Density Results for Hilbert Subsets

Pierre Dèbes

Abstract. A classical tool for studying Hilbert's irreducibility theorem is Siegel's finiteness theorem for S-integral points on algebraic curves. In [De3] we presented a different approach based on s-integral points rather than S-integral. Given an integer $s > 0$, s-integral points of a field K with the product formula are those points t for which the set of places $v \in M_K$ such that $|t|_v > 1$ is *of cardinality* $\leq s$ (instead of *contained in* S for "S-integral"). [De3] contains a general diophantine result for s-integral points and some applications to Hilbert's theorem. We gave in [De4] a second application to a problem raised by Dvornicich and Zannier. This paper presents new applications which include the possibility that K is of characteristic $p > 0$. Th.2.1 and Th.2.2 essentially conclude that, except in trivial cases, Hilbert subsets of K contain infinitely many powers of a given element $b \in K$ of height $h(b) > 0$. The only assumption on the polynomials involved is that they should be separable and tamely ramified above ∞. Th.3.4 shows the following general density property of Hilbert subsets of a field K with the product formula, of characteristic 0, or of characteristic $p > 0$ and imperfect : Hilbert subsets of K are dense in K for the strong approximation topology (*i.e.*, the topology involved in the strong approximation theorem), provided that 0 is not isolated in K. The spirit of these three results is that for a field with the product formula, strong arithmetical constraints can be added to the Hilbert property.

This paper is concerned with Hilbert's irreducibility theorem. In a general way Hilbert subsets of a field K are 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 [La2 ;Ch.9]. More generally, a field K with the same property is called *hilbertian*. Here the base field K will be assumed to be a field with the product formula [La2 ;Ch.2]. From results of Weissauer and Uchida, such fields are known to be hilbertian if they are of characteristic 0 or, of characteristic $p > 0$ and imperfect [FrJ ;Ch.11,14]. Number fields, regular function fields over a constant field k are typical examples.

Our first result extends results of [De2] where the field K was a number field. The method in [De2] used Siegel's finiteness theorem for S-integral

1991 *Mathematics Subject Classification.* Primary 12E25, 14H05 ; Secondary 11xx.

points on algebraic curves. The present paper uses instead the general diophantine result of [De3] for s-integral points (Cf. §.1.2). This alternate approach has two main advantages over Siegel's theorem : it is valid more generally over fields with the product formula, possibly of characteristic $p > 0$; and it is effective for number fields.

Theorem (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 $T = 0$ or 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 $m > 0$.

Clearly condition (*) cannot be removed in general : take $P(T, Y) = Y^\ell - T$ if $b \in K^\ell$ and $P(T, Y) = Y^4 + 4T$ if $-b \in K^2$. On the other hand, the assumption "$P(T, Y)$ tamely ramified above $T = 0$ or above $T = \infty$" is a technical assumption coming from the method ; it is unclear whether it is really necessary (Cf.§2.4). Recall that this condition is automatically satisfied in characteristic 0.

Th.2.2 does not extend to several polynomials : take $n = 2$, $P_1 = Y^2 - T$, $P_2 = Y^2 - 2T$; for $K = \mathbb{Q}$, $b = 2$ does satisfy (*) but H_{P_1,P_2} contains no power of 2. Nevertheless, if condition (*) is slightly modified, then one can prove this version of Th.2.2 for several polynomials.

Theorem (Th.2.1) — *Let K be a field with the product formula. Let $H = H_{P_1,\dots,P_n}$ be a Hilbert subset of K with $P_1, \dots, P_n$ irreducible and separable over $K(T)$ and tamely ramified above $T = \infty$. Then there exists a finite extension L of K with the following property. Let b be an element of K of height $h(b) > 0$ and such that condition (*) above holds but with L replacing K. Then the Hilbert subset H contains infinitely many powers b^m ($m > 0$) of b.*

The extension L/K will be described quite explicitely. In the example above the extension L is $L = \mathbb{Q}(\sqrt{2})$. Th.2.2 is not a special case of Th.2.1. Both follow from Th.1.1 which we call the basic result in the sequel. But different final arguments eventually lead to Th.2.1 and Th.2.2. We note in §2.4 that these results do not extend to general hilbertian fields. The

following problem however remains open : does each Hilbert subset of a hilbertian field K contain infinitely many powers b^m of some element $b \in K$? From Th.2.1, this is true for fields with the product formula. Further comments and open problems are given in §2.3 and §2.4.

Th.2.1 and Th.2.2 can be used in problems requiring the Hilbert property with additional arithmetical constraints : they allow for example to produce elements of Hilbert subsets with prescribed prime divisors. Furthermore, for this, one can even remove the "tame ramification" assumption that is present in Th.2.1 and Th.2.2. More specifically, our last result, which is another application of the basic result, shows the following general density property of Hilbert subsets. Fix a place v_o of K, consider the set $\mathfrak{V}_{v_o} = \prod_{v \neq v_o} K_v$ endowed with the "strong approximation topology", *i.e.*, the topology involved in the strong approximation theorem for global fields [CaFr ;Ch.2] (see §3 for precise definitions).

Theorem (Th.3.4) — *Let K be a field with the product formula, of characteristic 0 or imperfect of characteristic $p > 0$. Let $v_o \in M_K$ be a place of K. Assume that 0 is not isolated in K for the induced topology of $\mathfrak{V}_{v_o}$. Then every Hilbert subset of K is dense in K for the same topology.*

In other words, given any Hilbert subset $H_{P_1,\dots,P_n}$, any positive real number ε, any finite subset $S \subset M_K \backslash \{v_o\}$ such that $S \cup \{v_o\}$ contains all the archimedean places of K and any element $\beta \in K$, it is possible to find an element $a \in H_{P_1,\dots,P_n}$ such that

$$(1) \qquad \begin{cases} (i) & |a-\beta|_v < \epsilon, \text{ for all } v \in S \\ (ii) & |a-\beta|_v \leq 1, \text{ for all } v \notin S, v \neq v_o \end{cases}$$

The assumption "0 is not isolated in K" is clearly necessary in Th.3.4. When K is a number field or the function field of a curve over an algebraically closed field, this assumption is automatically satisfied : indeed it is a consequence of the Riemann-Roch theorem.

The strong approximation theorem states that for global fields, K is dense in $\mathfrak{V}_{v_o}$. Conclude then from Th.3.4 that Hilbert subsets of a global field K are actually dense in $\mathfrak{V}_{v_o}$. That is, using Morita's terminology [Mo], the strong approximation theorem is "compatible" with Hilbert's irreducibility theorem.

Density of Hilbert subsets for the "weak approximation topology", *i.e.*, the same statement but without condition (ii), is classical. The "strong density" is more difficult. Except when $K = \mathbb{Q}$ and v_o is the archimedean place, in which case this follows from the fact that Hilbert subsets of $\mathbb{Q}$ contains infinitely many *integers*. The general case of a number field was known ([Se ;Ch.9.7], [Mo], [De2]), but only as a consequence of Siegel's theorem. Due to the possibility of unseparability and wild ramification, the case of a field K of characteristic $p > 0$ is still more delicate. In this case Th.3.4 answers a question of B. Kunyavsky.

I wish to thank L. Denis and J-C. Douai for helpful discussions regarding the positive characteristic case.

NOTATION

Heights. We adhere to the notation of [La2]. 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 $(x_o, \dots, x_n) \in \mathbb{P}^n(\overline{F})$ is then defined by

$$h(x_o, \dots, x_n) = \frac{1}{[K : F]} \sum_{v \in M_K} [K_v : F_v] \ \mathrm{Log}(\max(|x_o|_v, \dots, |x_n|_v)) \tag{2}$$

where K is any field containing $x_o, \dots, x_n$. One defines the height of an element $x \in \overline{F}$ to be the height in $\mathbb{P}^1(\overline{F})$ of $(1, x)$. 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.

