On a Problem of Dvornicich and Zannier

Pierre Dèbes

Let k be a number field and $P(T,Y) \in k[T,Y]$ be an absolutely irreducible polynomial such that $\deg_Y P \geq 2$. For each integer $N > 0$ and each $t \in k$, define $D(t,N)$ to be the minimal degree over k of a field generated by N distinct elements $y(t+1), \ldots, y(t+N) \in \overline{k}$ respectively roots of $P(t+1,Y), \ldots, P(t+N,Y)$. Obviously $D(t,N) \leq (\deg_Y P)^N$. We wish to obtain lower bounds for $D(t,N)$. This problem was studied by Dvornicich and Zannier in the special case $k = \mathbb{Q}$. In [DvZa1] they prove the following asymptotic estimate for $D(N) = D(0,N)$,

$$D(N) \gg c^{\frac{N}{\mathrm{Log}(N)}}$$

where $c > 1$ depends only on $P(T,Y)$. The exponent $\frac{N}{\mathrm{Log}(N)}$ is the best possible. Indeed, they note that if $P(T,Y) = Y^d - T$ for some integer $d > 1$, then, for suitably large N,

$$D(t,N) \leq d^{\pi(N+t)} \leq d^{\frac{2(N+t)}{\mathrm{Log}(N)}} \tag{1}$$

Then they raise this question : when does $D(N)$ have exponential growth ? And prove an interesting special case of a conjecture due to Schinzel about this question (see also [DvZa2] for an another result towards Schinzel's conjecture). Here we study how $D(n,N)$ grows (instead of $D(0,N)$) : we do obtain an exponential lower bound $D(n,N) \gg c^N$, when the integer n is large compared to N.

Theorem 1 — *For each integer $N > 0$, there exists an explicitely computable constant $n_1 > 0$ depending on P, N and $[k : \mathbb{Q}]$ such that for each integer $n > n_1$, we have*

$$D(n,N) \geq \frac{2^N}{[k : \mathbb{Q}]\ (\deg_Y(P))^{\deg_Y(P)+3}} \tag{2}$$

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

The main term 2^N is essentially the best possible in (2). Indeed, for all but finitely many integers n, $D(n,N)$ is less than the "functional" analog $D(T,N)$, *i.e.*, the minimal degree over $k(T)$ of a field generated by N distinct elements $y(T+1),\dots,y(T+N) \in \overline{k(T)}$ respectively roots of $P(T+1,Y),\dots,P(T+N,Y)$. Now examples are given in [DVZa1] for which the functional degree $D(T,N)$ is $\ll 2^N$ (and so much smaller than the obvious upper bound $(\deg_Y P)^N$). On the other hand, the other term $[k:\mathbb{Q}]\ (\deg_Y P)^{\deg_Y P+3}$ in (2) can probably be improved but it is unclear what the right term should be. As for the constant n_1, inequality (1) shows that it has to depend on N in Th.1. More precisely, one needs $n \gg N\,\mathrm{Log}(N)$.

Th.1 will be established as a special case of a more general result which we call the Main Theorem in the sequel. Th.2 below, which can be viewed as a multiplicative version of Th.1, is another special case of the Main Theorem. The base field k can be any field with the product formula, possibly of characteristic $p>0$. For $u \in K$ and n,N positive integers, define $D_u^{\times}(n,N)$ to be the minimal degree over K of a field generated by N distinct elements $y(u^{n+1}),\dots,y(u^{n+N})$ respectively roots of $P(u^{n+1},Y),\dots,P(u^{n+N},Y)$.

THEOREM 2 — *Let $P(T,Y) \in k(T)[Y]$ be a polynomial, separable over $k(T)$, tamely ramified above $T=\infty$ and ramified over some point $T=b$ different from 0 and ∞. Assume further that $P(T^m,Y)$ is absolutely irreducible for all integers $m>0$. Let u be an element of k of height $h(u)>0$. Then for each integer $N>0$, there exists an explicitely computable constant m_1 depending on u, P and N such that, for each integer $m>m_1$, we have*

$$D_u^{\times}(m,N) \geq \frac{2^N}{s\ (\deg_Y(P))^{\deg_Y(P)+3}} \tag{3}$$

where s is an integer larger than the number of places v of k for which $|u|_v>1$.

