two approaches of Sprindzuk's theorem. We refer to [5] for more details.

Geometrical viewpoint. Thanks to the assumption "$P(T,Y)$ separable over $K(T)$", one may restrict to the case where P is absolutely irreducible. In fact, the separability over K of the constant field of P is sufficient (see [3 ;Ch.5 §2]). Then the data can be viewed geometrically as follows : an algebraic curve C and a finite separable morphism $\varphi : C \to \mathbb{P}^1$, both defined over K ; furthermore, the map φ is assumed to have only simple poles. By taking A sufficiently large one may assume that t is not a root of the discriminant $\Delta(T)$ of $P(T,Y)$. Then the roots of $P(t,Y)$ correspond to the points in the fiber $\varphi^{-1}(t)$. Let M be a point in this fiber that corresponds to a root of the divisor $D(Y)$ of $P(t,Y)$ and let $\bar{v}$ be an extension to $\overline{K}$ of the given place $v \in M_K$.

If M is $\bar{v}$-adically suitably close to some pole Q of φ(*), one may apply Th.3 of [5] to obtain

$$(3) \qquad \frac{[K(Q,M)_{\bar{v}} : F_v]}{[K(Q,M) : F]}\ \mathrm{Log}^+\,|\varphi(M)|_v \le \frac{1}{\deg(\varphi)} h(\varphi(M)) + O(\sqrt{h(\varphi(M))})$$

(*) The exact condition on M is that, for some pole Q of φ, we have $\lambda_Q(M,v) > \delta_v$ where λ_Q is the Weil function associated to the divisor (Q) and $(\delta_v)_{v\in M_k}$ is a certain M_k-constant depending on the zeroes and poles of φ (here k is a field of rationality for C, φ and the zeroes and poles of φ). The M_k-constant $(\delta_v)_{v\in M_k}$ is the one that appears in Th.3 of [5]

Then use the inequalities

$$(4) \qquad \begin{cases} [K(Q,M):F] \leq [K(Q):F]\,[K(M):K] \\ [K(Q,M)_{\bar{v}}:F_v] \geq [K_v:F_v] \end{cases}$$

to obtain

$$(5) \qquad \frac{[K_v:F_v]\ \mathrm{Log}\,|\varphi(M)|_v}{\max\limits_{\varphi(Q)=\infty}[K(Q):F]} \leq \frac{[K(M):K]}{\deg(\varphi)}\,h(\varphi(M)) + O\left(\sqrt{h(\varphi(M))}\right)$$

which is the geometrical form of (1).

If M is $\bar{v}$-adically "far from" all the poles of φ(**), then Weil's decomposition theorem [14 ;Ch.10] readily shows that the lefthand term in (3) can be bounded even more sharply by a term $O(1)$. □

Arithmetical viewpoint (in characteristic 0 only). We can restrict to the case

$$\frac{[K_v:F_v]\ \mathrm{Log}\,|t|_v}{\max\limits_{1\leq i\leq d}[K(y_i(\infty)):F]} > A$$

Indeed (1) is trivial in the opposite case. Then taking A suitably large insures that the power series $y_i(t)$ are convergent in K_v, $i=1,\ldots,d$. The corresponding sums, $y_{i,v}(t)$, $i=1,\ldots,d$, are the d roots of $P(t,Y)$. At least one of them is a root of $D(Y)$. Then Th.2 of [5] (with $X=1/T$) yields the required inequality. □

Remark 1. There is no preliminary reduction to the "absolutely irreducible" case in the arithmetical proof : Th.2 of [5] was proved directly under the more general hypothesis "$P(T,Y)$ irreducible in $K[T,Y]$". This "irreducible vs absolutely irreducible" question is not a totally minor point. In the sequel, we will apply Th.1.1 to a composite field extension $K(T,y_1,\ldots,y_m)$. This extension may have a non trivial constant field even though the function fields $K(T,y_i)$, $i=1,\ldots,r$ do not (take $y_1=\sqrt{1+T}$ and $y_2=\sqrt{2(1+T)}$).

(**) According to the previous footnote, the precise condition is that $\lambda_Q(M,\bar{v}) \leq \delta_{\bar{v}}$ for all poles Q of φ. That the left-hand side term of (3) can be bounded by a term $O(1)$ immediately follows from Th.3.7 p.263 of [14]

1.2 s-integral points

Definition 1.2 — *Given an integer $s \geq 0$, an element $t \in K$ is said to be s-integral in K if the number of places $v \in M_K$ such that $|t|_v > 1$ is less than or equal to s.*

Classically, if S is a finite subset of M_K containing the archimedean places in M_K, S-integral points are defined to be the points $t \in K$ such that all the places $v \in M_K$ for which $|t|_v > 1$ are contained in S. If $|S| \leq s$, S-integral points are s-integral. The point of the notion of "s-integral point" is this. If $s > 0$ then s-integral points $t \in K$ satisfy this condition :

(6) For at least one place $v \in M_K$ we have $\dfrac{[K_v : F_v]}{[K : F]} \operatorname{Log} |t|_v \geq \dfrac{h(t)}{s}$

Th.1.1 has this consequence.

Corollary 1.3 — *Under the assumptions of Th.1.1, there exists a constant $h_o = h_o(P)$ with the following property. Let t be s-integral in K and of height $h(t) > h_o s^2$. Then for each root $y(t) \in \overline{K}$ of $P(t, Y)$, we have*

$$(7) \qquad [K(y(t)) : K] \geq \frac{\deg_Y P}{s \max\limits_{1 \leq i \leq d} [K(y_i(\infty)) : K]}$$

Addition to Cor.1.3. *Assume further that K is a number field and that the polynomial $P(T, Y)$ is irreducible in $K[T, Y]$ and totally split in $\overline{K}[[1/T]]$. Then the constant $h_o = h_o(P)$ can be taken to be*

$$(8) \qquad h_o = 2700 \deg(P)^{12} + 48 \deg(P)^{10} h(P)^2 + 12 \deg(P)^8 (\operatorname{Log}(E))^2$$

Proof. Let $D(Y) \in K[Y]$ be the irreducible polynomial of $y(t)$ over K. Apply Th.1.1 to this divisor $D(Y)$ of $P(t, Y)$ and to a place v for which the inequality of (6) holds. Conclude that

$$\frac{h(t)}{s \max\limits_{1 \leq i \leq d} [K(y_i(\infty)) : K]} \leq \frac{\deg(D)}{\deg_Y P} h(t) + A + B\sqrt{h(t)}$$

This leads to the announced inequality (7) provided that t is of suitably large height (the precise condition is easily seen to be of the form $h(t) > h_o s^2$). □

As already mentioned in the introduction, Coates noticed that Cor.1.3 contains the following classical diophantine result due to Runge : take $K = \mathbb{Q}$, if

the function T on the curve $P(t,y)=0$ has at least two poles that are not conjugate over $\mathbb{Q}$, then the equation $P(t,y)=0$ has only finitely many solutions $(t,y)\in\mathbb{Z}^2$. Unfortunately the situation where all the poles of φ are simple and conjugate over $\mathbb{Q}$, in which case inequality (7) is trivial, may happen quite often. Indeed this is the spirit of Hilbert's irreducibility theorem. In the next paragraph, we show that this difficulty disappears when one works with several curves.

1.3 Main result

From now on, fix an algebraic closure $\overline{K}$ of K and an algebraic closure $\overline{K(T)}$ of $\overline{K}(T)$. Let $\mathbf{P}=\{P_1(T,Y),\dots,P_m(T,Y)\}$ be a family of (not necessarily distinct) polynomials in $K(T)[Y]$. For $i=1,\dots,n$, denote the branch point set of $P_i(T,Y)$ by $Br(P_i)$ and set $Br(\mathbf{P})=\bigcup_{1\le i\le n}Br(P_i)$. For each point $t\in\mathbb{P}^1\setminus Br(\mathbf{P})$, define the parameters $D_t(\mathbf{P})$ and $D_t^+(\mathbf{P})$ by the following formulas

$$\text{(9)}\qquad \begin{cases} D_t(\mathbf{P})=\min\limits_{(y_1,\dots,y_m)}\,[K(t,y_1(t),\dots,y_m(t)):K(t)] \\ D_t^+(\mathbf{P})=\max\limits_{(y_1,\dots,y_m)}\,[K(t,y_1(t),\dots,y_m(t)):K(t)] \end{cases}$$

where in the "min" and in the "max", $(y_1,\dots,y_m)$ ranges over all m-tuples with ith entry a root $y_i\in\overline{K}((T-t))$ of $P_i(T,Y)$ and with no two equal entries. The field $K(t,y_1(t),\dots,y_m(t))$ should be understood as the compositum of the fields $K(t),K(y_1(t)),\dots,K(y_m(t))$ (which are precisely defined in Notation). When $t=T$ is the generic point of $\mathbb{P}^1$, we use the subscript "gen" instead of "t". Recall that in this case, $\overline{K}((T-t))$ should be replaced by $\overline{K(T)}$.

Remark 2. In the special case where the polynomial $P_i(t,Y)$ has $\deg_Y P_i$ simple roots in $\overline{K}$, $i=1,\dots,m$, $D_t(\mathbf{P})$ (resp. $D_t^+(\mathbf{P})$) is the minimal (resp. maximal) degree over K of a field generated by m distinct elements $y_1(t),\dots,y_m(t)\in\overline{K}$ such that $y_i(t)$ is a root of $P_i(t,Y)$, $i=1,\dots,m$. This holds if t is not a root of the discriminant $\Delta_i(T)\in K(T)$ of $P_i(T,Y)$, $i=1,\dots,m$, (so in particular for all $t\in K$ of sufficiently large height). Similar statements are obtained for $t=\infty$ by changing T to $1/T$.