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 $\overline{K(T)}$. If $P(T, Y) \in K(T)[Y]$ is separable over $K(T)$, 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 $y_1, \dots, y_d$ in $\overline{K}((T - t_o))$. Then the field generated by the coefficients of y_i will be denoted by $K(y_i(t_o))$, $i = 1, \dots, d$. 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, $i=1,\dots,d$. 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 $\varphi : C \to \mathbb{P}^1$ is the finite morphism induced by T on the smooth projective model C of the curve $P(t,y)=0$, 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 $Q_1,\dots,Q_d$, which correspond to the distinct Laurent series $y_1,\dots,y_d$ 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, $i=1,\dots,d$.

§ 1 THE BASIC RESULT

1.1 Statement

The three main results of this paper are based on Th.1.1 below. Given a polynomial $P(T,Y)\in K(T)[Y]$, the *separable degree* of $P(T,Y)$ with respect to Y is defined in the following way. If K is of characteristic p, let $k\geq 0$ be the largest integer such that $P(T,Y)\in K(T)[Y^{p^k}]$; if $p=0$, the convention is that $p^k=1$. Then the separable degree of P is $\mathrm{sepdeg}_Y P=\deg_Y P/p^k$. If k is a field and u is an indeterminate, we denote the ring of power series in u with coefficients in k by $k[[u]]$ and its quotient field by $k((u))$.

THEOREM 1.1 — *Let $P_1,\dots,P_n$ be n polynomials, irreducible in $K(T)[Y]$, totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ for some integer $\mathrm{e}>0$ and such that $\deg_Y P_i\geq 2$, $i=1,\dots,n$. Let $a\in K^\times$ be a nonzero element of K such that $P_i(aT^{\mathrm{e}},Y)$ is irreducible in $K(T)[Y]$, $i=1,\dots,n$. Let b be an element of K of height $h(b)>0$. Then there exist infinitely many integers m such that each of the irreducible factors of $P_i(ab^{m\mathrm{e}},Y)$ in $K[Y]$ is of degree $\geq \max(2,\mathrm{sepdeg}_Y P_i)$, $i=1,\dots,n$.*

With no loss we may assume that $P_1,\dots,P_n$ are in $K[T,Y]$ with leading

coefficient in Y equal to 1. The rest of §1 is devoted to the proof of Th.1.1. The proof divides into two cases.

Case 1 : $P_1, \dots, P_n$ are separable over $K(T)$ and totally split in $\overline{K}((1/T))$ (*i.e.*, $\mathrm{e} = 1$) and $a = 1$.

More specifically, case 1 of Th.1.1 consists in proving this statement.

THEOREM 1.1 /Case 1 — *Let $P_1, \dots, P_n$ be n polynomials irreducible in $K[T, Y]$, separable over $K(T)$, monic in Y, unramified above $T = \infty$ and such that $\deg_Y P_i \geq 2$, $i = 1, \dots, n$. Let b be an element of K of height $h(b) > 0$. Then the Hilbert subset $H = H_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b.*

Case 2 : general case.

The main ingredient of the proof of Case 1 is the diophantine result of [De3] for "s-integral points". This result is recalled in §1.2. Then the proof of Case 1, which takes up all of §1.3, consists of five steps. Finally we prove Case 2 in §1.4, by reducing to Case 1.

1.2 s-integral points [De3]

A classical tool for studying the Hilbert property is Siegel's finiteness theorem for S-integral points on algebraic curves [La2 ;Ch.8]. We presented in [De3] 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". Th.1.2 below is one of the main results of [De3] : it is a general diophantine result for s-integral points.

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 $Br(\mathbf{P}) = \bigcup_{1 \leq i \leq n} Br(P_i)$. 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

$$(1)\qquad \begin{cases} D_t(\mathbf{P}) = \min\limits_{(y_1,\dots,y_m)} [K(t, y_1(t), \dots, y_m(t)) : K(t)] \\ D_t^+(\mathbf{P}) = \max\limits_{(y_1,\dots,y_m)} [K(t, y_1(t), \dots, y_m(t)) : K(t)] \end{cases}$$

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 $K(t), K(y_1(t)), \dots, K(y_m(t))$. Recall from the Notation that the field $K(y_i(t))$ is the field generated by the coefficients of the power series $y_i \in \overline{K}((T-t))$, $i = 1, \dots, d$. When $t = T$ is the generic point of $\mathbb{P}^1$, we use the subscript "gen" instead of "t". In this case, "$y_i \in \overline{K}((T-t))$" should be understood as "$y_i = y_i(T) \in \overline{K(T)}$".

Remark 1. 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 $P_i(T, Y)$, $i = 1, \dots, m$, and so for all but finitely many t.

Theorem 1.2 — *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*

$$(2)\qquad s\ D_\infty^+(\mathbf{P})\ D_t(\mathbf{P}) \geq D_{\mathrm{gen}}(\mathbf{P})$$

Before passing to the general proof of Th.1.1/Case 1 we give an argument that works only in characteristic 0 and explain why the possibility of wild ramification makes the case of characteristic $p > 0$ more difficult. A point $a \in \mathbb{P}^1$ is called a *tamely ramified* branch point of $\mathbf{P}$ if the polynomials $P_i(T, Y)$, $i = 1, \dots, n$ 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 $\overline{K}((T-a))$, $i=1,\dots,n$. Ramification above $T=a$ is said to be *wild* otherwise.

Proof of Th.1.1/Case 1 : characteristic 0**.** We need to show that the Hilbert subset $H=H_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b. By assumption, $\infty\notin Br(\mathbf{P})$. In addition we may assume that $1\notin Br(\mathbf{P})$: otherwise replace the polynomial $P_i(T,Y)$ by $P_i(b^\mu T,Y)$, $i=1,\dots,n$, with μ sufficiently large. Eventually ramification is automatically tame above $T=0$ in characteristic 0. It follows from Cor.2.9 of [De3] that

(3) for any integer $s>0$ there exist an integer $M>0$ and a constant h_2 with this property. For all s-integral points $t\in K$ of height $h(t)>h_2s^2$, at least one out of the M elements $t,\dots,t^M$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$.

Now take for s the number of places of K such that $|b|_v>1$. For all suitably large integers $u>0$, b^u is an s-integral point of K of height $h(b^u)=uh(b)>h_2s^2$. Conclude that for these integers u, at least one out of the M elements $b^u,\dots,b^{uM}$ belongs to the Hilbert subset $H_{P_1,\dots,P_n}$. This clearly implies that $H_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b. □

Why this does not work in characteristic $p>0$**.** For simplicity assume there is only one polynomial $P(T,Y)$ involved. The point is that the polynomial $P(T,Y)$, $i=1,\dots,n$ may be wildly ramified above $T=0$, in which case Cor.2.9 of [De3] cannot be applied. A crucial step of the proof of Cor.2.9 of [De3] consists in constructing a sequence of integers $(m_j)_{j>0}$ such that two distinct polynomials $P(T^{m_j},Y)$ can only have 0 as common branch point. In characteristic 0, this implies that the associated field extensions are linearly disjoint over $\overline{K(T)}$. This is not true in characteristic $p>0$. Another argument will be necessary to show that still one may arrange for these extensions be "relatively disjoint". Rather than the ramification, this argument will use the fact that the field extensions associated to the polynomials $P(T^{m_j},Y)$ have many automorphisms (Cf. Lemma 1.5).

