THEOREM 1. $|\{P_r\colon p+h = P_r,\ p \leqslant x\}| \ll c_h x \log^{-2} x (\log\log x)^{r-1},\ r \geqslant 1.$

Proof. Since

$$|\{P_r\colon p+h = P_r,\ p \leqslant x\}| = \sum_{i=1}^{r} |\{P_r\colon p+h = P_r,\ p \leqslant x,\ \nu(P_r) = i\}|,$$

by Proposition 2, Theorem 1 follows.

**5. More precise results for the lower bounds.**

THEOREM 2. *Let $\delta$ be a fixed number with $0 < \delta < 1$. Then for any $r \geqslant 3$,*

$$|\{p\colon p \leqslant x,\ p+h = p_1 \cdot \ldots \cdot p_{r-1} \text{ or } p_1 \cdot \ldots \cdot p_r,\ p_r > p_{r-1} > \ldots$$
$$\ldots > p_1 \geqslant \exp(\log^\delta x)\}|$$
$$> 0.965\left((1-\delta)^{r-2}/(r-2)!\right) c_h x \log^{-2} x (\log\log x)^{r-2}.$$

Proof. From Proposition 2 we have

$$(32)\qquad |\{p\colon p \leqslant x,\ p+h = p_1 \cdot \ldots \cdot p_{r-2}\}| \ll c_h x \log^{-2} x (\log\log x)^{r-3}, \quad r \geqslant 3.$$

From Proposition 1 and (32), Theorem 2 follows.

COROLLARY 3. *For all $r \geqslant 3$,*

$$|\{p\colon p \leqslant x,\ p+h = p_1 \cdot \ldots \cdot p_{r-1} \text{ or } p_1 \cdot \ldots \cdot p_r,\ p_r > p_{r-1} > \ldots > p_1\}|$$
$$\geqslant 0.965\left((1-\delta)^{r-2}/(r-2)!\right) \geqslant 0.965/(r-2)!.$$

Proof. In Theorem 2 let $\delta \to 0^+$.

**References**


[1] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. 156 (1986), 203–251.

[2] E. Fouvry and H. Iwaniec, *Primes in arithmetic progressions*, Acta Arith. 42 (1983), 197–218.

[3] E. Fouvry and F. Grupp, *On the switching principle in sieve theory*, J. Reine Angew. Math. 370 (1986), 101–126.

[4] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, 1974.

[5] H. Iwaniec, *Rosser's sieve*, in: *Recent Progress in Analytic Number Theory*, Vol. 1, 203–230, Academic Press, 1981.

[6] Pan Cheng-dong, *A new mean value theorem and its applications*, ibid. 275–287.



NANJING INSTITUTE OF POST AND TELECOMMUNICATION
210003 Nanjing
Nanjing, Jiangsu
P. R. China


*Received on 17.2.1989* (1907)


ACTA ARITHMETICA
LVI (1990)


# On an estimate for the orders of zeros of Mahler type functions


by

KUMIKO NISHIOKA (Nara)


Nesterenko [6] gives a very good measure of the algebraic independence for the values of functions of Mahler type.

NESTERENKO'S THEOREM [6]. *Let $f_1(z), \ldots, f_m(z)$ be power series in $z$ with coefficients in an algebraic number field $K$, which converge in some neighborhood $U$ of the point $z = 0$, which satisfy the equalities*

$$f_i(z^d) = a_i(z) f_i(z) + b_i(z), \quad a_i(z),\ b_i(z) \in K(z), \quad i = 1, \ldots, m,$$