Theorem 1.4 — *Assume that the polynomials $P_1(T,Y),\dots,P_m(T,Y)$ are separable over $K(T)$ and unramified above $T=\infty$. Let $s>0$ be an integer. There exists a constant $h_1=h_1(\mathbf{P})$ depending on $\mathbf{P}=\{P_1,\dots,P_m\}$ with the following property. If t is s-integral in K and if $h(t)>h_1 s^2$, then $t\notin Br(\mathbf{P})$ and*

$$\text{(10)}\qquad s\,D_\infty^+(\mathbf{P})\,D_t(\mathbf{P})\ge D_{\mathrm{gen}}(\mathbf{P})$$

Addition to Th.1.4. *Assume further that K is a number field and that the polynomials $P_1, \dots, P_m$ are in $K[T,Y]$ and satisfy this condition*

(11) *0 is not a root of the discriminant of the polynomials $P_i(1/T,Y)$, $i = 1,\dots,m$,*

then the constant h_1 can be taken to be

$$h_1 = 2^{15m+4} D^{14m} (H^2 + 800) \tag{12}$$

where $h(P_i) \leq H$ and $\deg(P_i) \leq D$, $i = 1,\dots,m$.

Cor.1.3 corresponds to the special case $m = 1$ of Th.1.4. But in general m has to be taken > 1 so that (10) is not trivial. Indeed for $m = 1$, the ratio $D_{\text{gen}}(\mathbf{P})/D^+_\infty(\mathbf{P})$ may be equal to 1, in which case inequality (10) reduces to $sD_t(\mathbf{P}) \geq 1$. On the contrary, inequality (10) always yields interesting conclusions for large m if one can arrange for this to hold : $D_{\text{gen}}(\mathbf{P})$ is increasing with m whereas $D^+_\infty(\mathbf{P})$ is bounded by a constant not depending on m. That will be the case in our applications. This idea already appears implicitly as a basic principle of the proofs of Fried and Weissauer that a field with the product formula of characteristic 0 is hilbertian ([12 ;Ch.14]).

Proof of Th.1.4. Let t be s-integral in K and $y_1(t), \dots, y_m(t)$ be m distinct elements of $\overline{K}$ such that $P_i(t, y_i(t)) = 0$, $i = 1,\dots,m$. One may assume that $h(t)$ is large enough to guarantee that the polynomial $P_i(t,Y)$ has only simple roots in $\overline{K}$, $i = 1,\dots,m$. Consequently, there exists a unique power series $y_i \in \overline{K}[[T-t]]$ with constant term equal to $y_i(t)$ such that $P_i(T, y_i) = 0$, $i = 1,\dots,m$. These power series $y_1, \dots, y_m$ are necessarily distinct for their constant terms are. Consider the function field $K(T, y_1, \dots, y_m)$. From the separability assumption, the extension $K(T, y_1, \dots, y_m)/K(T)$ has a primitive element z. A field with the product formula is necessarily infinite ; it is classical then that z can be taken of the form

$$z = c_1 y_1 + \cdots + c_m y_m, \text{ with } c_i \in K, i = 1,\dots,m \tag{13}$$

Let $P(T,Y)$ be irreducible in $K[T,Y]$ and such that $P(T,z) = 0$. From the assumptions, all the conjugates of y_i over $\overline{K}(T)$ are in $\overline{K}((1/T))$, $i = 1,\dots,m$. Therefore the polynomial $P(T,Y)$ is totally split in $\overline{K}((1/T))$. More precisely, each root $z_\infty \in \overline{K}((1/T))$ of $P(T,Y)$ can be written out

$$z_\infty = c_1 y_{1\infty} + \cdots + c_m y_{m\infty}$$

with $y_{i\infty} \in \overline{K}((1/T))$ a root of $P_i(T,Y)$. This shows that

$$[K(z_\infty(\infty)) : K] \leq D^+_\infty(\mathbf{P})$$

Now by construction the element $c_1y_1(t)+\cdots+c_my_m(t)$ is a root in $\overline{K}$ of the polynomial $P(t,Y)$. Apply Cor.1.3 to get

$$[K(c_1y_1(t)+\cdots+c_my_m(t)):K]\geq\frac{\deg_Y P}{s\ D^+_\infty(\mathbf{P})} \tag{14}$$

provided $h(t)>h_1s^2$ where $h_1=h_o(P)$ is the constant of Cor.1.3 associated with the polynomial P. Inequality (10) easily follows from these inequalities

$$\begin{cases}\deg_Y P=[K(T,y_1,\ldots,y_m):K(T)]\geq D_{\text{gen}}(\mathbf{P})\\ [K(c_1y_1(t)+\cdots+c_my_m(t)):K]\leq[K(y_1(t),\ldots,y_m(t):K]\end{cases}\quad\square \tag{15}$$

Remark 3. (a) The proof actually shows this more precise inequality : if t is s-integral in K and if $h(t)>h_1s^2$, then

$$s\ D^+_\infty(\mathbf{P})\ [K(y_1(t),\ldots,y_m(t):K]\geq[K(T,y_1,\ldots,y_m):K(T)] \tag{16}$$

where $y_i\in\overline{K}[[T-t]]$ is the unique power series with constant term equal to $y_i(t)$ such that $P_i(T,y_i)=0$, $i=1,\ldots,m$.

(b) The proof of Th.1.4 can be presented in a more geometrical way by using fiber products of curves. Indeed, regard the polynomial $P_i(T,Y)$ as an algebraic curve C_i and the T variable as a morphism $\varphi_i:C_i\to\mathbb{P}^1$, $i=1,\ldots,m$. Denote the fiber product of $C_1,\ldots,C_m$ over the maps $\varphi_1,\ldots,\varphi_m$ by $\mathfrak{C}_m$ and the map $\mathfrak{C}_m\to\mathbb{P}^1$ extending the φ_is by Φ_m. For each point t for suitably large height, the r-tuple $(y_1(t),\ldots,y_m(t))$ correspond to some point $M=(M_1,\ldots,M_m)$ on $\mathfrak{C}_m$. The argument of the proof of Th.1.4 essentially consists in applying Th.1.1 in its geometrical form (5) (or its corollary 1.3) to the irreducible component of $\mathfrak{C}_m$ that contains $M=(M_1,\ldots,M_m)$.

2 HILBERT SUBSETS

2.1 Statement of the result

Let $\mathbf{P}=\{P_1(T,Y),\ldots,P_n(T,Y)\}$ be a family of n polynomials absolutely irreducible and separable over $K(T)$ and such that $\deg_Y P_i\geq 2$, $i=1,\ldots,n$. Under suitable assumptions, Th.2.1 below produces explicit elements of the Hilbert subset $H_{P_1,\ldots,P_n}$. As before $Br(\mathbf{P})$ is the union of the branch point sets of the polynomials $P_1(T,Y),\ldots,P_n(T,Y)$. A point $a\in\mathbb{P}^1$ is called a *tamely ramified* branch point of $\mathbf{P}$ if the polynomials $P_i(T,Y)$, $i=1,\ldots,n$ are tamely ramified above $T=a$, that is, if K is of characteristic 0 or of characteristic $p>0$ with p dividing none of the degrees of the irreducible factors of $P_i(T,Y)$ in $\overline{K}((T-a))$, $i=1,\ldots,n$.

Let $\mathbf{f}$ be an infinite set of non constant rational functions $f(T) \in K(T)\backslash K$. A point $x \in \mathbb{P}^1(\overline{K})$ is called *exceptional* for $\mathbf{f}$ if there exists an element $t \in \mathbb{P}^1(\overline{K})$ such that $f(x) = t$ for infinitely many $f \in \mathbf{f}$. A point $x \in \mathbb{P}^1(\overline{K})$ is called *exceptional for* $\mathbf{f}$ *relative to* $\mathbf{P}$ if

(1) There is some $t \in Br(\mathbf{P})$ such that $f(x) = t$ for infinitely many $f \in \mathbf{f}$.

An exceptional point x for $\mathbf{f}$ relative to $\mathbf{P}$ is called *regular* if the t in the definition (1) can be taken to be a *tamely* ramified branch point of $\mathbf{P}$.

Let $\mathbf{f}$ be an infinite set of non constant polynomials $f(T) \in K[T]\backslash K$. Th.2.1 has these two basic assumptions.

(A) $\infty \notin Br(\mathbf{P})$, *i.e.*, the polynomials $P_1, \ldots, P_n$ are unramified over $T = \infty$.

(B) Either there is no exceptional point for $\mathbf{f}$ relative to $\mathbf{P}$, or, there is a unique one, which, in addition, should be regular.

Theorem 2.1 — *Assume that conditions (A) and (B) hold. Let $s > 0$ be an integer. Then there exist a constant $h_2 > 0$ and a finite subset $\mathbf{f}_o$ of $\mathbf{f}$ with the following property. If t is any s-integral point in K of height $h(t) > h_2 s^2$, there exists a polynomial $f \in \mathbf{f}_o$ such that $f(t)$ lies in the Hilbert subset $H_{P_1,\ldots,P_n}$.*

Addition to Th.2.1. *Let $m_o > 0$ be an integer such that*

$$2^{m_o} > s(\deg_Y P_1)! \cdots (\deg_Y P_n)! \tag{2}$$

Under conditions (A), (B), the finite subset $\mathbf{f}_o$ can be taken to be the set consisting of the m_o first terms of a sequence $(f_m)_{m>0}$ satisfying condition (4) of Lemma 2.4. Assume further that K is a number field and that the polynomials $P_i(f_j(T), Y)$, $i = 1, \ldots, n$, $j = 1, \ldots, m_o$, satisfy condition (11) of Th.1.4. Then the constant h_2 can be taken to be

$$h_2 = 2^{15m_o+4}\,(DD(\mathbf{f}_o))^{14m_o+2}\,(3H^2 + 3H(\mathbf{f}_o)^2 + 812) \tag{3}$$

where as usual $\deg_Y P_i \leq D$, $h(P_i) \leq H$, $i = 1, \ldots, n$ and $D(\mathbf{f}_o)$ and $H(\mathbf{f}_o)$ are integers such that $\deg f_j \leq D(\mathbf{f}_o)$ and $h(f_j) \leq H(\mathbf{f}_o)$, $j = 1, \ldots, m_o$.