1.3 Proof of Th.1.1/Case 1

Step 1 : *Preliminary reductions.*

From a standard argument (*e.g.* [La2 ;Ch.9,Prop.1.1]), there exist polynomials $Q_1, \dots, Q_N \in K[T,Y]$, irreducible over $K(T)$, with $\deg_Y Q_i \geq 2$, $i = 1, \dots, N$ and such that the set $V'_{Q_1,\dots,Q_N}$ defined by

$$V'_{P_1,\dots,P_n} = \{t \in K | P_i(t,Y) \text{ has no root in } K, i = 1, \dots, N\} \tag{4}$$

is contained in the Hilbert subset $H_{P_1,\dots,P_n}$, possibly up to a finite set F. The proof given in [La2] is quite precise ; in particular, this proof shows that

(5) If the polynomials $P_1, \dots, P_n$ are separable over $K(T)$, then so are the polynomials $Q_1, \dots, Q_N$.

(6) For all $a \in \mathbb{P}^1(\overline{K})$, if the polynomials $P_1, \dots, P_n$ are unramified above $T = a$, then so are the polynomials $Q_1, \dots, Q_N$.

[More precisely, the proof given in [La2] shows that the polynomials $Q_1, \dots, Q_N$ can be obtained in the following way. For each index $i = 1, \dots, n$, denote the roots of $P_i(T,Y)$ in $\overline{K(T)}$ by $y_{i1}, \dots, y_{id_i}$ where $d_i = \deg_Y P_i$. For each subset $A \subset \{1, \dots, d_i\}$, consider all the symmetric functions $S(y_{ij})$ in y_{ij} with $j \in A$. When i ranges from 1 to n and A over all possible subsets of $\{1, \dots, d_i\}$, one obtains a big subset of algebraic functions in $\overline{K(T)}$. Remove from it elements of $K(T)$. Then the polynomials $Q_1, \dots, Q_N$ can be taken to be the irreducible polynomials over $K(T)$ of the remaining algebraic functions. From this description, (5) and (6) follow quite easily. □]

Another classical argument shows that if a polynomial $P(T,Y) \in K[T,Y]$ is irreducible and separable over $K(T)$, but not absolutely irreducible, then the equation $P(t,y) = 0$ with $(t,y) \in K \times K$ has only finitely many solutions. More precisely, such solutions correspond to singular points on the affine curve $P(t,y) = 0$ (*i.e.*, $P'_T(t_o,y_o) = P'_Y(t_o,y_o) = 0$).

Therefore, the polynomials $Q_1, \dots, Q_N$ above can also be required to be absolutely irreducible. The conclusion of this first step is that, in order to prove Th.1.1/Case 1, it is sufficient to prove the weaker statement where the conclusion is replaced by

(7) The set $V' = V'_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b. That is, for infinitely many integers $m > 0$, the polynomial $P_i(b^m, Y)$ has no root in K, $i = 1, \dots, n$.

and where the polynomials $P_1, \dots, P_n$ are assumed to be absolutely irreducible and with $\deg_Y Q_i \geq 2$, $i = 1, \dots, N$.

Remark 2. The reduction to the case the polynomials are absolutely irreducible uses the separability assumption. Without the separability, one can still reduce to a slightly weaker property. Namely, Prop.1.3 below shows that one may assume that the polynomials $Q_1, \dots, Q_N$ have a trivial constant field. This will be used in §3.2. Recall that given a polynomial $P(T, Y)$ irreducible in $K(T)[Y]$ and an embedding of the associated function field $R_P = K(T)[Y]/(P(T, Y))$ in $\overline{K(T)}$, the constant field C_P of P over K is defined by $C_P = R_P \cap \overline{K}$. If $P(T, Y)$ is absolutely irreducible, then $C_P = K$. The converse is true if the polynomial $P(T, Y)$ is separable over $K(T)$.

Proposition 1.3 — *Let $P(T, Y)$ be irreducible in $K(T)[Y]$. Assume that the constant field C_P of P over K is a proper extension of K. Then there are only finitely many solutions $(t_o, y_o) \in K^2$ to the equation $P(t, y) = 0$.*

Proof. Let $\alpha \in \overline{K}$ and $M(Y)$ be the irreducible polynomial of α over K. If $\alpha \in C_P$, then the polynomial $M(Y)$ has a root in the function field R_P of $P(T, Y)$. That is, there exists $F(T, Y), Q(T, Y) \in K(T)[Y]$ such that

$$M(F(T, Y)) = Q(T, Y)P(T, Y) \tag{8}$$

Now assume that there are infinitely many points $(t_o, y_o) \in K^2$ on the affine curve $P(t, y) = 0$. All but finitely many of these points (t_o, y_o) can be substituted for (T, Y) in (8). We obtain $M(F(t_o, y_o)) = 0$ for infinitely many $(t_o, y_o) \in K \times K$. In particular, $M(Y)$ has a root in K. That is, $\alpha \in K$. This shows that $C_P = K$, which contradicts the hypotheses. □

Step 2 : *For each integer $m > 0$, the polynomial $P_i(T^m, Y)$ is absolutely irreducible and unramified above $T = \infty$, $i = 1, \dots, n$.*

For $m = 1$, this is part of the assumption. The "unramified" part for all integers $m > 0$ is then clear. The "absolutely irreducible" part follows for

example from results of [De2] which we recall in §2.2.4, or also, from the more general Prop.2.3 of [De3].

Step 3 : *Construction of a sequence $(m_j)_{j>0}$ of integers with certain properties.*

The goal of this step is to show the following.

PROPOSITION 1.4 — *There exists a strictly increasing sequence $(m_j)_{j>0}$ of integers with this property. Denote the splitting field over $\overline{K}(T)$ of the polynomial $P_i(T^{m_j}, Y)$ by E_{ij}, $i = 1, \ldots, n$, $j > 0$. For all $j > 0$ and $i = 1, \ldots, n$, if $y_{i\,j+1} \in \overline{K(T)}$ is an arbitrary root of $P_i(T^{m_{j+1}}, y_{i\,j+1}) = 0$, we have*

$$\overline{K}(T, y_{i\,j+1}) \not\subset E_{11} \cdots E_{n1} \cdots E_{1j} \cdots E_{nj} \tag{9}$$

Proof. The sequence $(m_j)_{j>0}$ is defined inductively. Let $m_1 > 0$ be any integer. Assume that $m_1, \ldots, m_J$ are J integers such that $m_1 < \cdots < m_J$ and such that (9) holds for each $j = 1, \ldots, J-1$. Denote the field $E_{11} \cdots E_{n1} \cdots E_{1J} \cdots E_{nJ}$ by $E(J)$. Since $\infty \notin Br(\mathbf{P})$, the field $E(J)$ can be viewed as a subfield of $\overline{K}((1/T))$. We need to prove that there exists an integer m_{J+1} such that $E(J)$ contains none of the finite list of all the roots in $\overline{K}((1/T))$ of the polynomials $P_i(T^{m_{J+1}}, Y)$, $i = 1, \ldots, n$. Assume the contrary holds. Then, there exists $i = 1, \ldots, n$ and $y \in \overline{K}((1/T))$ such that $P_i(T, y) = 0$ and such that $y(T^m) \in E(J)$ for infinitely many integers m. This contradicts the following lemma. □

LEMMA 1.5 — *Let $(n_j)_{j>0}$ be any strictly increasing sequence of integers not divisible by the characteristic p of K. Then if i is any index in $\{1, \ldots, n\}$ and y is any root in $\overline{K}((1/T))$ of $P_i(T, y) = 0$, then the subfield*

$$\overline{K}(T, \{y(T^{n_j}), j > 0\})$$

of $\overline{K}((1/T))$ generated by all the $y(T^{n_j})$ with $j > 0$, is of infinite degree over $\overline{K}(T)$.