The tame ramification hypothesis above $T=\infty$ is automatically satisfied in characteristic 0. This hypothesis implies in general that there exists an integer e such that $P(T,Y)$ is totally split in $\overline{K}(((1/T)^{1/\mathrm{e}}))$ (this is Puiseux's theorem in characteristic 0). Then from Prop.2.2 of [De2], the

assumption "$P(T^m, Y)$ absolutely irreducible for all integer $m > 0$" is actually equivalent to the absolute irreducibility of the single polynomial $P(T^e, Y)$. Th.2 may be false if this irreducibility assumption is removed. Take for example $P(T, Y) = Y^d - T$: we have $D_u^{\times}(m, N) \leq d^2$ for all $u \in k$ and all integers $m, N > 0$. On the other hand, the exact significance of the assumption "$P(T, Y)$ is ramified over some point $T = b$ different from 0 and ∞" is unclear. Classical arguments show that this condition is actually already contained in the irreducibility assumption if k is of characteristic 0. But this is not the case in characteristic $p > 0$. For example, the polynomial $P(T, Y) = Y^p - Y - (1/T)$ has only 0 as branch point and has the property that $P(T^m, Y)$ is absolutely irreducible for all integers $m > 0$.

§ 1 THE MAIN THEOREM

1.1 Preliminaries

Height. We adhere to the notation of [La]. 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 a point $x \in \overline{F}$) is then defined by

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

where K is any field containing 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.

s-integral points. A classical result in diophantine geometry is Siegel's finiteness theorem for S-integral points on algebraic curves. In [De3] we introduced the notion of *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". [De3] contains a general diophantine result for s-integral points. This result, which we recall in §2.1, will be the main ingredient of the proof of the Main Theorem stated below in §1.2.

Ramification. 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 $\overline{K}((T-t_o))$. When $t_o = \infty$, $T - t_o$ should be replaced by $1/T$. The finite set of all branch points of $P(T,Y)$ is denoted by $Br(P)$. The polynomial $P(T,Y)$ is said to be *tamely ramified* above $T = t_o$ if K is of characteristic 0 or of characteristic $p > 0$ with p dividing none of the degrees of the irreducible factors of $P(T,Y)$ in $\overline{K}((T-t_o))$. Ramification above $T = t_o$ is said to be *wild* otherwise.

1.2 Statement of the Main Theorem

Let k be a field with the product formula. Let $P(T,Y) \in k(T)[Y]$ be an irreducible polynomial such that $\deg_Y(P) \geq 2$. Assume that $P(T,Y)$ is separable over $k(T)$ and tamely ramified above $T = \infty$.

Let φ be an automorphism of $\mathbb{P}^1_k$ fixing ∞, *i.e.*, $\varphi(z) = uz + v$ with $u, v \in k$, $u \neq 0$. For each integer $j \in \mathbb{Z}$, denote the automorphism of $\mathbb{P}^1$ obtained by composing φ with itself j times by $\varphi^{[j]}$.

Assume that

(2) There exists at least one branch point $b \in Br(P)$ of $P(T,Y)$ such that

$$(*) \qquad \varphi^{[j_1]}(b) \neq \varphi^{[j_2]}(b) \text{ for all integers } j_1 \neq j_2$$

and that

(3) There exists an integer j_o such that for all integers $j \geq j_o$, the polynomials $P(\varphi^{[j]}(T^m), Y)$ are absolutely irreducible for all integers $m > 0$.