*where $d$ is an integer, $d \geqslant 2$, and which are algebraically independent over $\mathbf{C}(z)$. Suppose that $\alpha$ is an algebraic number, $\alpha \in U$, $0 < |\alpha| < 1$, and the numbers $\alpha, \alpha^d, \alpha^{d^2}, \ldots$ are distinct from the poles of the functions $a_i(z)$ and $b_i(z)$. Then there exists a function $\varphi(s)$ such that, for any $H$ and $s \geqslant 1$ with $H \geqslant \varphi(s)$ and for any polynomial $R \in \mathbf{Z}[x_1, \ldots, x_m]$ whose degree does not exceed $s$ and whose coefficients are not greater than $H$ in absolute value, the following inequality holds:*

$$(0)\qquad |R(f_1(\alpha), \ldots, f_m(\alpha))| > H^{-\gamma s^m},$$

*where $\gamma$ is a positive constant which depends only on $\alpha$ and the functions $f_1, \ldots, f_m$.*

The above function $\varphi(s)$ is ineffective in the parameter $s$. In order to make it effective, we prove an estimate for the orders of zeros of such functions. By using our estimate, Becker [1] shows that the right side of the estimate (0) can be replaced by $\exp(-\gamma s^m (\log H + s^{2m+2}))$ for any $H$ and $s \geqslant 1$. (See also Becker and Nishioka [2].)

For a formal power series $f(z)$, we denote by $\operatorname{ord} f(z)$ the order of zeros of $f(z)$ at $z = 0$.

THEOREM. *Let $f_1(z), \ldots, f_m(z) \in C[[z]]$ be formal power series with coefficients in a field $C$ of characteristic 0 and satisfy*

$$f_i(z^d) = \frac{A_i(z, f_1(z), \ldots, f_m(z))}{A_0(z, f_1(z), \ldots, f_m(z))} \quad (1 \leqslant i \leqslant m),$$

*where $d \geqslant 2$ is a rational integer and $A_i(z, x_1, \ldots, x_m) \in C[z, x_1, \ldots, x_m]$ $(0 \leqslant i \leqslant m)$ are polynomials with $\deg_z A_i \leqslant s$ and $\operatorname{tot.deg}_x A_i \leqslant t$. Suppose that*

*$t^m < d$ and $Q(z, x_1, \ldots, x_m) \in C[z, x_1, \ldots, x_m]$ is a nonzero polynomial with* $\deg_z Q \leqslant M$, $\mathrm{tot.deg}_x Q \leqslant N$ *where $M \geqslant N \geqslant 1$. If $Q(z, f_1(z), \ldots, f_m(z)) \neq 0$, then*

$$\mathrm{ord}\, Q(z, f_1(z), \ldots, f_m(z)) \leqslant c_0 M N^m N^{m^2 \log t/(\log d - m \log t)},$$

*where*

$$c_0 = \max\{c_1/(d-t),\ 8m^2(8d)^m(1+s/(d-t))\, t^m (12m(8d)^{m-1})^{m \log t/(\log d - m\log t)}\},$$

$$c_1 = \mathrm{ord}\, A_0(z, f_1(z), \ldots, f_m(z)).$$

The theorem is proved by using the results analogous to Nesterenko's [6] over the polynomial ring $C[z]$.

This paper was written during a stay at the University of Cologne supported by the Alexander von Humboldt Foundation. The author is grateful to P. Bundschuh for giving her such an opportunity.

**1. Preliminaries.** Let $C$ be a field of characteristic 0. For a polynomial $P$ of $z$, by $B(P)$ we denote the degree in $z$. By $v$ we denote the valuation ord of the field $C((z))$. We can extend $v$ uniquely to the algebraic closure $\overline{C((z))}$ of $C((z))$. We extend $v$ to the ring of polynomials with coefficients in $C((z))$ which is defined for a polynomial $P$, the minimum of the values $v(a)$ of all coefficients $a$ of $P$. Then we have