Proof. Set $P_i = P$ for simplicity. Assume that the field extension

$$\overline{K}(T, \{y(T^{n_j}), j > 0\})/\overline{K}(T)$$

is of finite degree. From Galois theory, there exists a subextension $E/\overline{K}(T)$ such that

$$E = \overline{K}(T, y(T^{n_j})) \tag{10}$$

for infinitely many $j > 0$. (This uses the separability assumption of Case 1 of Th.1.1).

Let $j > 0$ and $\zeta \in \overline{K}$ be a n_jth root of 1. The automorphism of $\overline{K}((1/T))$ mapping T to ζT induces an automorphism of $\overline{K}(T, y(T^{n_j}))$, which we denote by Λ. Let $\phi : C \to \mathbb{P}^1$ be the finite morphism of smooth projective curves corresponding to the field extension $E/\overline{K}(T)$. Denote the automorphism of $\mathbb{P}^1$ corresponding to the rational function ζT by λ. If the integer j satisfies (10), the automorphism Λ corresponds to an automorphism $C \to C$, still denoted by Λ, such that $\phi \circ \Lambda = \lambda \circ \phi$. In particular, since $\lambda(\infty) = \infty$, Λ permutes the elements of the fiber $\phi^{-1}(\infty)$. Similarly, Λ permutes the elements of the fiber $\phi^{-1}(0)$. Since $P(T^{n_j}, Y)$ is unramified above $T = \infty$ and is absolutely irreducible (Step 1), the fiber $\phi^{-1}(\infty)$ consists of at least $\deg_Y P$ distinct points. Conclusion : if the integer j is such that (10) holds, then the curve C has at least n_j automorphisms (corresponding to the n_j n_jth roots of 1 in $\overline{K}$), which permute the elements of a fixed subset of C of cardinality $\geq \deg_Y P + 1 \geq 3$ (namely the subset $\phi^{-1}(\infty) \cup \phi^{-1}(\infty)$). Lemma 1.6 below shows this cannot occur for infinitely many integers n_j. □

LEMMA 1.6 — *Let C be an algebraic curve defined over $\overline{K}$. Then there are only finitely many automorphisms of C sending three given points of C in a finite subset of C.*

Proof. We need to prove that there are only finitely many automorphisms of C fixing three given points of C. Let g be the genus of C. For $g = 0$, it is a classical property of $\mathrm{Aut}(\mathbb{P}^1) = PGL(2)$. If $g \geq 2$, the curve C has anyway only finitely many automorphisms. This is Hurwitz's theorem in characteristic 0 [Hu] ; the case of positive characteristic is due to Schmid [Sch]. As for $g = 1$, the result is true with "three given points" replaced by

"one given point". Indeed select one point $O \in C(\overline{K})$; (C, O) is an elliptic curve. Any automorphism ϕ of C is of the form $\phi = \tau \circ F$ where τ is a translation and F is an automorphism of the elliptic curve (C, O). The automorphism ϕ is completely determined by F and the image $\phi(A)$ of any given point A of C. Conclusion follows from the fact that the number of automorphisms of an elliptic curve is finite [Si ;Ch.3]. □

Step 4 : *Final strategy and choice of parameters.*

We will establish the following statement (which is the same as (3) except that "$H_{P_1,\dots,P_n}$" is replaced by "$V'_{P_1,\dots,P_n}$").

(11) For any integer $s > 0$ there exist an integer $M > 0$ and a constant h_2 with this property. For all s-integral points $t \in K$ of height $h(t) > h_2 s^2$, at least one out of the M elements $t, \dots, t^M$ belongs to the set $V'_{P_1,\dots,P_n}$.

As explained in §1.2, it then suffices to take $t = b^u$ with u any suitably large integer to obtain that $V'_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b, *i.e.*, conclusion (7).

From now on fix an integer $s > 0$. Select an integer J such that

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

Then take for M the Jth term of the sequence $(m_j)_{j>0}$ constructed in Step 3. Finally define the constant h_2 to be the largest one of the constants h_1 of Th.1.2 associated with the families $\mathbf{P_i} = \{P_{i_1}(T, Y), \dots, P_{i_M}(T^M, Y)\}$ where $\mathbf{i} = (i_1, \dots, i_m)$ ranges over all families of indices $i_j \in \{1, \dots, n\}$ indexed by $\{1, \dots, M\}$.

Let t be an s-integral point of K of height $h(t) > h_2 s^2$. Assume that conclusion (11) does not hold, *i.e.*, that, for each $m = 1, \dots, M$, at least one out of the polynomials $P_i(t^m, Y)$ $(i = 1, \dots, n)$ has a root in K. In particular

(13) for each $j = 1, \dots, J$ there exists an index $i_j \in \{1, \dots, n\}$ such that the polynomial $P_{i_j}(t^{m_j}, Y)$ has a root $y_j(t) \in K$.

We show now how this leads to a contradiction.

Step 5 : *Applying* [De3].

Consider the family of polynomials $\mathbf{P_i} = \{P_{i_1}(T^{m_1}, Y), \dots, P_{i_J}(T^{m_J}, Y)\}$ where $\mathbf{i} = (i_1, \dots, i_J)$ is the J-tuple given by (13). By hypothesis, polynomials in $\mathbf{P_i}$ are separable over $K(T)$. From Step 2, they are unramified above $T = \infty$. Applying Th.1.2 to the family $\mathbf{P_i}$ gives

$$1 = [K(y_1(t), \dots, y_J(t)) : K] \geq \frac{D_{\text{gen}}(\mathbf{P_i})}{sD^+_\infty(\mathbf{P_i})} \tag{14}$$

Now it follows from Prop.2.2 of [De3] that

$$D^+_\infty(\mathbf{P_i}) \leq (\deg_Y P_1)! \cdots (\deg_Y P_n)! \tag{15}$$

Substitute (15) back in (14) to obtain

$$D_{\text{gen}}(\mathbf{P_i}) \leq s(\deg_Y P_1)! \cdots (\deg_Y P_n)! \tag{16}$$

Now it follows from Prop.1.4 that $D_{\text{gen}}(\mathbf{P_i}) \geq 2^J$, which, together with (16), contradicts (12). This achieves the proof of Th.1.1/Case1. □

1.4 Proof of Th.1.1 : general case

We will reduce to the first case. For $i = 1, \dots, n$, let $k_i \geq 0$ be the largest integer such that $P_i(T, Y) \in \overline{K}(T)[Y^{p^{k_i}}]$ and $\hat{P}_i(T, Y) \in K[T, Y]$ be the polynomial defined by

$$\hat{P}_i(T, Y^{p^{k_i}}) = P_i(aT^{\text{e}}, Y)$$

The polynomial $\hat{P}_i(T, Y)$ is irreducible in $K[T, Y]$. Furthermore, it is separable over $K(T)$. Finally from the assumption on e, it is unramified above $T = \infty$. From the first case, there exist infinitely many powers b^m of b such that $\hat{P}_i(b^m, Y)$ is irreducible in $K[Y]$, $i = 1, \dots, n$. This implies that for those m, $P_i(ab^{m\text{e}}, Y)$ has all of its roots of degree over K larger than or equal to $\deg_Y \hat{P}_i = \text{sepdeg}_Y P_i$, $i = 1, \dots, n$.