Remark 1. In Th.2.1, $\mathbf{f}$ is a set of non-constant polynomials. More generally, $\mathbf{f}$ can be taken to be an infinite set of non-constant rational functions $f(T) \in K(T)\backslash K$. Condition (A) should be then replaced by the more general condition

(A) The set $\mathbf{f}(\infty) = \{f(\infty) \mid f \in \mathbf{f}\}$ consists of a single point $\omega \in \mathbb{P}^1(\overline{K})$, not a branch point of $\mathbf{P}$. Furthermore the point ω is a totally ramified point of each of the covers $f : \mathbb{P}^1 \to \mathbb{P}^1$ induced by the rational functions $f \in \mathbf{f}$.

Our proof of Th.2.1 can be used without any change in this more general context. This remark is used in Example 3 of §2.5.

2.2 General results

The proof of Th.2.1 is given in §2.3 and §2.4. We start with some general results involved in this proof and in other places of the paper.

Proposition 2.2 — *Let $P(T,Y) \in K(T)[Y]$ be a polynomial, irreducible and separable over $K(T)$ and $f(T) \in K(T)$ be a rational function. Let $a \in \mathbb{P}^1(K)$ and set $b = f(a)$. Assume that $P(T,Y)$ is unramified over $T = b$. Then*

(a) The polynomial $P(f(T),Y)$ is unramified over $T = a$.

Let $\mathbf{P}(d)$ be the family of polynomials consisting of P repeated $d = \deg_Y P$ times.

(b) The field generated by the coefficients of the Laurent series $y \in \overline{K}((T-a))$ solution of $P(f(T),y) = 0$ is an extension of K of degree $\leq D_b^+(\mathbf{P}(d))$.

(c) The term $D_b^+(\mathbf{P}(d))$ can be bounded from above independently on b by $\deg_Y(P)$!

Proof. The rational function $f(T) - b$ can be expanded as a power series in $T - a$ with coefficients in K and with constant term equal to 0. It follows that, if $y(T-b) \in \overline{K}((T-b))$ is any root of $P(T,Y)$, then $f(T)$ can be substituted for T in $y(T-b)$ to give a root $y(f(T)-b) \in \overline{K}((T-a))$ of $P(f(T),Y)$. This proves (a). Furthermore the coefficients of $y(f(T)-b) \in \overline{K}((T-a))$ lie in the field $K(y(b))$ of the coefficients ot the initial Laurent series $y(T-b)$. Thus (b) follows from the definition of $D_b^+(\mathbf{P}(d))$. It remains to prove (c). Let $y_1, \ldots, y_d$ be the d roots in $\overline{K}((T-b))$ of the polynomial $P(T,Y)$ and let $\zeta_1, \ldots, \zeta_d$ be r K-linearly independent elements of $K(y_1(b), \ldots, y_d(b))$. We wish to show that $r \leq d!$. Observe that there exist

$$Z_1, \ldots, Z_r \in K(T, y_1, \ldots, y_d) \cap \overline{K}[[T-b]]$$

such that $Z_i(b) = \zeta_i$, $i = 1, \ldots, r$. Now $Z_1, \ldots, Z_r$ are automatically linearly independent over $K(T)$. Conclude that $r \leq [K(T, y_1, \ldots, y_d) : K(T)]$. This last dimension is clearly $\leq d!$. □

Proposition 2.3 — *Let $P(T,Y) \in K[T,Y]$ be an absolutely irreducible polynomial and $f(T) \in K(T) \setminus K$ be a nonconstant rational function. If $f(\infty) = \omega$ is a totally ramified point of the cover $f : \mathbb{P}^1 \to \mathbb{P}^1$ but is not a branch point of P, then the polynomial $P(f(T),Y)$ is absolutely irreducible.*

In particular, under condition (A) of Th.2.1, the polynomials $P_i(f(T),Y)$ are absolutely irreducible, for all $f \in \mathbf{f}$, $i = 1, \ldots, n$.

Proof. Recall from the introduction that if $f(T) = A(T)/B(T)$ with A and B relatively prime in $K[T]$, then $f(\infty) = \omega$ is a totally ramified point of the cover $f : \mathbb{P}^1 \to \mathbb{P}^1$ if and only if the polynomial $A(Y) - TB(Y)$ is irreducible in $\overline{K}((T-\omega))$. Now, if $\omega \notin Br(P)$, the splitting field N of $P(T,Y)$ over $\overline{K}(T)$ is contained in $\overline{K}((T-\omega))$. Conclude then that the polynomial $A(Y) - TB(Y)$ is irreducible over N. Now if $y(T), U \in \overline{K(T)}$ respectively denote a root in Y of the polynomials $P(T,Y)$ and $f(Y) - T$, this implies that the field extensions $\overline{K}(T, y(T))/\overline{K}(T)$ and $\overline{K}(U)/\overline{K}(T)$ are linearly disjoint over $\overline{K}(T)$. Conclude that

$$[\overline{K}(U, y(T)) : \overline{K}(U)] = [\overline{K}(T, y(T)) : \overline{K}(T)] = \deg_Y(P)$$

and so that $P(f(U), Y)$ is irreducible over $\overline{K}(U)$. □

2.3 Proof of Th.2.1 : a preliminary lemma

Assume conditions (A), (B) hold. Under condition (B),

- either there exists a unique exceptional point α for $\mathbf{f}$ relative to $\mathbf{P}$, that is, α is the only point in $\mathbb{P}^1(\overline{K})$ such that $f(\alpha) \in Br(\mathbf{P})$ for infinitely many $f \in \mathbf{f}$. Furthermore, the exceptional point α is regular, that is, there exists a tamely ramified branch point a of $\mathbf{P}$ with $f(\alpha) = a$ for infinitely many $f \in \mathbf{f}$.

- or, there is no exceptional point for $\mathbf{f}$ relative to $\mathbf{P}$. In that case, set $\alpha = \infty$ and $a = \infty$ (or $a = \omega$ in the more general context of Remark 1).

Lemma 2.4 — *(a) There exists a sequence $(f_m)_{m>0}$ of elements of $\mathbf{f}$ such that*

$$(4) \qquad \begin{cases} f_m(\alpha) = a \\ f_m^{-1}(Br(\mathbf{P})) \cap f_{m'}^{-1}(Br(\mathbf{P})) \subset \{\alpha\} \end{cases}$$

for all distinct integers $m, m' > 0$.

(b) If $(f_m)_{m>0}$ is any sequence of $\mathbf{f}$ satisfying (4), then we have the following conclusion.

(5) Denote the splitting field over $\overline{K}(T)$ of the polynomial $P_i(f_m(T), Y)$ by E_{im}, $i = 1, \ldots, n$, $m > 0$. For all $m \geq 0$ and $i = 1, \ldots, n$, if $y_{i\,m+1} \in \overline{K(T)}$ is an arbitrary root of $P_i(f_{m+1}(T), y_{i\,m+1}) = 0$, then the extension $\overline{K}(T, y_{i\,m+1})$ is linearly disjoint from the extension $E_{11} \cdots E_{n1} \cdots E_{1m} \cdots E_{nm}$ over $\overline{K}(T)$.

Proof. (a) The sequence $(f_m)_{m>0}$ is defined inductively. Let $\mathbf{f}_{\alpha,a}$ be the subset of $\mathbf{f}$ of all $f \in \mathbf{f}$ such that $f(\alpha) = a$. Pick f_1 in $\mathbf{f}_{\alpha,a}$. Then, given $f_1, \ldots, f_M$ satisfying (4) for all distinct integers $m, m' = 1, \ldots, M$, consider the set

$$S = \bigcup_{1 \le j \le M} f_j^{-1}(Br(\mathbf{P}))$$

We need to prove that there exists an element $f_{M+1} \in \mathbf{f}_{\alpha,a}$ distinct from $f_1, \dots, f_M$ such that $f_{M+1}^{-1}(Br(\mathbf{P})) \cap S \subset \{\alpha\}$. Assume the contrary holds. Then, since $Br(\mathbf{P})$ and S are finite and $\mathbf{f}_{\alpha,a}$ is infinite, there exists $r \in Br(\mathbf{P})$ and $s \in S$, $s \neq \alpha$ such that $f(s) = r$ for infinitely many $f \in \mathbf{f}$. This contradicts assumption (B).

(b) Suppose given in general a sequence $(f_m)_{m>0}$ of elements of $\mathbf{f}$ satisfying (4). Fix an integer $m \geq 0$. From Prop.2.2, if y_{ij} is an arbitrary root of $P_i(f_j(T), Y)$, then the branch point set of the extension $\overline{K}(T, y_{ij})/\overline{K}(T)$ is contained in $f_j^{-1}(Br(\mathbf{P}))$, $i = 1, \dots, n$ and $j > 0$. Classically, extensions that are conjugate over $\overline{K}(T)$ have the same branch points; also the branch point set of a compositum of function fields is the union of the branch point sets of the function fields; in addition, ramification remains tame in the compositum extension if it is in the original function fields. Thus it follows from (4) that the extension

$$\widehat{\overline{K}(T, y_{i\,m+1})} \cap E_{11} \cdots E_{n1} \cdots E_{1m} \cdots E_{nm} \tag{6}$$

of $\overline{K}$ can have only one branch point, namely α, $i = 1, \dots, n$. The "hat" indicates that we took the Galois closure over $\overline{K}(T)$. In addition, ramification above α in this extension is tame. It is a classical consequence of Hurwitz's formula [13 ;Ch.4] that this forces the extension (6) to be trivial. And that implies the linearly disjointness statement of Lemma 2.4.