$$v(P_1 \ldots P_n) = v(P_1) \ldots v(P_n). \tag{1}$$

Let $R = C[z]$. Suppose that $r$ is an integer, $1 \leqslant r \leqslant m$, and $u_{ij}$, $1 \leqslant i \leqslant r$, $0 \leqslant j \leqslant m$, are variables which are algebraically independent over the field $C(z)$. For an arbitrary unmixed homogeneous ideal $I$ of $R[x_0, \ldots, x_m] = R[X]$ with $r = m+1-h(I)$, we can define a nonzero principal ideal $\bar{I}(r)$ of $R[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r]$. (See [3], Proposition 2.) Let $F$ be the generator of the principal ideal $\bar{I}(r)$. Then $F$ is homogeneous with respect to each set of variables $\boldsymbol{u}_j = (u_{j0}, \ldots, u_{jm})$ and $F$ has the same degree in each set of variables $\boldsymbol{u}_j$. We let $B(I) = B(F)$ and $N(I) = \deg_{\boldsymbol{u}_1} F$. Suppose that $\boldsymbol{\omega} = (\omega_0, \ldots, \omega_m) \in \overline{C((z))}^{m+1}$ is a nonzero vector, and $S^{(i)} = \|s_{jk}^{(i)}\|$ $(j, k = 0, 1, \ldots, m;\ i = 1, \ldots, r)$ are skew-symmetric matrices whose entries are not connected by any algebraic relation over $R[X, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_r]$ except for the skew symmetry $s_{jk}^{(i)} + s_{kj}^{(i)} = 0$. For any polynomial $E \in R[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r]$ let $\varkappa(E)$ denote the polynomial in the variables $s_{jk}^{(i)}$, $j < k$, $i = 1, \ldots, r$, which is obtained by substituting the vectors $S^{(i)}\boldsymbol{\omega}$, $i = 1, \ldots, r$, in place of the variables $\boldsymbol{u}_i$ in $E$. If $F$ is the generator of the ideal $\bar{I}(r)$, then we define

$$v(I(\boldsymbol{\omega})) = v(\varkappa(F)) - rN(I)\, v(\boldsymbol{\omega}),$$

where $v(\boldsymbol{\omega}) = \min_{0 \leqslant i \leqslant m} v(\omega_i)$.



We have the following propositions and lemmas obtained analogously to [6], §2. Hence we omit the proofs.

PROPOSITION 1. *Let $I = (P)$ be the principal ideal of $R[X]$ which is generated by the nonzero homogeneous polynomial $P$. Then*

$$N(I) = \deg P, \qquad B(I) \leqslant B(P),$$

$$v(I(\boldsymbol{\omega})) \geqslant v(P(\boldsymbol{\omega})) - \deg P\, v(\boldsymbol{\omega}).$$

PROPOSITION 2. *Suppose that $I$ is a nonzero unmixed homogeneous ideal in $R[X]$, $h(I) \leqslant m$; $I = I_1 \cap \ldots \cap I_s \cap \ldots \cap I_t$ is its irreducible primary decomposition in which for $l \leqslant s$ we have $I_l \cap R = (0)$, $I_{s+1} \cap \ldots \cap I_t \cap R = (b)$; $b \in R - \{0\}$*; for $l \leqslant s$ *let $\mathfrak{p}_l = \sqrt{I_l}$ and let $k_l$ be the exponent of the ideal $I_l$. Then*

1) $\sum_{l=1}^{s} k_l N(\mathfrak{p}_l) = N(I)$;

2) $B(b) + \sum_{l=1}^{s} k_l B(\mathfrak{p}_l) = B(I)$;

3) $v(b) + \sum_{l=1}^{s} k_l v(\mathfrak{p}_l(\boldsymbol{\omega})) = v(I(\boldsymbol{\omega}))$;

4) $0 \leqslant v(b) \leqslant B(b) \leqslant B(I)$.

When $s = 0$ the terms corresponding to the ideal $\mathfrak{p}_l$ do not occur in 1)–3); and if $s = t$ then the terms $B(b)$ and $v(b)$ are missing.