We are left with the case that for some index i, $\text{sepdeg}_Y P_i = 1$. Then K is necessarily of characteristic $p > 0$. The proof will be complete if we show that for all but finitely many m, $P_i(ab^{m\text{e}}, Y)$ has no root in

K. The polynomial $P_i(T,Y)$ is of the form $P_i(T,Y) = Y^{p^k} - A(T)$ with $A(T) \in K[T]$. The polynomial $P_i(aT^{\mathrm{e}},Y) = Y^{p^k} - A(aT^{\mathrm{e}})$ is totally split in $\overline{K}((1/T))$, so $A(aT^{\mathrm{e}}) \in \overline{K}((1/T))^p \cap K(T) = K(T^p)$. But by hypothesis $P_i(aT^{\mathrm{e}},Y) = Y^{p^k} - A(aT^e)$ is irreducible in $K[T,Y]$ so $A(aT^{\mathrm{e}}) \notin K(T)^p$. Therefore $A(aT^{\mathrm{e}})$ is of the form $B(T^p)$ with $B \in K[T] \setminus K^p[T]$. Conclude from Lemma 2.8 (a) of [De3] that there are only finitely many integers $m > 0$ such that $B((b^m)^p) = A(ab^{m\mathrm{e}}) \in K^p$. □

Th.1.1 is the main ingredient of the proofs of the three main results of this paper. The rest of this paper essentially consists in reducing to a situation where the assumption of Th.1.1 holds, *i.e.*, where there exists a nonzero element $a \in K^\times$ and an integer $\mathrm{e} > 0$ such that the polynomials $P(T,Y)$ involved have the property that $P(aT^{\mathrm{e}},Y)$ is irreducible in $K(T)[Y]$ and unramified above $T = \infty$. This is a function field part. For Th.2.1, the main argument is Prop.3 of [De1]. For Th.2.2 and Th.3.4, we use previous results of [De2] on the irreducibility of polynomials of the form $P(T^m,Y)$.

§ 2 SPECIALIZING TO POWERS

2.1 Proof of Theorem 2.1

We start with Th.2.1 which is a little easier to establish.

2.1.1. Restatement of Th.2.1.

THEOREM 2.1 — *Let K be a field with the product formula. Let $H_{P_1,\dots,P_n}$ be a Hilbert subset of K with $P_1,\dots,P_n$ irreducible in $K(T)[Y]$ and totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ for some integer $\mathrm{e} > 0$. Then there exists a finite extension L of K with the following property. Let b be an element of K of height $h(b) > 0$ and such that*

(1) $b \notin L^\ell$ for all prime divisors ℓ of e and $b \notin -4L^4$ if 4 divides e.

Then the Hilbert subset $H_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b.

Th.2.1 is more precise than the one stated in the introduction. Assumption on b was essentially that (1) holds for all integers $\mathrm{e} > 0$. Also the polynomials are here only assumed to be totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$. This holds if the polynomials are, as in the introduction, separable and tamely ramified above $T = \infty$. But the converse is not true (take $P(T,Y) = Y^p - T \in$

$\mathbb{F}_p(T)[Y]$). Recall that these conditions automatically hold in characteristic 0. Finally the proof below gives a description of the extension L/K of Th.2.1.

2.1.2. Proof of Th.2.1. It is sufficient to prove the weaker conclusion where $H = H_{P_1,\dots,P_n}$ is replaced by $V'_{P_1,\dots,P_n}$ (with the extra assumption that $\deg_Y P_i \geq 2$, $i = 1,\dots,n$). For $i = 1,\dots,n$, let

$$P_i(T^{\mathrm{e}}, Y) = \Pi_{i1} \cdots \Pi_{ir_i}$$

be a factorization of $P_i(T^{\mathrm{e}}, Y)$ in irreducible polynomials in $\overline{K}(T)[Y]$. Define the extension L/K as follows

(2) L is the extension of K generated by the coefficients in $\overline{K}$ of all the polynomials Π_{ij}, $i = 1,\dots,n$, $j = 1,\dots,r_i$.

The extension L/K is finite. Let b be an element of K of height $h(b) > 0$ and such that condition (1) holds. From Capelli's lemma [La1 ;p.221], the polynomial $Y^{\mathrm{e}} - b$ is irreducible in $L[Y]$. It follows then from Prop.3 of [De1] that the polynomial $P_i(bT^{\mathrm{e}}, Y)$ is irreducible in $K(T)[Y]$ (in [De1], the result is stated for $K = \mathbb{Q}$ but the proof is valid for any field).

Conclude from Th.3.1 that for infinitely many integers m, the polynomial $P_i(b^{m\mathrm{e}+1}, Y)$ has all of its irreducible factors of degree ≥ 2, $i = 1,\dots,n$. □

2.2 Proof of Theorem 2.2

2.2.3. Restatement and generalisation of Th.2.2 and Th.2.3. The following result is a little more precise than the one stated in the introduction.

THEOREM 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 for some integer $\mathrm{e} > 0$, $P(T,Y)$ is totally split either in $\overline{K}((T^{1/\mathrm{e}}))$ or in $\overline{K}(((1/T)^{1/\mathrm{e}}))$. Let b be an element of K of height $h(b) > 0$ such that*

(3) $b \notin K^\ell$ for all prime divisors ℓ of e and $-b \notin K^2$ if 4 divides e.

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

Th.2.2 is not a special case of Th.2.1, but rather of Th.2.3 below. This new result is similar to Th.2.1 : several polynomials are involved, the condition on b is of the same kind as in Th.2.1, but for another extension C/K instead of L/K. In certain situations this extension is easier to control than the extension L/K. For example, the extension L/K can be non trivial even though the polynomials $P_1, \dots, P_n$ are absolutely irreducible : take $n = 2$, $P_1 = Y^2 - T$, $P_2 = Y^2 - 2T$, then $L = K(\sqrt{2})$. In the same example, the extension C/K of Th.2.3 is trivial. On the other hand, there is in Th.2.3 an extra assumption on the number of polynomials $P_1, \dots, P_n$. Miraculeously this assumption is always empty in the special case of a single absolutely irreducible polynomial. This special case of Th.2.3 is Th.2.2.

THEOREM 2.3 — *Let K be a field with the product formula. Let $P_1(T,Y), \dots, P_n(T,Y)$ be n irreducible polynomials in $K(T)[Y]$, separable over $K(T)$ and totally split in $\overline{K}((T^{1/\mathrm{e}_1})), \dots, \overline{K}((T^{1/\mathrm{e}_n}))$ respectively for some integers $\mathrm{e}_1, \dots, \mathrm{e}_n > 0$. Let D_{P_i} be the set of divisors ℓ of e_i such that ℓ is a prime or $\ell = 4$ and let $y_{P_i} \in \overline{K(T)}$ be a root of $P_i(T,Y)$, $i = 1, \dots, n$. Set $D_{\mathbf{P}} = \bigcup_{1 \le i \le n} D_{P_i}$. Assume that*

(4) for each $\ell \in D_{\mathbf{P}}$, the number of indices $i \in \{1, \dots, n\}$ such that $\ell \in D_{P_i}$ is $< \ell$ if $\ell \neq 4$ and is < 2 if $\ell = 4$.

Let C be a field containing all the constant fields of the function fields $K(T, y_{P_i})$, $i = 1, \dots, n$. Let b be an element of K of height $h(b) > 0$ such that

(5) $b \notin C^\ell$ for all prime divisors ℓ of e and $-b \notin K^2$ if 4 divides e.

Then the Hilbert subset $H_{P_1,\dots,P_n}$ contains infinitely many powers b^m of b.

2.2.4. Preliminary results. The following result is used in the proof and in several other places of this section.

PROPOSITION 2.4 — *Let $P(T,Y)$ be a polynomial irreducible in $K(T)[Y]$ and totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ for some integer $\mathrm{e} > 0$. Let $y_P \in \overline{K(T)}$ be a root of $P(T,Y)$. Let $m > 0$ be an integer. The following statements are equivalent.*

(i) The polynomial $P(T^m, Y)$ is reducible in $K(T)[Y]$.