For each b such that (*) holds in (2), there can be only one integer j_b such that $\varphi^{[-j_b]}(b) = 0$. Pick an integer J larger than all integers j_b ($b \in Br(P)$) and larger than j_o. Fix an integer $N > 0$ and consider the family of polynomials

$$P(\varphi^{[J+1]}(T), Y) \dots, P(\varphi^{[J+N]}(T), Y)$$

For each $b \in k$, define $D_\varphi(b, N)$ to be the minimal degree over k of a field generated by N distinct elements $y_1, \dots, y_N \in \overline{k}$ respectively roots of $P(\varphi^{[J+1]}(b), Y) \dots, P(\varphi^{[J+N]}(b), Y)$.

MAIN THEOREM — *Let $s > 0$ be an integer. There exists a constant $h_2 > 0$ depending only on the polynomial $P(T, Y)$ and on the integer N with the following property. For each s-integral point $b \in k$ such that $h(b) > h_2 s^2$, we have*

$$D_\varphi(b, N) \geq \frac{2^N}{s(\deg_Y(P))^{\deg_Y(P)+3}} \tag{4}$$

1.3 Proof of Th.1

Consider the special case of the Main Theorem for which k is a number field and $\varphi(z) = z + 1$. Thus the polynomial $P(T, Y)$ is automatically separable and tamely ramified above $T = \infty$. Condition (2) is immediate since from Riemann-Hurwitz formula, the polynomial $P(T, Y)$ as at least two branch points and so at least one of them is different from ∞.

From Prop.2.2 of [De2], if a polynomial $Q(T, Y) \in k(T)[Y]$ is absolutely irreducible and has a root in $\overline{k}((T))$ then $Q(T^m, Y)$ is absolutely irreducible for all integers m. Pick an integer j_o larger than the largest root in $\mathbb{Z}$ of the discriminant of $P(T, Y)$ with respect to Y. Then for $j \geq j_o$, $P(T + j, Y)$ is unramified above $T = 0$, *i.e.*, is totally split in $\overline{k}((T))$. Conclude that $P(\varphi^{[j]}(T^m), Y) = P(T^m + j, Y)$ is absolutely irreducible for each integer $m > 0$. This proves condition (3).

Take $s = [k : \mathbb{Q}]$. Apply the Main Theorem to usual integers b, which are s-integral in k. Inequality (4) then corresponds to inequality (2) of Th.1. The constant n_1 can be taken to be $n_1 = \exp\left(h_2[k : \mathbb{Q}]^2\right) + J$. Using [De3], the constant n_1 can be explicitly computed : it is of order

$$\exp\left[(rD^N H)^{O(1)}\right]$$

where D is the degree of P, H the logarithmic height of P and $r = [k : \mathbb{Q}]$. □

Remark. The proof actually provides this more general conclusion. Given an integer $s > 0$ we have

$$D(b, N) \geq \frac{2^N}{s\ (\deg_Y(P))^{\deg_Y(P)+3}} \tag{5}$$

for all s-integral point $b \in k$ of height $h(b) > h_2 s^2$. Furthermore this holds more generally if k is a field with the product formula of characteristic 0. We assumed that k is a number field in Th.1 so to insure that there exists integers n with arbitrarily large height. Assuming that k has at least one archimedean place would have been sufficient. But from a result of Artin and Whaples, this implies that k is a number field [ArWh]. On the other hand, Th.1 is not true if integers are of bounded height in k. Indeed take $k = \mathbb{C}(X)$ where X is an indeterminate and $P(T,Y) \in \mathbb{C}[T,Y]$ an irreducible polynomial such that $\deg_Y(P) \geq 2$. Then $P(T,Y)$ is irreducible in $k[T,Y]$ as well. But for all $t \in \mathbb{C}$, the polynomial $P(t,Y)$ is totally split in $k[Y]$.

1.4 Proof of Th.2

Let u be an element of k such that $h(u) > 0$. Consider the special case of the Main Theorem for which $\varphi(z) = uz$. Condition (2) holds since it is assumed that $P(T,Y)$ has a branch point different from 0 and ∞. Condition (3) readily follows from the irreducibility assumption of Th.2. Take for s an integer larger than the number of places $v \in M_k$ such that $|u|_v > 1$. Then all powers u^m of u are s-integral points of k. Apply the Main Theorem to $b = u^m$. For all suitably large integers m, we will have $h(u^m) = mh(u) > h_2 s^2$. Inequality (4) in the Main Theorem then corresponds to inequality (3) of Th.2. □

§ 2 PROOF OF THE MAIN THEOREM

2.1 Diophantine result for s-integral points [De3]

Th.3 below is one of the main results of [De3] : it is a general diophantine result for s-integral points.