Remark 2. Denote the set of exceptional points for $\mathbf{f}$, *i.e.*, such that there exists an element $t \in \mathbb{P}^1(\overline{K})$ such that $f(x) = t$ for infinitely many $f \in \mathbf{f}$, by $Exc(\mathbf{f})$. Given the set $\mathbf{f}$, a natural assumption that insures that condition (B) (and so conclusion (a) of Lemma 2.4) holds is that the values $t = f(x)$ that correspond to exceptional points $x \in Exc(\mathbf{f})$ do not meet the branch point set $Br(\mathbf{P})$, or at most in one point (which should in addition be a tamely ramified branch point).

Consider the special case $\mathbf{f} = \{T^m | m > 0\}$. Then both the set $Exc(\mathbf{f})$ and the set of corresponding values t consist of 0, 1, ∞ and all roots of unity in $\overline{K}$. The natural assumption above that insures condition (B) is that none of these elements (except possibly one) lie in the branch point set $Br(\mathbf{P})$. In that special case however, the weaker condition

(7) $\infty, 1 \notin Br(\mathbf{P})$ and 0 is a tamely ramified branch point set of $\mathbf{P}$

guarantees conclusion (a) of Lemma 2.4. In other words, roots of 1 other than 1 can be disregarded.

Indeed take $\alpha = a = 0$. The proof of conclusion (a) of Lemma 2.4 is the same as above except that the end of the argument should be replaced by this :

"Since $Br(\mathbf{P})$ and S are finite, there exists $r \in Br(\mathbf{P})$ and $s \in S$, $s \neq 0$ such that $f(s) = r$ for infinitely many $f \in \mathbf{f}$ of the form $f(T) = T^k$ with k a suitably large multiple of all the orders of roots of unity in S. Since $s \neq 0$ and $\infty \notin Br(\mathbf{P})$, the only possibility is that s is a root of 1. But then $r = f(s) = 1$, which contradicts "$1 \notin Br(\mathbf{P})$"."

This remark will be used in Example 4 of §2.5.

2.4 End of proof of Th.2.1

Part 1 : The basic inequality. Let $(f_m)_{m>0}$ be a sequence of elements of $\mathbf{f}$. Let $s > 0$ be an integer. Fix an integer $m > 0$ such that

$$2^m > s(\deg_Y P_1)! \cdots (\deg_Y P_n)! \tag{8}$$

With no loss we may assume that the polynomials $P_i(f_j(T), Y)$, $i = 1, \ldots, m$, $j = 1, \ldots, m$ are irreducible in $K[T, Y]$: if necessary, multiply these polynomials by suitable elements in $K[T]$. Let h_2 be the largest one of the constants h_1 of Th.1.4 associated with the families

$$\mathbf{P}_{\mathbf{i}}(\mathbf{f}_m) = \{P_{i_1}(f_1(T), Y), \ldots, P_{i_m}(f_m(T), Y)\}$$

where $\mathbf{i} = (i_1, \ldots, i_m)$ ranges over all families of indices $i_j \in \{1, \ldots, n\}$ indexed by $\{1, \ldots, m\}$. Let t be an s-integral point of K of height $h(t) > h_2 s^2$. Let $\delta_1, \ldots, \delta_n$ be n positive real numbers.

Assume that for each $j = 1, \ldots, m$ there exists $i_j \in \{1, \ldots, n\}$ such that the polynomial $P_{i_j}(f_j(t), Y)$ has a root $y_j(t) \in \overline{K}$ of degree $[K(y_j(t) : K] \leq \delta_{i_j}$. Consider the family of polynomials $\mathbf{P}_{\mathbf{i}}(\mathbf{f}) = \{P_{i_1}(f_1(T), Y), \ldots, P_{i_m}(f_m(T), Y)\}$. They are separable over $K(T)$ since the polynomials $P_1, \ldots, P_n$ are. From assumption *(A)* and Prop.2.2 (a), they are unramified above $T = \infty$. Applying Th.1.4 to the family $\mathbf{P}_{\mathbf{i}}(\mathbf{f})$ gives

$$\delta_{i_1} \cdots \delta_{i_m} \geq [K(y_1(t), \ldots, y_m(t)) : K] \geq \frac{D_{\mathrm{gen}}(\mathbf{P}_{\mathbf{i}}(\mathbf{f}))}{s D_\infty^+(\mathbf{P}_{\mathbf{i}}(\mathbf{f}))} \tag{9}$$

Now it follows from Prop.2.2 (b) that

$$D_\infty^+(\mathbf{P}_{\mathbf{i}}(\mathbf{f})) \leq \prod_{1 \leq i \leq n} D_\omega^+(\mathbf{P}_{\mathbf{i}}(d_i)) \tag{10}$$

where $\mathbf{P}_{\mathbf{i}}(d_i)$ is the family of polynomials consisting of P_i repeated $d_i = \deg_Y P_i$ times, $i = 1, \ldots, n$. Use Prop.2.2 (c) and substitute (10) back in (9) to obtain

$$D_{\text{gen}}(\mathbf{P_i(f)}) \leq s(\deg_Y P_1)! \cdots (\deg_Y P_n)!\ \delta_{i_1} \cdots \delta_{i_m} \tag{11}$$

Part 2 : Conclusion of the proof. In this part, the sequence $(f_m)_{m>0}$ is selected to be a sequence of elements of $\mathbf{f}$ satisfying condition (5) of Lemma 2.4 (*e.g.* the sequence $(f_m)_{m>0}$ constructed in Lemma 2.4 (a)). If y_j is an arbitrary root in $\overline{K(T)}$ of $P_{i_j}(f_j(T), Y)$, $j = 1, \ldots, m$, then

$$\begin{aligned}[\overline{K}(T, y_1(T), \ldots, y_m(T)) : \overline{K}(T)] &= \prod_{1 \leq j \leq m} [\overline{K}(T, y_j(T)) : \overline{K}(T)] \\ &= \deg_Y P_{i_1} \cdots \deg_Y P_{i_m}\end{aligned}$$

The second equality comes from the absolute irreducibility of the polynomials $P_i(f_j(T), Y)$ (Cf. Prop.2.3). A fortiori we have

$$[K(T, y_1(T), \ldots, y_m(T)) : K(T)] = D_{\text{gen}}(\mathbf{P_i(f)}) = \deg_Y P_{i_1} \cdots \deg_Y P_{i_m}$$

For $\delta_i = \deg_Y P_i/2$, $i = 1, \ldots, n$, (11) then gives

$$2^m \leq s(\deg_Y P_1)! \cdots (\deg_Y P_n)! \tag{12}$$

which contradicts (8). Conclude that there exists an integer $j \in \{1, \ldots, m\}$ with the property that the polynomial $P_i(f_j(t), Y)$ has all of its roots of degree over K larger than $\deg_Y P_i/2$, $i = 1, \ldots, n$. Then necessarily the polynomial $P_i(f_j(t), Y)$ is irreducible in $K[Y]$, $i = 1, \ldots, n$. That is, $f_j(t)$ is in the Hilbert subset $H_{P_1, \ldots, P_n}$. □

Remark 3. There usually is a preliminary step in proofs of Hilbert's irreducibility theorem, which reduces the problem to studying sets of the form

$$V'_{Q_1, \ldots, Q_N} = \{t \in K | Q_i(t, Y) \text{ has no root in } K, i = 1, \ldots, N\} \tag{13}$$

rather than Hilbert subsets $H_{P_1, \ldots, P_n}$ themselves (*e.g.* [14 ;Ch.9,Prop.1.1]). Here we do not use this reduction : our proof directly provides elements of $H_{P_1, \ldots, P_n}$. This remark is important for effectiveness. Indeed, this reduction step turns out to be quite expensive in terms of constants : degrees and heights of the polynomials $Q_1, \ldots, Q_N$ that replace the polynomials $P_1, \ldots, P_n$ are respectively of order D^D and $D^D H$ (where $\deg_Y P_i \leq D$, $h(P_i) \leq H$, $i = 1, \ldots, n$) in general. Only because our proof avoids this usual reduction step could we obtain the bound of Cor.3.7.

2.5 Examples

We give a series of special cases of Th.2.1. In these examples, the n polynomials $P_1(T,Y),\dots,P_n(T,Y) \in K[T,Y]$ are absolutely irreducible and separable over $K(T)$ and $s > 0$ is an integer. Denote the set of exceptional points for $\mathbf{f}$, *i.e.*, such that there exists an element $t \in \mathbb{P}^1(\overline{K})$ such that $f(x) = t$ for infinitely many $f \in \mathbf{f}$, by $Exc(\mathbf{f})$.