(ii) $T \in K(T,y_P)^\ell$ *for some common prime divisor* ℓ *of* e *and* m*, or* 4 *divides* e *and* m *and* $T \in -4K(T,y_P)^4$*.*

In particular, if $P(T,Y)$ *is unramified above* $T=\infty$ *(i.e.,* e $=1$*), then* $P(T^m,Y)$ *is irreducible in* $K(T)[Y]$ *for all integers* m*.*

Proof. See [De2 ;§2]. (In [De2], the base field is of characteristic 0 but the only role of this assumption is to guarantee that polynomials $P(T,Y) \in K(T)[Y]$ are totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ for some integer e >0. Thus [De2 ;§2] is valid for any field provided that such a condition is added to the hypotheses.) □

The basic lemma for Th.2.2 and Th.2.3 is this.

LEMMA 2.5 — *Let* $P(T,Y) \in K(T)[Y]$ *be a polynomial, irreducible in* $K(T)[Y]$ *and totally split in* $\overline{K}(((1/T)^{1/\mathrm{e}}))$ *for some integer* e >0*. Let* $y_P \in \overline{K(T)}$ *be a root of* $P(T,Y)$*. Let* D_P *be the set of divisors* ℓ *of* e *such that* ℓ *is a prime or* $\ell=4$*. Let* $C \subset \overline{K}$ *be a field containing the constant field* C_P *of the function field* $K(T,y_P)$*, i.e.,* $C_P = K(T,y_P)\cap\overline{K}$*. Let* b *be an element of* K *such that (5) holds. Then there exists a family of integers* $(u_\ell)_{(\ell\in D_P)}$ *with the following property. For all* $\ell \in D_P$*, if* u *is an integer such that*

$$(6)\qquad \begin{cases} u \not\equiv u_\ell \pmod{\ell} & \text{if } \ell \neq 4 \\ u \not\equiv u_\ell \pmod{\ell} \text{ and } u \not\equiv u_2 \pmod 2 & \text{if } \ell = 4 \end{cases}$$

Then $P(b^uT^\ell,Y)$ *is irreducible in* $K(T)[Y]$*.*

Proof. For each $\ell \in D_P \setminus \{4\}$, define the integer u_ℓ in the following way : if $P(b^uT^\ell,Y)$ is irreducible in $K(T)[Y]$ for all integers $u>0$, set $u_\ell = 0$; in the opposite case, pick an arbitrary u such that $P(b^uT^\ell,Y)$ is reducible in $K(T)[Y]$ and set $u_\ell = u$. For $\ell=4$, take for u_4 an arbitrary integer such that $b^{-u_4}T$ lies in $-4K(T,y_P)^4$ and set $u_4=0$ if there are none of them.

Let $\ell \in D_P$ and u be an integer satisfying (6). Assume that $P(b^uT^\ell,Y)$ is reducible in $K(T)[Y]$.

1st case : $\ell \neq 4$. From Prop.2.4, both $b^{-u}T$ and $b^{-u_\ell}T$ lie in $K(T,y_P)^\ell$. Consequently, b^{u-u_ℓ} is the ℓth power of some element in $K(T,y_P)$, which is

automatically in C. Conclude from (5) that $u \equiv u_\ell \pmod{\ell}$, a contradiction.

2nd case : $\ell = 4$. From the first case, since $u \not\equiv u_2 \pmod 2$, $P(b^u T^2, X)$ is irreducible in $K(T)[Y]$. So $b^{-u}T \notin K(T, y_P)^2$. It follows then from Prop.2.4 that if $P(b^u T^4, Y)$ is reducible in $K(T)[Y]$, then both $b^{-u}T$ and $b^{-u_4}T$ lie in $-4K(T, y_P)^4$. Conclude like in the first case that b^{u-u_ℓ} is the 4th power of some element in C. Then it follows from "$b \notin C^2$" that $u \equiv u_4 \pmod 2$ and $b^2 \in C^4$. Therefore b or $-b$ is a square in C, a contradiction. □

2.2.5. Proof of Th.2.2. (and Th.2.2.3). One may assume that $P(T, Y)$ is totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$: otherwise change T to $1/T$ and b to $1/b$ (note that condition (3) holds equivalently for b and $1/b$. The polynomial $P(T, Y)$ is also assumed to be absolutely irreducible. Hence, one can take $C = K$ in Lemma 2.5. Let b be an element of K of height $h(b) > 0$ and such that (3) holds. We wish to show that the polynomial $P(b^m, Y)$ is irreducible in $K[Y]$ for infinitely many m.

Apply the Chinese remainder theorem to find an integer u such that $u \not\equiv u_\ell \pmod{\ell}$ for all $\ell \in D_P$. Conclude from Lemma 2.5 that $P(b^u T^\ell, Y)$ is irreducible in $K(T)[Y]$ for all $\ell \in D_P$. It follows then from Prop.2.4 that $P(b^u T^{\mathrm{e}}, Y)$ is irreducible in $K(T)[Y]$. Apply Th.1.1 to complete the proof of Th.2.2 (note that $\mathrm{sepdeg}_Y P = \deg_Y P$ because of the separability assumption).

The same argument works for several polynomials $P_1, \ldots, P_n$ provided that one can find an integer u satisfying (6) for all the polynomials simultaneaously. It is the role of assumption (4) in Th.2.2.3. □

2.3 Cyclhilbertian Hilbert subsets

From Capelli's lemma, condition (3) of Th.2.2 (or condition (1) of Th.2.1) is essentially equivalent to the irreducibility of the polynomial $Y^{\mathrm{e}} - b$ in $K[Y]$. So Th.2.2 says this in particular : the knowledge of elements in the Hilbert subset associated with the polynomial $Y^{\mathrm{e}} - T$ automatically provides explicit elements in the Hilbert subset H_P. More generally, call cyclhilbertian a Hilbert subset $H_{P_1,\ldots,P_n}$ if the polynomials $P_1, \ldots, P_n$ are of the form $Y^{\mathrm{e}} - aT$ where $\mathrm{e} > 0$ is an integer and $a \in K^\times$. It is tempting to ask whether a field K such that all cyclhilbertian subsets are infinite is hilbertian ? The

answer is "No". The subfield $K = \mathbb{Q}^{tr}$ of $\overline{\mathbb{Q}}$ of all totally real algebraic numbers is a counterexample. Indeed, $\mathbb{Q}^{tr}$ is not hilbertian : the Hilbert subset H_P with $P = Y^2 - (T^2+1)$ is empty. Now we have.

PROPOSITION 2.6 — *If* $\mathrm{e} > 0$ *is an integer and* $a \in K^\times$*, then* $Y^{\mathrm{e}} - a\sqrt{q}$ *is irreducible in* $\mathbb{Q}^{tr}[Y]$ *for all but finitely many prime numbers* $q > 0$*. In particular, cyclhilbertian subsets of* $\mathbb{Q}^{tr}$ *are infinite.*

Proof. Let D_{e} be the set of divisors ℓ of e such that

$$\text{(7)} \qquad \begin{cases} \bullet\ \ell \text{ is a prime and } \exists\ b \in \mathbb{Q} \text{ such that } a^{-1}\sqrt{b} \in \left(\mathbb{Q}^{tr}\right)^{\ell}, \text{ or} \\ \bullet\ \ell = 4 \text{ and } \exists\ b \in \mathbb{Q} \text{ such that } a^{-1}\sqrt{b} \in -4\left(\mathbb{Q}^{tr}\right)^{4} \end{cases}$$

For each $\ell \in D_{\mathrm{e}}$, pick an integer $b = b_\ell$ satisfying (7). Then let $q > 0$ be a prime number such that $|b_\ell|_q = 1$ for all $\ell \in D_{\mathrm{e}}$.