For any two nonzero vectors $\boldsymbol{\omega} = (\omega_0, \ldots, \omega_m)$, $\boldsymbol{\theta} = (\theta_0, \ldots, \theta_m) \in \overline{C((z))}^{m+1}$, we define $V(\boldsymbol{\omega}, \boldsymbol{\theta})$ by

$$V(\boldsymbol{\omega}, \boldsymbol{\theta}) = -v(\boldsymbol{\omega}) - v(\boldsymbol{\theta}) + \min_{0 \leqslant i, j \leqslant m} v(\omega_i \theta_j - \omega_j \theta_i).$$

LEMMA 1. *Let $P$ and $Q$ be homogeneous polynomials of degree $\nu$ in $R[X]$. Then for any nonzero vectors $\boldsymbol{\omega}$, $\boldsymbol{\theta} \in \overline{C((z))}^{m+1}$,*

$$v(P(\boldsymbol{\omega})Q(\boldsymbol{\theta}) - P(\boldsymbol{\theta})Q(\boldsymbol{\omega})) \geqslant V(\boldsymbol{\omega}, \boldsymbol{\theta}) + v(P) + v(Q) + \nu v(\boldsymbol{\omega}) + \nu v(\boldsymbol{\theta}).$$

Suppose that $\mathfrak{p}$ is a nonzero homogeneous prime ideal of $R[X]$, $r = m+1-h(\mathfrak{p}) \geqslant 1$, $\mathfrak{p} \cap R = (0)$ and $x_0 \notin \mathfrak{p}$. Let the principal ideal $\bar{\mathfrak{p}}(r)$ be generated by the polynomial $F$. Lemma 2 of [4] describes a certain algebraic extension $K_1$ of the field $C(z)(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1})$ and elements $\alpha_i^{(j)} \in K_1$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant g = N(\mathfrak{p})$ such that the points $(1: \alpha_1^{(j)}: \ldots : \alpha_m^{(j)})$, $1 \leqslant j \leqslant g$, are common zeros of the ideal $\mathfrak{p}$ and satisfy

$$F = a \prod_{j=1}^{N(\mathfrak{p})} (u_{r0} + \alpha_1^{(j)} u_{r1} + \ldots + \alpha_m^{(j)} u_{rm}),$$

where $a \in R[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}]$ and $\mathrm{tot.deg}_{\boldsymbol{u}_1} a = N(\mathfrak{p})$ for $r \geq 2$. Let $Q$ be a homogeneous polynomial from $R[X]$ and define

$$G = a^{\deg Q} \prod_{j=1}^{N(\mathfrak{p})} Q(1, \alpha_1^{(j)}, \ldots, \alpha_m^{(j)}).$$

Then by Lemma 4 in [4] we have $G \in R[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}]$ and the inequalities:

(2) $$B(G) \leq B(\mathfrak{p}) \deg Q + N(\mathfrak{p}) B(Q);$$

(3) $$v(G) \geq v(F) \deg Q + N(\mathfrak{p}) v(Q).$$

LEMMA 2. *Suppose that $\mathfrak{p}$ is a nonzero homogeneous prime ideal of $R[X]$, $r = m+1-h(\mathfrak{p}) \geq 1$, $\mathfrak{p} \cap R = (0)$, $x_0 \notin \mathfrak{p}$ and $\varkappa(a) \neq 0$. Then there exists a homomorphism*

$$\tau\colon R[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \alpha_1^{(1)}, \ldots, \alpha_m^{(g)}, a^{-1}] \to \overline{C((z))}$$

*such that for $\beta_i^{(j)} = \tau(\alpha_i^{(j)}) \in \overline{C((z))}$ the vectors $\boldsymbol{\beta}_j = (1, \beta_1^{(j)}, \ldots, \beta_m^{(j)})$, $1 \leq j \leq N(\mathfrak{p})$, are zeros of the ideal $\mathfrak{p}$ and*

1) $v(\tau(a)) + \sum_{j=1}^{N(\mathfrak{p})} v(\boldsymbol{\beta}_j) \geq v(F) + (r-1) N(\mathfrak{p}) v(\boldsymbol{\omega})$;

2) $v(\tau(a)) + \sum_{j=1}^{N(\mathfrak{p})} (V(\boldsymbol{\omega}, \boldsymbol{\beta}_j) + v(\boldsymbol{\beta}_j)) \geq v(\mathfrak{p}(\boldsymbol{\omega})) + (r-1) N(\mathfrak{p}) v(\boldsymbol{\omega})$;