Example 1. Let $(a_m)_{m>0}$ be a sequence of distinct elements of the field K. Set $\mathbf{f} = \{T + a_m | m > 0\}$. Then $Exc(\mathbf{f}) = \{\infty\}$. We obtain

Corollary 2.5 — *Assume $P_1(T,Y),\dots,P_n(T,Y) \in K[T,Y]$ are unramified above $T = \infty$. Then there exist an integer $M_o > 0$ and a constant h_2 with this property. For all s-integral point $t \in K$ such that $h(t) > h_2 s^2$, at least one out of the M_o elements $t + a_1,\dots,t + a_{M_o}$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.*

Example 2. Let $(a_m)_{m>0}$ be a sequence of distinct non-zero elements of K and $\mathbf{f} = \{a_m T | m > 0\}$. Then $Exc(\mathbf{f}) = \{0, \infty\}$. We obtain

Corollary 2.6 — *Assume $P_1(T,Y),\dots,P_n(T,Y) \in K[T,Y]$ are unramified above $T = \infty$ and tamely ramified above $T = 0$. Then there exist an integer $M_o > 0$ and a constant h_2 with this property. For all s-integral point $t \in K$ such that $h(t) > h_2 s^2$, at least one out of the M_o elements $a_1 t,\dots,a_{M_o} t$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.*

Example 3. This example uses the slightly more general form of Th.2.1 given in Remark 1. Let $b_o \in \mathbb{P}^1(K) \setminus Br(\mathbf{P})$ not a branch point of $P_1,\dots,P_n$. Let $(a_m)_{m>0}$ be a sequence of distinct elements of K. Set

$$f_m(T) = b_o + \frac{1}{T + a_m} \quad (m > 0)$$

and $\mathbf{f} = \{f_m(T) | m > 0\}$. Then $\mathbf{f}(\infty) = \{b_o\}$ and $Exc(\mathbf{f}) = \{b_o\}$. Thus conditions (A) (of Remark 1) and (B) hold. We obtain

Corollary 2.7 (Fried, Weissauer) — *There exist an integer $M_o > 0$ and a constant h_2 with this property. For all s-integral point $t \in K$ such that $h(t) > h_2 s^2$, at least one out of the M_o elements*

$$b_o + \frac{1}{t + a_1},\dots,b_o + \frac{1}{t + a_{M_o}}$$

belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.

Both Weissauer [21] and Fried [11] use in the special case of Example 3 arguments that are similar to ours. But Weissauer's approach uses non standard

analysis while Fried's one assumes the existence of non principal ultrafilters on $\mathbb{N}$. Our method is completely explicit. We will compute in §3 all the constants involved and will obtain a new effective version of Hilbert's irreducibility theorem over a number field (Cor.3.7). In Cor.2.7, the polynomials $P_1, \dots, P_n$ are assumed to be absolutely irreducible. We will use the following lemma to reduce to this case.

Lemma 2.8 — *(a) Let L/K be a field extension with $K \neq L$ and $P(T)$ be a polynomial in $L[T] \setminus K[T]$. Then the number of elements $t \in K$ such that $P(t) \in K$ is less than or equal to* $\deg(P)$.
(b) Let $P(T,Y)$ be an irreducible polynomial in $K[T,Y]$. Let

$$P(T,Y) = a_n(T)\ \Pi_1(T,Y) \cdots \Pi_r(T,Y)$$

be a factorization of $P(T,Y)$ in $\overline{K}[T,Y]$, with $a_n(T) \in K[T]$ and $\Pi_1, \dots, \Pi_r$ monic polynomials (in Y). Let L be an extension of K containing the coefficients of $\Pi_1, \dots, \Pi_r$. Then, for all but finitely many elements $t \in K$, if $\Pi_i(t,Y)$ is irreducible in $L[Y]$, $i = 1, \dots, r$, then $P(t,Y)$ is irreducible in $K[Y]$.

Proof. (a) Use for example the Lagrange interpolation formulas.

(b) Let $t \in K$ such that $\Pi_i(t,Y)$ is irreducible in $L[Y]$, $i = 1, \dots, r$ and $a_n(t) \neq 0$. Assume $P(t,Y) = a_n(t)Q(Y)R(Y)$ with $Q(Y), R(Y) \in K[Y]$ monic. Then necessarily there exists a subset $I \subset \{1, \dots, r\}$ such that $Q(Y) = \prod_{i \in I} \Pi_i(t,Y)$ and $R(Y) = \prod_{i \notin I} \Pi_i(t,Y)$. From (a), except for finitely many $t \in K$, one can infer that both polynomials $\prod_{i \in I} \Pi_i(T,Y)$ and $\prod_{i \notin I} \Pi_i(T,Y)$ must be in $K[T,Y]$. Conclude then from the irreducibility of $P(T,Y)$ in $K[T,Y]$ that necessarily $I = \emptyset$ or $I = \{1, \dots, n\}$. (It is readily checked that the number of exceptional t is $< \deg(P) 2^{\deg(P)}$). □

Example 4. Let $\mathbf{f} = \{T^m | m > 0\}$. Then $Exc(\mathbf{f}) = \{0, 1, \infty\} \cup \mu_\infty$ where μ_∞ is the set of all the roots of unity in $\overline{K}$. Taking Remark 2 into account we obtain

Corollary 2.9 — *Assume $P_1(T,Y), \dots, P_n(T,Y) \in K[T,Y]$ are unramified above $T = \infty$ and above $T = 1$ and are tamely ramified above $T = 0$. Then there exist an integer $M_o > 0$ and a constant h_2 with this property. For all s-integral point $t \in K$ such that $h(t) > h_2 s^2$, at least one out of the M_o elements $t, t^2 \dots, t^{M_o}$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.*

Example 5. This is a special case of Example 4. Take $K = \mathbb{Q}$, $n = 1$, $P_1(T,Y) = T(aY^2 + Y + 1) - 1$ where $a \in \mathbb{Z}, a \neq 0$. The assumptions of Cor.2.9 hold. Take $s = 1$. Inverses of prime powers $1/p^m$ are 1-integral points of $\mathbb{Q}$. Cor.2.9 yields that there exists an integer $M_o > 0$ and a constant h_2 with this property. For all prime powers p^m such that $p^m > h_2$, at least one out of the M_o elements

$p^m, \ldots, p^{mM_o}$ is not of the form $ay^2 + y + 1$ with $y \in \mathbb{Q}$. Furthermore, the integer M_o can be explicitely determined by using the "Addition to Th.2.1". Fix an integer m_o such that $2^{m_o} > (\deg_Y P_1)!$. Then M_o can be taken to be the m_oth term k_{m_o} of a sequence of integers $(k_m)_{m>0}$ such that the sequence $(T^{k_m})_{m>0}$ satisfies condition (4) of Lemma 2.4. It is easily checked that one can take $m_o = 2$, $k_1 = 1$ and $k_2 = k$ any integer $k > 1$. Finally we obtain the following result.

Corollary 2.10 — *Let $a \geq 1$ and $k \geq 2$ be two integers. Then there exist only finitely many prime powers p^m (p prime, $m > 0$) such that p^m and p^{km} are of the form $ay^2 + y + 1$ with $y \in \mathbb{Q}$.*

This example can be easily generalized to the situation $P(T, Y)$ of the form $TM(Y) - 1$ with $M(Y) \in \mathbb{Q}[Y]$ to give results about the diophantine equation $M(y) = p^m$.

2.6 Th.2.1 versus Siegel's theorem

In the introduction, we mentioned some advantages of our results over Siegel's theorem. Th.1.4 and Th.2.1 lead to

- more general results : here the field K is a field with the product formula, possibly of characteristic $p > 0$ whereas Siegel's theorem is valid for number fields (or, more generally for extensions of finite type of $\mathbb{Q}$ [14]). Also "s-integral" is more general than "S-integral".
- effective results : unlike Siegel's theorem, the constants involved in the statements can be explicitely computed from the data.

Now of course, when Siegel's theorem is valid and if one is not interested with effectiveness, then Siegel's conclusions are better than ours for S-integral points. For example, thanks to Siegel's theorem, one can prove the following result, which should be compared to Th.2.1. Keep the notation of Th.2.1. Assume that K is a number field. Let S be a finite set of places of K containing the archimedean ones.

Proposition 2.11 — *Assume conditions (A), (B) hold. Then there exists a constant $h_2 > 0$ and two polynomials $f_1, f_2 \in \mathbf{f}$ with the following property. If t is any S-integral point of K of height $h(t) > h_2$, then either $f_1(t)$ or $f_2(t)$ lies in the Hilbert subset $H_{P_1,\ldots,P_n}$.*

That is, for S-integral points, conclusion of Th.2.1 holds with $|\mathbf{f}_o| = 2$.

Proof. Classically, it is sufficient to prove the weaker conclusion where $H = H_{P_1,\ldots,P_n}$ is replaced by $V' = V'_{P_1,\ldots,P_n}$ (defined in Remark 3). Let f_1, f_2 be two *a priori* arbitrary polynomials in $\mathbf{f}$. For each bi-index $\mathbf{i} = (i_1, i_2)$ with

entries i_1, i_2 in $\{1,\dots,n\}$, denote the function field over $\overline{K}$ of the affine curve $P_{i_j}(f_j(t),y)=0$ by E_{i_j}, $j=1,2$ and the compositum field $E_{i_1}E_{i_2}$ by $E_{\mathbf{i}}$. From Lemma 2.4, f_1 and f_2 can be selected such that

$$[E_{\mathbf{i}}:\overline{K}(T)]=[E_{i_1}:\overline{K}(T)][E_{i_2}:\overline{K}(T)]\geq 4$$

From assumption (B), ∞ is not a branch point of the extension $E_{\mathbf{i}}/\overline{K}(T)$. Consequently if $C_{\mathbf{i}}$ denotes a smooth projective model of the function field $E_{\mathbf{i}}$, then the function T has 4 distinct poles on $C_{\mathbf{i}}$. From Siegel's theorem, the set of points $M\in C(K)$ such that $T(M)$ is S-integral is a finite set $F_{\mathbf{i}}$.

Now if t is an S-integral point of K such that both $f_1(t)$ and $f_2(t)$ are not in $V'_{P_1,\dots,P_n}$, then either $t\in Br(\mathbf{P})$ or there exists a bi-index $\mathbf{i}=(i_1,i_2)$ and a point $M\in C_{\mathbf{i}}$ such that $t=T(M)$. □

3 EFFECTIVE RESULTS

In this section the field K is assumed to be a number field.