Let ℓ be a prime divisor of e. We claim that

$$\text{(8)} \qquad a\sqrt{q} \notin \left(\mathbb{Q}^{tr}\right)^{\ell}$$

This is clear if $\ell \notin D_{\mathrm{e}}$. So assume $\ell \in D_{\mathrm{e}}$. Then showing (8) is equivalent to showing $\sqrt{qb_\ell} \notin (\mathbb{Q}^{tr})^{\ell}$. From Capelli's lemma, $Y^{2\ell} - qb_\ell$ is irreducible in $\mathbb{Q}[Y]$. Consequently, the conjugates of $(\sqrt{qb_\ell})^{1/\ell}$ over $\mathbb{Q}$ are all the $\zeta(\sqrt{qb_\ell})^{1/\ell}$ where ζ runs over the set $\mu_{2\ell}$ of all 2ℓth roots of 1. Since $\mu_{2\ell} \not\subset \mathbb{R}$, conclude that $\sqrt{qb_\ell} \notin (\mathbb{Q}^{tr})^{\ell}$.

Similarly, one shows that if 4 divides e then

$$\text{(9)} \qquad a\sqrt{q} \notin -4\left(\mathbb{Q}^{tr}\right)^{4}$$

Again use Capelli's lemma to conclude from (8) and (9) that $Y^{\mathrm{e}} - a\sqrt{q}$ is irreducible in $\mathbb{Q}^{tr}[Y]$. □

REMARK 1. Prop.2.6 shows that Th.2.2 is not true for elements $b \in K$ of height $h(b) = 0$. Indeed let $P(T,Y) \in \mathbb{Q}^{tr}[T,Y]$ be an absolutely irreducible polynomial. If X is an indeterminate, the polynomial $P(T,Y)$, regarded in $\mathbb{Q}^{tr}(X,T)[Y]$, is still absolutely irreducible. The field $\mathbb{Q}^{tr}(X)$ is a field with the product formula. From Prop.2.6, one can pick an element $b \in \mathbb{Q}^{tr}$ such that $Y^{(\deg_Y P)!} - b$ is irreducible in $\mathbb{Q}^{tr}[Y]$. Then $Y^{(\deg_Y P)!} - b$ is still irreducible in $\mathbb{Q}^{tr}(X)[Y]$ and $h(b) = 0$ where h is the height attached

to $\mathbb{Q}^{tr}(X)$. If Th.2.2 were true with $h(b) = 0$, then $P(b^m, Y)$ would be irreducible in $\mathbb{Q}^{tr}(X)[Y]$ and a fortiori in $\mathbb{Q}^{tr}[Y]$, for infinitely many integers $m > 0$. This contradicts the fact that, as we noted above, Hilbert subsets H_P of $\mathbb{Q}^{tr}$ may be empty.

2.4 Further remarks and problems

Th.2.1 has this hypothesis :

(10) The polynomials $P_1, \ldots, P_n$ are totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ for some integer $\mathrm{e} > 0$.

What happens if this hypothesis is removed ? That is, essentially, if there is wild ramification above ∞ for some of the polynomials $P_1, \ldots, P_n$. Of course this can occur only in characteristic $p > 0$.

More precisely, let K be a field with the product formula. For simplicity, take $n = 1$ and $P_1(T, Y) = P(T, Y)$ absolutely irreducible and separable over $K(T)$ (as in Th.2.2). But do not assume anymore that (10) holds. Let $b \in K$ of height $h(b) > 0$ and such that

(11) $b \notin K^\ell$ for all prime numbers ℓ and $-b \notin K^2$.

The questions are :

Problem 2.7 — *Under the conditions above is it true that $P(b^m, Y)$ is irreducible in $K[Y]$ for infinitely many integers $m > 0$? Can condition (11) be removed if ramification is wild above ∞ ?*

We have other questions. By using Siegel's theorem the two following statements can be proved in the case that K is a number field [De2 ;Cor.1.6 and Cor.1.7].

(12) If $P(T, Y)$ is irreducible in $K(T)[Y]$ and is unramified above $T = \infty$, then for each $b \in K^\times$ of height $h(b) > 0$, the polynomial $P(b^m, Y)$ is irreducible in $K[Y]$ for all but finitely many integers $m > 0$.

(13) Let H be a Hilbert subset of K and b be an element of K of height $h(b) > 0$. Then there exists $a \in K \setminus \{0\}$ such that $P(ab^m, Y)$ is irreducible in $K[Y]$ for all but finitely many integers $m > 0$.

Th.2.2 gives (12) for a field with the product formula but with "for all but finitely many integers $m > 0$" replaced by "for infinitely many integers $m > 0$". The following example shows one cannot expect (12) to extend to fields with the product formula in general.

EXAMPLE 1. Take $K = \mathbb{F}_p(X)$ with X an indeterminate and $P(T, Y) = Y^p - Y - \frac{1}{T}$. Then if $b = 1/(u^p - u)$ with $u \in K$, then we have, for all integers $k > 0$

$$1/b^{p^k} = (u^p - u)^{p^k} = (u^{p^k})^p - (u^{p^k})$$

Therefore $P(b^m, Y)$ has a root in K for all integers of the form $m = p^k$ $(k > 0)$.

On the other hand, concerning (13) the question is still open.

PROBLEM 2.8 — *Does (13) hold if K is a field with the product formula ?*

Finally the following example, due to Geyer [FrJ ;Ex.14.19], shows that Th.2.2 does not extend to general hilbertian fields, even in characteristic 0.

EXAMPLE 2. Take $K = k((X_1, X_2))$ the field of formal power series in two variables over an arbitrary field k (of characteristic $p \neq 2$). This is an hilbertian field [FrJ ;Cor.14.18]. Take $P(T, Y) = Y^2 - (1 + X_1 T)$. Then $P(b, Y)$ is reducible in $K[Y]$ for all $b \in k[[X_1, X_2]]$.

But the following weaker problem remains open.

PROBLEM 2.9 — Prove or disprove the following statement :

(14) Let K be a hilbertian field and H be a Hilbert subset of K. Then there exists $b \in K$ such that H contains infinitely many powers b^m of b.

§ 3 THE STRONG APPROXIMATION PROPERTY

The goal of this paragraph is to prove Th.3.4 below (also stated in the introduction). The main tool is Th.1.1. The role of Lemma 3.1 is to reduce to the case "$P_1, \ldots, P_n$ totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ for some integer $\mathrm{e} > 0$". It remains then to show the existence of an element a like in Th.1.1. This

is the purpose of Lemma 3.2. Putting together these three results yields Th.3.3. Th.3.4 follows then readily from Th.3.3.