Let $\mathbf{P} = \{P_1(T,Y), \ldots, P_m(T,Y)\}$ be a family of (not necessarily distinct) polynomials in $K(T)[Y]$. Denote the union of the branch point sets $Br(P_i)$, $i = 1, \ldots, m$ by $Br(\mathbf{P})$. For each point $t \in \mathbb{P}^1 \setminus Br(\mathbf{P})$, the polynomial $P_i(T,Y)$ has $d = \deg_Y P_i$ distinct roots in $\overline{K}((T-t))$, $i = 1, \ldots, m$. For each index $i = 1, \ldots, m$, each root $y \in \overline{K}((T-t))$ of the polynomial $P_i(T,Y)$ corresponds to a point in the unramified fiber above $T = t$ of the finite morphism $C_i \to \mathbb{P}^1$ induced by T on the smooth projective model C_i of the curve $P(t,y) = 0$. The field of definition of this point then corresponds to the field generated by the coefficients of the power series

$y \in \overline{K}((T-t))$. We denote this field by $K(y(t))$. When $t = \infty$, $T-t$ should be replaced by $1/T$. For convenience, we generalize these definitions so to also include the case that $t = T$ is the generic point of $\mathbb{P}^1$: in this case, "$y \in \overline{K}((T-t))$" should be understood as "$y = y(T) \in \overline{K(T)}$" and the field $K(y(t))$ as $K(y(T))$.

For each point $t \in \mathbb{P}^1 \setminus Br(\mathbf{P})$, define then 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 $K(t), K(y_1(t)), \dots, K(y_m(t))$. For the generic point of $\mathbb{P}^1$, we use the subscript "gen" instead of "T".

Remark. In the special case 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 in particular 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 3 [De3 ;Th.1.4] — *Assume that the m 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*

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

Furthermore the constant h_1 is an absolute constant, i.e., remains the same if the polynomials in the family $\mathbf{P}$ are considered as polynomials with coefficients in any finite extension of K.

The constant h_1 is given explicitly in [De3] in the case that K is a number field. It is clear then that it is an absolute constant. This remains true in

general but the constants have not been computed explicitly. Th.3 uses a general result on algebraic functions due to Sprindzuk [Sp], Bombieri [Bo] and the author [De1]. For the general case, only the most general algebraic approach of Bombieri can be used. It is unclear whether this method is effective in general. Still the constants that appear in the proof of Bombieri have the property not to depend on the base field. Essentially these constants come from the use of Weil's decomposition theorem and a theorem of Néron based on the quadraticity of the canonical height on abelian varieties [La].

2.2 Proof of the Main Theorem

Retain the notation and hypotheses of §1.2. The polynomial $P(T,Y)$ is assumed to be separable over $k(T)$ and tamely ramified above $T=\infty$. Consequently there exists an integer $\mathrm{e}>0$ such that $P(T,Y)$ is totally split in $\overline{k}(((1/T)^{1/\mathrm{e}}))$ and such that e is relatively prime to the characteristic p of k if $p>0$.