3.1 The constants A, B and h_o of Th.1.1 and Cor.1.3

For a number field K, the constants A and B are explicitely given p. 20 of [3] (or, in a more general context, p. 379 of [5]). They are expressed in terms of the partial degrees, the height and the Eisenstein constant of the polynomial P. Recall the definition of the latter. Denote the roots of $P(T,Y)$ in $\overline{K}[[1/T]]$ by $y_1,\dots,y_d$. Set

$$y_i=\sum_{m\geq 0} y_{im}\frac{1}{T^m},\qquad i=1,\dots,d \tag{1}$$

Then the Eisenstein constant of P is the smallest integer $E\in\mathbb{Z}$ such that $E^m y_{im}$ is an algebraic integer for all $m>0$, $i=1,\dots,d$. In [10], Dwork and Van der Porten give a general bound for the Eisenstein constant of a polynomial. But this bound is not fully satisfactory for our purposes for it makes A and B depend on the field K. We prefer to postpone the evaluation of the Eisenstein constant to next paragraph where the situation is more specific and where more elementary results can be used. The constant h_o of Cor.1.3 is easily obtained from the constants A and B.

3.2 The constant h_1 of Th.1.4

As in §1.3, let $\mathbf{P}=\{P_1(T,Y),\dots,P_m(T,Y)\}$ be a family of polynomials in $K(T)[Y]$ unramified above $T=\infty$. Let $H,D>0$ be two real numbers such that

$$h(P_i)\leq H,\ \deg(P_i)\leq D,\ i=1,\dots,m$$

From the proof of Th.1.4, the constant $h_1 = h_1(\mathbf{P})$ can be obtained in the following way. Let $y_i \in \overline{K(T)}$ be a root of the polynomial $P_i(T, Y)$, $i = 1, \ldots, m$ and

$$z = c_1 y_1 + \cdots + c_m y_m, \text{ with } c_i \in \mathbb{Z}, i = 1, \ldots, m \tag{2}$$

be a primitive element of the extension $K(T, y_1, \ldots, y_m)/K(T)$. Let $P(T, Y) \in K[T, Y]$ be an irreducible polynomial such that $P(T, z) = 0$. Then the constant h_1 is the constant $h_o(P)$ of Cor.1.3. The problem consists in evaluating the degree and the height of the polynomial $P(T, Y)$. Since we just need upper bounds, we can work with a multiple in $K[T, Y]$ of the polynomial $P(T, Y)$ and then use the following result (*e.g.* [14 ;Prop.2.12 p.61]).

Proposition 3.1 — *If $f_1, f_2 \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_n]$, then*

$$h(f_1) \leq h(f_1) + h(f_2) \leq h(f_1 f_2) + n \deg(f_1 f_2)$$

In §3.3 we show that such a multiple can be obtained by iteration of resultants and we give estimates for the degree and the height of this polynomial in terms of $P_1, \ldots, P_m$ and $c_1, \ldots, c_m$. Then we bound $c_1, \ldots, c_m$ (Prop.3.6). Finally we will obtain the following result.

Proposition 3.2 — *Assume that the polynomials $P_1, \ldots, P_m$ satisfy condition (11) of §1. Then we have*

$$\begin{cases} \deg(P) \leq (2D)^m \\ h(P) \leq 2^m D^{m-1} H + 8m(2D)^{2m} \end{cases} \tag{3}$$

Furthermore the polynomial is unramified above $T = \infty$ and the Eisenstein constant E of P can be bounded as follows

$$\mathrm{Log}(E) \leq 4mDH + 9mD^2 \tag{4}$$

Consequently we obtain

$$h_1 \leq 2^{15m+4} D^{14m} (H^2 + 800) \tag{5}$$

3.3 Preliminary results

The resultant of two polynomials

$$f(Y) = a_p Y^p + \cdots + a_o \qquad (\text{with } a_p \neq 0)$$
$$g(Y) = b_q Y^q + \cdots + b_o \qquad (\text{with } b_q \neq 0)$$

with coefficients in a ring R is denoted by $Res_Y(f,g)$. We also define the reduced resultant $\widehat{Res}_Y(f,g)$ by the formula

$$Res_Y(f,g) = a_p^q b_q^p \widehat{Res}_Y(f,g)$$

Let $F(T,Y_1,\dots,Y_m,Z) \in K[T,Y_1,\dots,Y_m,Z]$. We inductively define polynomials $\widehat{R}_i$, $i=1,\dots,m$ by the formulas :

$$\begin{cases} \widehat{R}_1 = \widehat{Res}_{Y_1}(F,P_1) \\ \widehat{R}_i = \widehat{Res}_{Y_i}(\widehat{R}_{i-1},P_i) \text{ for } 2 \le i \le m \end{cases} \tag{6}$$

From standard properties of resultants, we have

Proposition 3.3 — *For $i=1,\dots,m$, $\widehat{R}_i$ is a polynomial in the variables T,Z and Y_j with $j>i$ and with coefficients in K. In particular, $\widehat{R}_m \in K[T,Z]$. If $z \in \overline{K(T)}$ is a root of $\widehat{R}_m$, i.e., $\widehat{R}_m(T,z)=0$, then there exist $y_1,\dots,y_m$ in $\overline{K(T)}$ such that*

$$\begin{cases} P_1(T,y_1)=0 \\ \vdots \\ P_m(T,y_m)=0 \\ F(T,y_1,\dots,y_m,z)=0 \end{cases} \tag{7}$$

Let $P(T,Z)$ be an irreducible polynomial in $K[T,Z]$ such that $P(T,z)=0$. Thus the polynomial $\widehat{R}_m$ is a multiple in $K[T,Z]$ of the polynomial $P(T,Z)$.

Proposition 3.4 — *If $h(P_i) \le H$, $\deg(P_i) \le D$, $i=1,\dots,m$, and $\deg(F) \le \delta$, then*

$$\begin{cases} \deg(P) \le \delta(2D)^m \\ h(P) \le 2^m \delta D^{m-1} H + D^m h(F) + 7m\delta^2(2D)^{2m} \end{cases} \tag{8}$$

We first establish some general estimates of the size of a resultant.

Proposition 3.5 — *Let $A,B \in K[Y_1,\dots,Y_n]$ be two polynomials such that $\deg_{Y_1}(A), \deg_{Y_1}(B) > 0$. Set $R = Res_{Y_1}(A,B)$. Then*

$$\begin{cases} \deg(R) \le 2\deg(A)\deg(B) \\ h(R) \le \deg(A)h(B) + \deg(B)h(A) \\ \qquad\qquad +n\deg(AB)\,\mathrm{Log}(\deg(AB)) \end{cases} \tag{9}$$

Proof. Given a place $v \in M_K$ and a polynomial P with coefficients in K, define the v-adic height $h_v(P)$ of P to be the Log of the maximum of the v-adic absolute values of the coefficients of P. Note that

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v]\, h_v(P) \tag{10}$$

Also recall these elementary formulas. If $f_1, \dots, f_k \in \overline{\mathbb{Q}}[Y_1, \dots, Y_n]$ are of degree less than d, then

$$\begin{cases} h_v(f_1 \cdots f_k) \le h_v(f_1) + \cdots + h_v(f_k) + \varepsilon_v n(k-1)\,\mathrm{Log}(1+d) \\ h_v(f_1 + \cdots + f_k) \le h_v(f_1, \dots, f_k) + \varepsilon_v\,\mathrm{Log}(k) \end{cases} \tag{11}$$

where $\varepsilon_v = 0$ if v is finite and $\varepsilon_v = 1$ if v is archimedean. Also in the second inequality, $h_v(f_1, \dots, f_k)$ is the v-adic height of the collection of all the coefficients of $f_1, \dots, f_k$.

Now write R as a $(\deg_{Y_1}(A) + \deg_{Y_1}(B))$ determinant and use (11) to obtain

$$\deg(R) \le \deg_{Y_1}(B)\deg(A) + \deg_{Y_1}(A)\deg(B)$$

$$\begin{aligned} h_v(R) \le\ & \deg_{Y_1}(B)h_v(A) + \deg_{Y_1}(A)h_v(B) + \\ & + \varepsilon_v(n-1)\deg_{Y_1}(AB)\,\mathrm{Log}(1 + \max(\deg(A), \deg(B))) \\ & + \varepsilon_v\,\mathrm{Log}((\deg_{Y_1}(AB))!) \end{aligned}$$

The result readily follows. □

Proof of Prop. 3.4. Set $D_i = \deg(P_i)$, $i = 1, \dots, m$. We show by induction that for $i = 1, \dots, m$:

$$\begin{cases} \deg(\widehat{R}_i) \le 2^i \delta D_1 \cdots D_i \\ h(\widehat{R}_i) \le (\delta D_1 \cdots D_i)\left[\frac{h(P_1)}{D_1} + 2\frac{h(P_2)}{D_2} \cdots 2^{i-1}\frac{h(P_i)}{D_i} + \frac{h(F)}{\delta}\right] \\ \qquad\qquad + 2(m+2)(2^i \delta D_1 \cdots D_i)^2 \end{cases} \tag{12}$$

The result will then follow from $\deg(P) \le \deg(\widehat{R}_m)$ and $h(P) \le h(\widehat{R}_m) + 2\deg(\widehat{R}_m)$ (use Prop.3.1 for the latter).