3) *If $E \in R[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}]$, then the homomorphism $\tau$ can be chosen such that $v(\varkappa(E)) = v(\tau(E))$.*

LEMMA 3. *Suppose that $\boldsymbol{\omega} \in \overline{C((z))}^{m+1}$, $\boldsymbol{\omega} \neq 0$, $\mathfrak{p}$ is a nonzero homogeneous prime ideal of $R[X]$, $\mathfrak{p} \cap R = (0)$, $h(\mathfrak{p}) \leq m$; and $Q$ is a homogeneous polynomial in $R[X]$, $Q \notin \mathfrak{p}$. If $r = m+1-h(\mathfrak{p}) \geq 2$, then there exists an unmixed homogeneous ideal $I \subset R[X]$ whose zeros coincide with the zeros of the ideal $(\mathfrak{p}, Q)$, for which $h(I) = m-r+2$, and such that*

1) $N(I) \leq N(\mathfrak{p}) \deg Q$;

2) $B(I) \leq B(\mathfrak{p}) \deg Q + N(\mathfrak{p}) B(Q)$;

3) $v(I(\boldsymbol{\omega})) \geq \min\{v(\mathfrak{p}(\boldsymbol{\omega})),\ v(Q(\boldsymbol{\omega})) - v(\boldsymbol{\omega}) \deg Q\} - B(\mathfrak{p}) \deg Q - N(\mathfrak{p}) B(Q)$.

*If $h(\mathfrak{p}) = m$, then the right side of the inequality in 3) is not positive.*

LEMMA 4. *Suppose that the conditions of Lemma 3 are fulfilled, and $\mu$ is a real number $0 < \mu \leq 1$ such that the following inequality holds for every zero $\boldsymbol{\beta}$ of the ideal $\mathfrak{p}$:*

$$\mu V(\boldsymbol{\omega}, \boldsymbol{\beta}) \leq v(Q(\boldsymbol{\omega})) - v(\boldsymbol{\omega}) \deg Q.$$

*Then the ideal $I$ in Lemma 3 satisfies the inequality*

$$v(I(\boldsymbol{\omega})) \geq \mu \cdot v(\mathfrak{p}(\boldsymbol{\omega})) - B(\mathfrak{p}) \deg Q - N(\mathfrak{p}) B(Q).$$

*When $r = 1$ the right side of this inequality is not positive.*

LEMMA 5. *Suppose that $Q \in R[x_0, \ldots, x_m]$, $Q \not\equiv 0$, is a homogeneous polynomial; $\mathfrak{p} \subset R[x_0, \ldots, x_m]$ is a nonzero homogeneous prime ideal, $\mathfrak{p} \cap R = (0)$, $r = m+1-h(\mathfrak{p}) \geq 1$; $\boldsymbol{\omega} = (\omega_0, \ldots, \omega_m) \in \overline{C((z))}^{m+1}$, $\boldsymbol{\omega} \neq 0$,*

$$v(\mathfrak{p}(\boldsymbol{\omega})) \geq X, \quad \infty > X > 0, \quad v(Q(\boldsymbol{\omega})) - v(\boldsymbol{\omega}) \deg Q > 0,$$

*and finally, the following equality holds for some $\sigma > 1$:*

$$\min(X, \delta) = \sigma\big(v(Q(\boldsymbol{\omega})) - v(\boldsymbol{\omega}) \deg Q\big),$$

*where $\delta = \sup V(\boldsymbol{\omega}, \boldsymbol{\beta})$, and the supremum is taken over all zeros $\boldsymbol{\beta} \in \overline{C((z))}^{m+1}$, $\beta \neq 0$, of the ideal $\mathfrak{p}$. Then for $r \geq 2$ there exists an unmixed homogeneous ideal $I \subset R[x_0, \ldots, x_m]$, $h(I) = m-r+2$, for which inequalities 1) and 2) in Lemma 3 hold, and in addition,*

$$v(I(\boldsymbol{\omega})) \geq X/\sigma - B(\mathfrak{p}) \deg Q - N(\mathfrak{p}) B(Q).$$