Let K be a finite extension of k. Consider the family of polynomials

$$\mathbf{P}_N=\{P(\varphi^{[J+1]}(T^{\mathrm{e}}),Y)\ldots,P(\varphi^{[J+N]}(T^{\mathrm{e}}),Y)\},$$

regarded as polynomials with coefficients in K. We first generalize an argument of [DvZa1] to show that

Lemma 1 — *Under the conditions above we have*

$$D_{\mathrm{gen}}(\mathbf{P}_N)\geq 2^N \tag{3}$$

Proof. For each integer $i\geq 0$, let B_i be the branch point set of $P(\varphi^{[i]}(T^{\mathrm{e}}),Y)$. We will show that if $i>J$ then

$$B_i\not\subset\bigcup_{j=i+1}^{J+N}B_j \tag{4}$$

Since φ is an isomorphism and $z\to z^{\mathrm{e}}$ is ramified only above 0 and ∞, we have

$$(B_i\setminus\{0,\infty\})^e=\varphi^{[-i]}(Br(P))\setminus\{0,\infty\}$$

Thus so to establish (4) it suffices to prove that for all $i > J$,

$$\varphi^{[-i]}(Br(P)) \setminus \{0, \infty\} \not\subset \bigcup_{j=i+1}^{J+N} \varphi^{[-j]}(Br(P)) \setminus \{0, \infty\} \tag{5}$$

Assume the contrary holds for some integer $i > J$. Select an element $b = b_1 \in Br(P)$ satisfying (*) in condition (2) of §1. Then, from the definition of J, $\varphi^{[-i]}(b_1) \neq 0$. Furthermore, it follows from (*) and $\varphi(\infty) = \infty$ that $\varphi^{[-i]}(b_1) \neq \infty$. Thus we obtain

$$\varphi^{[-i]}(b_1) = \varphi^{[-j_1]}(b_2), \text{ for some } b_2 \in Br(P) \text{ and } j_1 > i$$

The same argument can be repeated to the element b_2 which also satisfies (*). By induction we construct a sequence $(b_n)_{n>0}$ of elements of $Br(P)$ satisfying (*) and such that

$$\varphi^{[-i]}(b_n) = \varphi^{[-j_n]}(b_{n+1}), \text{ for some integer } j_n > i \tag{6}$$

Since $Br(P)$ is finite, we will have $b_p = b_{p+q}$ for some integers p, $q \neq 0$. The equations (6) corresponding to $p, \ldots, p+q-1$ yield

$$\varphi^{[-qi]}(b_p) = \varphi^{[-(j_p + \cdots + j_{p+q-1})]}(b_p)$$

Conclude from (*) (applied to $b = b_p$) that

$$qi = j_p + \cdots + j_{p+q-1}$$

which contradicts $j_l > i$, $l = 1, \ldots, p+q$ and completes the proof of (4).

For each integer $j \geq J$, if y_j is any root of $P(\varphi^{[j]}(T^e), Y)$, then the branch point set of the extension $\overline{k}(T, y_j)$ is the set B_i (because $P(\varphi^{[j]}(T^e), Y)$ is absolutely irreducible). Conclude from (4) that the splitting field of $P(\varphi^{[i]}(T^e), Y)$ over $K(T)$ is not contained in any of the function fields $K(T, y_{i+1}, \ldots, y_{J+N})$ where y_j is any root of the polynomial $P(\varphi^{[j]}(T^e), Y)$, $j = i+1, \ldots, J+N$. (3) follows by induction. □

Proof of the Main Theorem. Let h_1 be the constant of Th.1.4 associated with the family of polynomials $\mathbf{P}_N$. Recall that h_1 is an *absolute* constant,

i.e., is the same if the polynomials are regarded as polynomials with coefficients in k or in any finite extension K of k. Then take $h_2 = h_1.(\deg_Y(P))^3$. Let $s > 0$ be an integer and b be an s-integral point of k of height $h(b) > h_2 s^2$. Let t be an eth root of b in $\overline{k}$. Then set $K = k(t)$.