3.1 Preliminaries

LEMMA 3.1 — *Let $P(T,Y)$ be a polynomial irreducible in $K(T)[Y]$. Then for all but finitely many $t_o \in K$, the polynomial $P(t_o + \frac{1}{T}, Y)$ is totally split in $\overline{K}(((1/T)^{1/p^{\deg_Y P}}))$ (with the convention that if K is of characteristic $p = 0$, then $p^{\deg_Y P} = 1$).*

Proof. This is standard in characteristic 0. Assume K is of characteristic $p > 0$. Let $k \geq 0$ be the largest integer such that $P(T,Y) \in \overline{K}(T)[Y^{p^k}]$ and $\hat{P}(T,Y) \in K[T,Y]$ be the polynomial defined by $\hat{P}(T,Y^{p^k}) = P(T,Y)$. The polynomial $\hat{P}(T,Y)$ is irreducible and separable over $K(T)$. Therefore the discriminant $\Delta(T) \in K(T)$ of $\hat{P}(T,Y)$ is a nonzero polynomial. Let $t_o \in K$ such that $\Delta(t_o) \neq 0$. Then the polynomial $\hat{P}(t_o + \frac{1}{T}, Y)$ is totally split in $\overline{K}((1/T))$. Conclude that $P(t_o + \frac{1}{T}, Y)$ is totally split in $\overline{K}(((1/T)^{1/p^k}))$. □

LEMMA 3.2 — *Assume that the field K is imperfect of characteristic $p > 0$ (i.e., K^p is properly contained in K). Then the group $K^\times/(K^\times)^p$ is infinite.*

Proof. The following argument is inspired by the proof of Lemma 11.15 of [FrJ]. Assume on the contrary that $K^\times/(K^\times)^p$ consists of the classes of finitely many elements $\gamma_1, \ldots, \gamma_\rho$ of $K^\times$. Pick an element β in $K \setminus K^p$. Then $\gamma_j T + \gamma_j \beta \notin K^p[T]$, $j = 1, \ldots, \rho$. Then, from Lemma 2.8 of [De3], for each $j = 1, \ldots, \rho$, there is at most one element $t \in K$ such that $\gamma_j t^p + \gamma_j \beta \in K^p$. Conclude that, excluding finitely many $t \in K$, $\gamma_j(t^p + \beta) \notin K^p$, $j = 1, \ldots, \rho$. A contradiction. □

3.2 Applying Th.1.1

Th.3.4 will be an easy consequence of the following more precise result.

THEOREM 3.3 — *Let K be a field with the product formula, of characteristic 0 or imperfect of characteristic $p > 0$. Let $H = H_{P_1,\ldots,P_n}$ be a Hilbert subset of K with $P_1, \ldots, P_n$ irreducible in $K(T)[Y]$. Then for all but*

finitely many $t_o \in K$, there exists $a \in K^\times$ with the following property. If b is an element of K of height $h(b) > 0$, then the Hilbert subset H contains infinitely many elements of K of the form $t_o + ab^m$ $(m > 0)$.

Proof. It is sufficient to prove the weaker conclusion where $H = H_{P_1,\dots,P_n}$ is replaced by $V' = V'_{P_1,\dots,P_n}$ (with the extra assumption that $\deg_Y P_i \geq 2$, $i = 1,\dots,n$). Also, from Prop.1.3, one may assume that the polynomials $P_1,\dots,P_n$ have a trivial constant field. Fix an integer D such that $D \geq \deg_Y P_i$, $i = 1,\dots,n$. Using Lemma 3.1, pick $t_o \in K$ such that $P_i(t_o + \frac{1}{T}, Y)$ is totally split in $\overline{K}(((1/T)^{1/p^D}))$, $i = 1,\dots,n$.

Set $\mathrm{e} = p^D$. We show next that

(1) There exists $a \in K^\times$ such that $P_i(t_o + \frac{a}{T^{\mathrm{e}}}, Y)$ is irreducible in $K(T)[Y]$, $i = 1,\dots,n$.

In characteristic 0, $\mathrm{e} = 1$; take $a = 1$. Assume K is of characteristic $p > 0$. In fact, from Prop.2.4, given $a \in K^\times$, if for some index i, $P_i(t_o + a/T^{\mathrm{e}}, Y)$ is reducible in $K(T)[Y]$, then aT should lie in the pth power of the function field over K of $P_i(t_o + 1/T, Y)$. Use the assumption on the constant fields of $P_1,\dots,P_n$ to conclude that two elements $a, a' \in K^\times$ with the same property are necessarily in the same coset of $K^\times$ modulo $(K^\times)^p$. Thus (1) follows from Lemma 3.2. The end of the proof is a straightforward application of Th.1.1. □

3.3 Proof of Th.3.4

We are now ready to prove the last result stated in the introduction (Th.3.4 below). Recall some notation. For $v_o \in M_K$, define $\mathfrak{V}_{v_o}$ to be the restricted topological product of the K_v with respect to the local rings O_v, where v ranges over all places $v \in M_K$, $v \neq v_o$. That is, $\mathfrak{V}_{v_o} = \prod_{v \neq v_o} K_v$ as a set and a basis of neighborhoods of 0 is given by the sets $U(\varepsilon, S)$ defined as follows : ε is any positive real number, S is any finite subset of $M_K \backslash \{v_o\}$ such that $S \cup \{v_o\}$ contains all the archimedean places of K and $U(\varepsilon, S)$ is the subset of $\mathfrak{V}_{v_o}$ consisting of all elements $(\beta_v)_{v \neq v_o}$ such that

$$(2) \qquad \begin{cases} |\beta_v|_v < \epsilon, \text{ for all } v \in S \\ |\beta_v|_v \leq 1, \text{ for all } v \notin S, v \neq v_o \end{cases}$$

The field K is embedded in $\mathfrak{V}_{v_o}$ by the diagonal embedding. Th.3.4 is the following density property of Hilbert subsets.

THEOREM 3.4 — *Let K be a field with the product formula, of characteristic 0 or imperfect of characteristic $p > 0$. Let $v_o \in M_K$. Assume that 0 is not isolated in K for the induced topology of $\mathfrak{V}_{v_o}$. Then every Hilbert subset of K is dense in K for the same topology.*

Proof. Let $H = H_{P_1,\dots,P_n}$ be a Hilbert subset of K. For all $t \in K$, $H - t$ is still a Hilbert subset, namely the Hilbert subset associated with the polynomials $P_1(T+t,Y),\dots,P_n(T+t,Y)$. Thus we only need to prove that 0 is in the topological closure of any Hilbert subset $H = H_{P_1,\dots,P_n}$. Let $U(\varepsilon,S)$ be a basic neighborhood of 0 with $0 < \varepsilon \leq 1$ and $S \neq \emptyset$. From the assumption "0 is not isolated in K", the subset $U(\varepsilon/2,S) \cap K$ of K is infinite. Pick t_o in $U(\varepsilon/2,S) \cap K$ and $a \in K^\times$ such that conclusion of Th.3.3 holds. Now let S_a be the subset of M_K consisting of the places in S and the places v for which $|a|_v > 1$. Pick b in $U(1,S_a)$. Then from Th.3.3, for infinitely many integers $m > 0$, we have $t_o + ab^m \in U(\varepsilon,S) \cap H_{P_1,\dots,P_n}$. □

REFERENCES

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

[De1] P. Dèbes, G-fonctions et Théorème d'irréductibilité de Hilbert, *Acta Arithmetica*, **47, 4** (1986).

[De2] P. Dèbes, On the irreducibility of the polynomials $P(t^m,Y)$, *J. Number Theory*, 42, 2, (1992).

[De3] P. Dèbes, Hilbert subsets and s-integral points, *Manuscripta Mathematica*, **89**, (1996), 107–137.

[De4] P. Dèbes, On a problem of Dvornicich and Zannier, *Acta Arithmetica*, **73.4**, (1995), 379–387.

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

[Hu] A. Hurwitz, Über algebraische Gebilde mit eindeutigen Transformationen in sich, *Math. Ann.*, **41**, (1893).

[La1] S. Lang, *Algebra*, Addison-Wesley, (1965).

[La2] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, (1983).

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

[Sch] H.L. Schmid, Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahl-charakteristik, *J. Reine Angew. Math.*, **179**, (1938).

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

[Si] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, (1986).

Univ. Lille, Mathématiques, 59655 Villeneuve d'Ascq Cedex, FRANCE
e-mail : pde@ccr.jussieu.fr