For $i = 1$, we have

$$\begin{aligned} \deg(\widehat{R}_1) &\le \deg(Res_{Y_1}(F, P_1) \le 2\deg(F)\deg(P_1) \\ h(\widehat{R}_1) &\le h(Res_{Y_1}(F, P_1)) + (m+2)\deg(Res_{Y_1}(F, P_1)) \\ &\le \delta h(P_1) + D_1 h(F) + (m+2)(\delta + D_1)\,\mathrm{Log}(\delta + D_1) + 2(m+2)\delta D_1 \\ &\le \delta D_1 \left(\frac{h(P_1)}{D_1} + \frac{h(F)}{\delta}\right) + (m+2)(2\delta D_1\,\mathrm{Log}(2\delta D_1) + 2\delta D_1) \end{aligned}$$

(Use $a+b \leq 2ab$, (for $a, b > 1$) for the last inequality and then $x\,\mathrm{Log}(x)+x \leq x^2$ (for $x > 1$) to get (12) in the case $m = 1$). We then proceed inductively. For $1 < i \leq m$, we have

$$\begin{aligned}\deg(\widehat{R}_i) &\leq \deg(Res_{Y_i}(\widehat{R}_{i-1}, P_i)) \\ &\leq 2\deg(\widehat{R}_{i-1})\deg(P_i) \\ &\leq 2(2^{i-1}\delta D_1 \cdots D_{i-1})D_i\end{aligned}$$

and

$$\begin{aligned}h(\widehat{R}_i) &\leq h(Res_{Y_i}(\widehat{R}_{i-1}, P_i)) + (m+2)\deg(Res_{Y_i}(\widehat{R}_{i-1}, P_i)) \\ &\leq \deg(\widehat{R}_{i-1})h(P_i) + D_i h(\widehat{R}_{i-1}) \\ &\quad + (m+2)(2^{i-1}D_1 \cdots D_{i-1}\delta + D_i)\,\mathrm{Log}(2^{i-1}D_1 \cdots D_{i-1}\delta + D_i) \\ &\quad + (m+2)(2^i \delta D_1 \cdots D_i) \\ &\leq (2^{i-1}\delta D_1 \cdots D_{i-1})h(P_i) \\ &\quad + D_i(\delta D_1 \cdots D_{i-1})\left[\frac{h(P_1)}{D_1} + 2\frac{h(P_2)}{D_2} \cdots 2^{i-2}\frac{h(P_{i-1})}{D_{i-1}} + \frac{h(F)}{\delta}\right] \\ &\quad + 2D_i(m+2)(2^{i-1}\delta D_1 \cdots D_{i-1})^2 \\ &\quad + (m+2)\left[(2^i \delta D_1 \cdots D_i)\,\mathrm{Log}(2^i \delta D_1 \cdots D_i)\right. \\ &\quad \left. + 2^i \delta D_1 \cdots D_i\right] \\ &\leq (\delta D_1 \cdots D_i)\left[\frac{h(P_1)}{D_1} + 2\frac{h(P_2)}{D_2} \cdots 2^{i-1}\frac{h(P_i)}{D_i} + \frac{h(F)}{\delta}\right] \\ &\quad + (m+2)(2^i \delta D_1 \cdots D_i)^2(1+\frac{1}{2}) \quad \square\end{aligned}$$

Proposition 3.6 — *The extension $K(T, y_1, \ldots, y_m)/K(T)$ has a primitive element of the form*

$$z = c_1 y_1 + \cdots + c_m y_m, \tag{13}$$

where $c_1, \ldots, c_m$ are integers such that $c_1 = 1$ and $c_i \leq D^{2m}$, $i = 2, \ldots, m$ (where as usual $\deg(P_i) \leq D$, $i = 1, \ldots, m$).

Proof. The following proof is due to D. Poulakis. Let S be the set of $(m-1)$-tuples $(z_2, \ldots, z_m) \in \mathbb{Z}^{m-1}$ with $0 < z_j \leq D^{2m}$, $j = 2, \ldots, m$. Consider the subset $S' \subset S$ consisting of the $(m-1)$-tuples $(z_2, \ldots, z_m) \in S$ such that there exist two distinct $K(T)$-homomorphisms σ, σ' of $K(T, y_1, \ldots, y_m)$ into $\overline{K(T)}$ for which

$$y_1^\sigma + z_2 y_2^\sigma + \cdots + z_m y_m^\sigma = y_1^{\sigma'} + z_2 y_2^{\sigma'} + \cdots + z_m y_m^{\sigma'}$$

Set $d_m = [K(T, y_1, \ldots, y_m) : K(T)]$. We have $d_m \leq D^m$ and so

$$card(S') \leq \binom{d_m}{2}(2D^{2m})^{m-2} < (2D^{2m})^{m-1} = card(S)$$

Therefore $S\backslash S' \neq \emptyset$. Classically if $z_2, \ldots, z_m \in S\backslash S'$, then $y_1 + c_2 y_2 + \cdots + c_m y_m$ satisfies the conclusion of Prop.3.6. □

Proof of Prop.3.2. (3) readily follows from Prop.3.4 and Prop.3.6 (applied to $F = Y_1 + c_2 Y_2 + \cdots + c_m Y_m$). The polynomial $P(T, Y)$ is unramified above $T = \infty$, *i.e.*, totally split in $\overline{K}((1/T))$, because so are the polynomials $P_1, \ldots, P_m$. Furthermore, the form of the roots of $P(T, Y)$ shows that the Eisenstein constant E of P can be bounded by $E_1 \cdots E_m$ where E_i is the Eisenstein constant of the polynomial P_i, $i = 1, \ldots, n$. Under assumption (11) of §1, the Eisenstein constants $E_1, \ldots, E_m$ can be bounded quite easily. For example, Prop. p.387 of [5] gives

$$\mathrm{Log}(E_i) \leq 4DH + 9D^2, \ i = 1, \ldots, m$$

which proves (4). The final bound for h_1 follows from (3), (4) of §3 and (8) of §1. □

3.4 The constant h_2 of Th.2.1

Let $\mathbf{P} = \{P_1(T, Y), \ldots, P_n(T, Y)\}$ be a family of polynomials and $(f_m)_{m>0}$ be a sequence of elements of $\mathbf{f}$ like in the "Addition to Th.2.1". Let $s > 0$ be an integer. From the proof of Th.2.1, the constant h_2 can be obtained in the following way. Fix an integer $m_o > 0$ such that

$$2^{m_o} > s(\deg_Y P_1)! \cdots (\deg_Y P_n)!$$

Consider the polynomials $P_i(f_j(T), Y)$, $i = 1, \ldots, n$, $j = 1, \ldots, m_o$. Multiply each $P_i(f_j(T), Y)$ appropriately by an element of $K(T)$ so to obtain a polynomial $\widetilde{P}_{ij}(T, Y)$ in $K[T, Y]$. Then h_2 is the largest one of the constants h_1 of Th.1.4 associated with the families $\widetilde{\mathbf{P}}_{\mathbf{i}} = \{\widetilde{P}_{i_1 1}(T, Y), \ldots, \widetilde{P}_{i_{m_o} m_o}(T, Y)\}$ where $\mathbf{i} = (i_1, \ldots, i_{m_o})$ ranges over all families of indices $i_j \in \{1, \ldots, n\}$ indexed by $\{1, \ldots, m_o\}$.

In the following estimates, we use the following notation : $\deg_Y P_i \leq D$, $h(P_i) \leq H$, $i = 1, \ldots, n$ and $\deg f_j \leq D(\mathbf{f}_o)$, $h(f_j) \leq H(\mathbf{f}_o)$, $j = 1, \ldots, m_o$. Using (10) and (11), one obtains

$$(14) \qquad \begin{cases} \deg(\widetilde{P}_{ij}) \leq DD(\mathbf{f}_o) \\ h(\widetilde{P}_{ij}) \leq H + DH(\mathbf{f}_o) + 2DD(\mathbf{f}_o) \end{cases}$$

Report these estimates in the formula for h_1 to get the bound for h_2 announced in Th.2.1, *i.e.*,

$$(15) \qquad h_2 = 2^{15m_o+4} \left(DD(\mathbf{f}_o)\right)^{14m_o+2} \left(3H^2 + 3H(\mathbf{f}_o)^2 + 812\right)$$

3.5 Effective version of Hilbert's irreducibility theorem

Our goal is to make Example 3 of §2.5 completely explicit so to give a completely effective version of Hilbert's irreducibility theorem. Recall some basic properties of the height on $\overline{K}$ [14;Ch.3]. For $\alpha_1, \dots, \alpha_k \in \overline{K}, (k \geq 1)$, then

$$\begin{aligned} h(\alpha_1 \alpha_2) &\leq h(\alpha_1) + h(\alpha_2) \\ h(\alpha_1 + \cdots + \alpha_k) &\leq h(\alpha_1) + \cdots + h(\alpha_k) + \mathrm{Log}(k) \end{aligned} \tag{16}$$

If $P \in K[Y]$ and $\alpha \in \overline{K}$ a root of P, we have the Liouville inequality

$$h(\alpha) < h(P) + \mathrm{Log}(2) \tag{17}$$

Let $P_1(T,Y), \dots, P_n(T,Y) \in K[T,Y] \setminus K[T]$ be n absolutely irreducible polynomials of total degree less than D and of height less than H. The following algorithm is an effective version of Example 3 of §2.5. It is the most precise result of this section.

ALGORITHM

(1) Take m_o an integer with $2^{m_o} > [K : \mathbb{Q}] D^{nD}$.

(2) Take $b_o \in K$ such that $h(b_o) > 6D^2 + 2DH + \mathrm{Log}(2)$.

(3) Take a integral in K such that $h(a) > 12D^2 + 4DH + 2h(b_o) + 5\,\mathrm{Log}(2)$.

(4) Set $f_m(T) = b_o + \frac{1}{T + ma} \quad (m > 0)$

(5) Compute
$h_2 = 2^{15m_o+4} D^{14m_o+2} (3H^2 + 9(h(b_o) + \mathrm{Log}(3))^2 + 9(\mathrm{Log}(m_o))^2 + 9h(a)^2 + 812)$.

(6) Take $t \in \mathbb{Z}$ of height $\mathrm{Log}\,|t| > h_2 [K : \mathbb{Q}]^2$

(7) Conclusion : at least one out of the m_o elements $f_1(t), \dots, f_{m_o}(t)$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.