The polynomials in the family $\mathbf{P}_N$ are separable over $\overline{k}(T)$. Observe next that these polynomials are unramified above $T = \infty$. Indeed, by definition of e, the polynomial $P(T^{\mathrm{e}}, Y)$ is totally split in $\overline{k}(((1/T))$. Then, since $\varphi(\infty) = \infty$, for each root $y(u) \in \overline{k}(((1/u)))$ of $P(u^{\mathrm{e}}, y(u)) = 0$ and for each $j \in \mathbb{Z}$, the power series

$$\frac{1}{\varphi^{[j]}(T^{\mathrm{e}})^{1/e}} = \frac{1}{T}\ \frac{1}{\left(a^j + \frac{b_j}{T^{\mathrm{e}}}\right)^{1/\mathrm{e}}} \in \overline{k}(((1/T))) \tag{7}$$

where $\varphi^{[j]}(z) = a^j z + b_j$, $(a \neq 0)$, can be substituted for $1/u$ in $y(u)$ to yield a power series $y_j(T) \in \overline{k}(((1/T)))$ solution of $P(\varphi^{[j]}(T^{\mathrm{e}}), y_j(T)) = 0$. Conclude that the polynomial $P(\varphi^{[j]}(T^{\mathrm{e}}), Y)$ is totally split in $\overline{k}(((1/T)))$, *i.e.*, is unramified above $T = \infty$ for each integer $j \in \mathbb{Z}$.

Since each place $v \in M_k$ has at most $[K : k] \leq \mathrm{e}$ extensions to M_K, the element t is an $s\mathrm{e}$-integral point of K. Furthermore it follows from "$\mathrm{e} \leq \deg_Y(P)$" that

$$h(t) = \frac{h(b)}{\mathrm{e}} > \frac{h_2 s^2}{\mathrm{e}} > h_1 s^2 (\mathrm{e})^2 \geq h_1 (s\mathrm{e})^2$$

From Th.3, which we apply to the field K, the family of polynomials $\mathbf{P}_N$ and the $s\mathrm{e}$-integral point $t \in K$, we obtain

$$(s\mathrm{e})\ D^+_\infty(\mathbf{P}_N)\ D_t(\mathbf{P}_N) \geq D_{\mathrm{gen}}(\mathbf{P}_N)$$

We explained above how to obtain the roots in $\overline{k}((((1/T))))$ of the polynomials $P(\varphi^{[j]}(T^{\mathrm{e}}, Y)$, $(j \in \mathbb{Z})$, from the roots of $P(T^{\mathrm{e}}, Y)$. This shows that

$$D^+_\infty(\mathbf{P}_N) \leq \mathrm{e}^2\ \left[D^+_\infty(P(T^{\mathrm{e}}, Y))\right]^{\deg_Y(P)}$$

(The extra term e^2 comes from the terms $a^{1/e}$ that possibly occur in the power series expansion of $1/\varphi^{[j]}(T^{\mathrm{e}})^{1/e}$, $(j \in \mathbb{Z})$ in (7) above). Hence we obtain

$$D^+_\infty(\mathbf{P}_N) \leq \mathrm{e}^2\ (\deg_Y(P))^{\deg_Y(P)}$$

which, with Lemma 1, yields

$$D_t(\mathbf{P}_N) \geq \frac{2^N}{s\mathrm{e}^3(\deg_Y(P))^{\deg_Y(P)}}$$

Note that the parameter $D_\varphi(b,N)$ of the Main Theorem coincides with the parameter $D_t(\mathbf{P}_N)$, except that the former is defined with k as base field. But this parameter $D_\varphi(b,N)$ can only get smaller when one extends the scalars. Therefore

$$D_\varphi(b,N) \geq D_t(\mathbf{P}_N) \geq \frac{2^N}{s\mathrm{e}^3(\deg_Y(P))^{\deg_Y(P)}} \qquad \square$$

REFERENCES

[ArWh] E. Artin and G. Whaples, Axiomatic characterisation of fields by the product formula, *Bull. Amer. Math. Soc.*, **51**, No.7, (1945).

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

[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, preprint (1994).

[DvZa1] R. Dvornicich and U. Zannier, Fields containing values of algebraic functions, preprint, (1992).

[DvZa2] R. Dvornicich and U. Zannier, Fields containing values of algebraic functions (II), preprint, (1994).

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

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

Univ. Lille 1, U.F.R. Math., 59655 VILLENEUVE D'ASCQ Cedex, FRANCE.
E-mail : pde@ccr.jussieu.fr