Comments. (a) We took $s = [K : \mathbb{Q}]$ so that integers $t \in \mathbb{Z}$ are s-integral in K. The quantity $6D^2 + 2DH$ is an upper bound for the height of the discriminants of the polynomials $P_1, \dots, P_n$. Thus condition (2) guarantees that the polynomials $P_i(f_j(T), Y)$, $i = 1, \dots, n$, $j = 1, \dots, m_o$, satisfy condition (11) of §1. Condition (3) insures that no non-zero multiple ma of a is of the form

$$ma = \frac{1}{r - b_o} - \frac{1}{r' - b_o} \tag{18}$$

with r, r' two branch points of $P_1, \dots, P_n$. This requirement on the element a guarantees that the sequence $(f_m)_{m>0}$ satisfies condition (4) of Lemma 2.4. (We selected a integral in K so to insure that $h(ma) \geq h(a)$ if $m \neq 0$).

(b) When some of the polynomials $P_1(T,Y),\dots,P_m(T,Y)$ are irreducible in $K[T,Y]$ but not absolutely irreducible, the following procedure can be used. Replace the polynomials $P_1,\dots,P_n$ by the collection $Q_1,\dots,Q_N$ of all their irreducible factors in $\overline{K}[T,Y]$. These polynomials have their coefficients in a certain field L. Apply the above algorithm (steps (1) through (5)) to the polynomials $Q_1,\dots,Q_N$. We have

$$(19)\qquad \begin{cases} N \le nD \\ [L:K] \le nD! \\ \deg(Q_i) \le D \\ h(Q_i) \le H + 2D \end{cases}$$

where $i = 1,\dots,N$. From Lemma 2.8, for all but possibly $nD2^D$ elements $t \in K$, if $Q_i(t,Y)$ is irreducible in $L[Y]$, $i = 1,\dots,N$, then $P_i(t,Y)$ is irreducible in $K[Y]$, $i = 1,\dots,n$. The final steps (6) and (7) of the algorithm become

(6') Take $M = nD2^D$ integers $t_1,\dots,t_M \in \mathbb{Z}$ of height $> h_2[L:\mathbb{Q}]^2$

(7') Conclusion : at least one out of the m_oM elements $f_1(t_k),\dots,f_{m_o}(t_k)$, $k = 1,\dots,M$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.

When the polynomials $P_1,\dots,P_n$ are absolutely irreducible, then one can pick m_o, b_o, a in $\mathbb{Z}$ such that

$$(20)\qquad \begin{cases} m_o \le \frac{1}{\mathrm{Log}(2)}(\mathrm{Log}(r) + nD\,\mathrm{Log}(D)) + 1 \\ h(b_o) + \mathrm{Log}(3) \le 7D^2 + 2DH \\ h(a) \le 27D^2 + 8DH \end{cases}$$

where $r = [K:\mathbb{Q}]$. Some calculations then lead to

$$(21)\qquad h_2 \le 0,95.10^{10} D^{58nD\,\mathrm{Log}(D)+43\,\mathrm{Log}(r)}(H^2+1)$$

The final steps (6) and (7) finally give conclusion (a) below. Conclusion (b) follows similarly from steps (6') and (7').

Corollary 3.7 — *(a) If the polynomials $P_1,\dots,P_n \in K[T,Y]$ are absolutely irreducible, then there exists in the Hilbert subset $H_{P_1,\dots,P_n}$ a rational number $x = u/v \in \mathbb{Q}$ of height*

$$(22)\qquad h(x) = \max(\mathrm{Log}\,|u|, \mathrm{Log}\,|v|) \le 10^{10} D^{58nD\,\mathrm{Log}(D)+46\,\mathrm{Log}(r)}(H^2+1)$$

(b) If the polynomials $P_1,\dots,P_n$ are only assumed to be irreducible in $K[T,Y]$, the same conclusion holds with this bound for $h(x)$:

$$(23) \qquad h(x) = \max(\mathrm{Log}\,|u|, \mathrm{Log}\,|v|) \leq 10^{10} D^{90nD^2\,\mathrm{Log}(D)+46\,\mathrm{Log}(r)}(H^2+1)$$

The right-hand term of (23) is actually an upper bound for the height of the $m_o M$ elements $f_1(t_k), \ldots, f_{m_o}(t_k)$, $k = 1, \ldots, M$ of step (7'). At least one out of these $m_o M$ elements lies in the Hilbert subset $H_{P_1,\ldots,P_n}$. Thus, finding an element in $H_{P_1,\ldots,P_n}$ requires at most to test for the irreducibility of the $m_o M$ polynomials $P_i(x, Y)$, where $i = 1, \ldots, n$ and x ranges over the list of $m_o M$ elements above. The height of these polynomials can be easily bounded :

$$h(P(x,Y)) \leq \mathrm{Log}(D+1) + h(P) + h(x)$$

Factoring polynomials in one variable of degree less than H and logarithmic height less than H takes polynomial time $(rDH)^{O(1)}$ ([16],[15]). Conclusion :

Corollary 3.8 — *Let $P_1, \ldots, P_n$ be n irreducible polynomials in $K[T,Y] \setminus K[T]$, with degree $\leq D$ and logarithmic height $\leq H$. Then one can find a specific specialization $x \in H_{P_1,\ldots,P_n}$ in time $H^{O(1)} \exp(nD^{O(1)}\mathrm{Log}^+(r))$ (where $\mathrm{Log}^+(r) = \max(\mathrm{Log}(r), 1)$).*

Thus we obtain a bound which is polynomial in H but not in D. A polynomial bound in both H and D would be a quite interesting improvement. This would indeed provide a deterministic algorithm for factoring polynomials in two variables in polynomial time. The nonpolynomial growth of our bound mainly comes from condition (2) of Th.2.1 which imposes to take the parameter m_o of the algorithm fairly big ; precisely the algorithm requires that $2^{m_o} > rD^{nD}$. From Prop.2.11, we know that m_o can actually be taken to be equal to 2. But Prop.2.11, which relies on Siegel's theorem, is not effective. Nevertheless this suggests that the above condition on m_o might be improved.

3.6 Hilbert subsets of higher dimension

In this paragraph we use the results of the previous one to deduce similar results for Hilbert subsets of arbitrary dimension $q \geq 1$. The classical tool for reducing to the dimension 1 is the Kronecker transformation [14 ;Ch.9]. Making it effective does not present any particular difficulty. We only state the result and leave the details to the reader.

Fix two integers $q, p > 0$. If $P_1, \ldots, P_n$ are n polynomials, irreducible in the ring $K[T_1, \ldots, T_q, Y_1, \ldots, Y_p]$, the Hilbert subset $H_{P_1,\ldots,P_n}$ is defined to be the subset of K^q consisting of all q-tuples $(t_1, \ldots, t_q)$ such that the polynomial $P_i(t_1, \ldots, t_q, Y_1, \ldots, Y_p)$ is irreducible in $K[Y_1, \ldots, Y_p]$, $i = 1, \ldots, n$. Let $D, H > 0$ such that $\deg(P_i) \leq D$ et $h(P_i) \leq H$, $i = 1, \ldots, n$.

Corollary 3.9 — *The Hilbert subset $H_{P_1,\dots,P_n}$ contains a q-tuple $(t_1,\dots,t_q)$ in $\mathbb{Q}^q$ such that, for $i = 1,\dots,q$,*

$$h(t_i) \leq 10^{10.2^q}\ (D+1)^{100\left[n(D+1)^{6(r+q)}+46p2^q\,\mathrm{Log}(r)\right]}\ (H+1)^{2^q} \tag{24}$$

REFERENCES

[1] E. Bombieri, On Weil's "Théorème de décomposition", *Amer. J. Math.*, **105**, (1983)

[2] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, (1967)

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

[4] P. Dèbes, Quelques remarques sur un article de Bombieri concernant le théorème de décomposition de Weil, *Amer. J. Math.*, **107**, (1985)

[5] P. Dèbes, G-fonctions et Théorème d'irréductibilité de Hilbert, *Acta Arithmetica*, **47**, 4 (1986)

[6] P. Dèbes, Résultats récents liés au théorème d'irréductibilité de Hilbert, *Sém. Th. Nombres, Paris, 1985-86*, Birkhauser, (1987)

[7] P. Dèbes, On the irreducibility of the polynomials $P(t^m, Y)$, *J. Number Theory*, 42, 2, (1992)

[8] P. Dèbes, Density results for Hilbert subsets, preprint (1994)

[9] P. Dèbes, On a problem of Dvornicich and Zannier, *Acta Arithmetica*, to appear

[10] B. Dwork and A. Van der Porten, The Eisenstein constant, preprint, (1991)

[11] M. Fried, On the Sprindzuk-Weissauer approach to universal Hilbert subsets, *Israel J. Math*, **51**, 4, (1985)

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

[13] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, (1977)

[14] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, (1983)

[15] A. K. Lenstra, Factoring Polynomials over algebraic Number Fields, *Proc. Conf. Math. Foundations of Computer Science*, Lecture Notes in Computer Science, **176**, (1983)

[16] A. K. Lenstra and H. W. Lenstra and L. Lovász, Factoring Polynomials with rational coefficients, *Math. Ann.*, **261**, (1982)

[17] Y. Morita, A note on Hilbert Irreducibility Theorem, *Proc. Japan Acad. Ser. A*, **66**, (1983)

[18] A. Schinzel and U. Zannier, The least admissible value of the parameter in Hilbert's Irreducibility Theorem, *Acta Arithmetica*, **69**, 3 (1995)

19] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, translated by M.Brown from notes by M.Waldschmidt, Vieweg, (1990)

[20] V.G. Sprindzuk, Arithmetic specializations in polynomials, *J. Reine Angew. Math.*, **340**, (1983)

[21] R. Weissauer, Hilbertsche Körper, Thesis, Heidelberg, (1980)