*In the case $r = 1$, the right side of the last inequality is not positive.*

LEMMA 6. *Suppose that $I \subset R[x_0, \ldots, x_m]$ is a nonzero unmixed homogeneous ideal. $I \cap R = (0)$, and $r = m+1-h(I) \geq 1$. For every nonzero vector $\boldsymbol{\omega} \in \overline{C((z))}^{m+1}$, we have*

$$N(I)\,\delta \geq v(I(\boldsymbol{\omega}))/r - 2B(I),$$

*where $\delta = \sup V(\boldsymbol{\omega}, \boldsymbol{\beta})$, and the supremum is taken over all zeros $\boldsymbol{\beta} \in \overline{C((z))}^{m+1}$, $\boldsymbol{\beta} \neq 0$, of the ideal $I$.*

**2. Proof of the theorem.** Suppose that a polynomial $Q$ satisfies the hypotheses of the theorem and

$$\operatorname{ord} Q(z, f_1(z), \ldots, f_m(z)) = v\big(Q(z, f_1(z), \ldots, f_m(z))\big) = \lambda M N^m,$$

where $\lambda > c_0 N^{m^2 \log t/(\log d - m \log t)}$. Let $Q_0(z, x_0, \ldots, x_m) \in C[z, x_0, \ldots, x_m] = R[X]$ be the homogeneous polynomial of degree $N$ in $x_0, \ldots, x_m$ which satisfies $Q_0(z, 1, x_1, \ldots, x_m) = Q(z, x_1, \ldots, x_m)$. We define a sequence of polynomials $Q_l \in R[X]$ for $l \geq 1$,

$$Q_l(z, x_0, \ldots, x_m) = Q_{l-1}(z^d, \bar{A}_0(z, x_0, \ldots, x_m), \ldots, \bar{A}_m(z, x_0, \ldots, x_m))$$

where $\bar{A}_i(z, x_0, \ldots, x_m)$ is the homogeneous polynomial of degree $t$ in $x_0, \ldots, x_m$ which satisfies $\bar{A}_i(z, 1, x_1, \ldots, x_m) = A_i(z, x_1, \ldots, x_m)$. Then $Q_l$ is a homogeneous polynomial of degree $t^l N$ in $x_0, \ldots, x_m$ and

$$Q_l(z, 1, f_1(z), \ldots, f_m(z))$$
$$= Q(z^{d^l}, f_1(z^{d^l}), \ldots, f_m(z^{d^l})) \prod_{j=0}^{l-1} \big(A_0(z^{d^j}, f_1(z^{d^j}), \ldots, f_m(z^{d^j}))^{t^{l-j-1}}\big)^N.$$

Hence we have

$$v\big(Q_l(z, 1, f_1(z), \ldots, f_m(z))\big) = \lambda d^l M N^m + c_1 N (d^l - t^l)/(d-t).$$

Since $\lambda > c_1/(d-t)$,

$$\lambda d^l MN^m \leqslant v\big(Q_l(z, 1, f_1(z), \ldots, f_m(z))\big) \leqslant 2\lambda d^l MN^m. \tag{4}$$

By induction,

$$B(Q_l) \leqslant d^l M + sN(d^l - t^l)/(d-t) \leqslant \mu d^l M, \tag{5}$$

where $\mu = 1 + s/(d-t)$. Put

$$l_1 = [\log(12m(8d)^{m-1}N^m)/(\log d - m\log t)] + 1. \tag{6}$$

We assert that for $n = 1, \ldots, m$, there exists a homogeneous prime ideal $\mathfrak{p}^{(n)} \subset R[X]$, $\mathfrak{p}^{(n)} \cap R = (0)$, $h(\mathfrak{p}) = n$ which satisfies the following inequalities:

$$N(\mathfrak{p}^{(n)}) \leqslant t^{l_1} N \cdot N(\mathfrak{p}^{(n-1)}) \leqslant t^{nl_1} N^n \qquad (N(\mathfrak{p}^{(0)}) = 1); \tag{7}$$

$$\begin{aligned} B(\mathfrak{p}^{(n)}) &\leqslant t^{l_1} N \cdot B(\mathfrak{p}^{(n-1)}) + \mu d^{l_1} M \cdot N(\mathfrak{p}^{(n-1)}) \\ &\leqslant n\mu t^{(n-1)l_1} d^{l_1} MN^{n-1} \qquad (B(\mathfrak{p}^{(0)}) = 0); \end{aligned} \tag{8}$$

$$\begin{aligned} v(\mathfrak{p}^{(n)}(\omega)) \geqslant{} & (\lambda/4(8d)^{n-1}) d^{l_1} t^{-nl_1} N^{m-n} M \cdot N(\mathfrak{p}^{(n)}) \\ & + (\lambda/4(8d)^{n-1} n\mu) t^{-(n-1)l_1} N^{m-n+1} \cdot B(\mathfrak{p}^{(n)}). \end{aligned} \tag{9}$$

We note that

$$\lambda > 8m^2(8d)^m \mu t^m (12m(8d)^{m-1}N^m)^{m\log t/(\log d - m\log t)} \geqslant 8m^2(8d)^m \mu t^{ml_1}. \tag{10}$$

Put $\omega = (1, f_1(z), \ldots, f_m(z))$. Then $v(\omega) = 0$. Let $I^{(1)} \subset R[X]$ be the principal ideal generated by $Q_{l_1}$. Then $I^{(1)} \cap R = (0)$, $h(I^{(1)}) = 1$, and by Proposition 1, we have

$$N(I^{(1)}) = \deg Q_{l_1} = t^{l_1} N,$$

$$B(I^{(1)}) \leqslant B(Q_{l_1}) \leqslant \mu d^{l_1} M,$$

$$v(I^{(1)}(\omega)) \geqslant v(Q_{l_1}(\omega)) \geqslant \lambda d^{l_1} MN^m.$$

We suppose that there is no homogeneous ideal $\mathfrak{p}$ which satisfies the assertion for $n = 1$. We consider the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ which are defined in Proposition 2 for the ideal $I^{(1)}$. Thus for all $j$, $1 \leqslant j \leqslant s$,

$$v(\mathfrak{p}_j(\omega)) < (\lambda/4) d^{l_1} t^{-l_1} N^{m-1} M \cdot N(\mathfrak{p}_j) + (\lambda/4\mu) N^m \cdot B(\mathfrak{p}_j).$$

By the equalities in Proposition 2,

$$\begin{aligned} v(I^{(1)}(\omega)) &= v(b) + \sum_{j=1}^{s} k_j v(\mathfrak{p}_j(\omega)) \\ &< v(b) + (\lambda/4) d^{l_1} t^{-l_1} N^{m-1} M \cdot N(I^{(1)}) + (\lambda/4\mu) N^m (B(I^{(1)}) - B(b)) \\ &\leqslant (\lambda/4) d^{l_1} t^{-l_1} N^{m-1} M \cdot N(I^{(1)}) + (\lambda/4\mu) N^m \cdot B(I^{(1)}) \\ &\leqslant (\lambda/2) d^{l_1} MN^m. \end{aligned}$$



This is a contradiction. Thus the assertion is true for $n = 1$. Assume that the assertion is true for $n-1$, $2 \leqslant n \leqslant m$. Put

$$\begin{aligned} X = {} & (\lambda/4(8d)^{n-2}) d^{l_1} t^{-(n-1)l_1} N^{m-n+1} M \cdot N(\mathfrak{p}^{(n-1)}) \\ & + (\lambda/4(8d)^{n-2}(n-1)\mu) t^{-(n-2)l_1} N^{m-n+2} \cdot B(\mathfrak{p}^{(n-1)}), \end{aligned}$$

and

$$\delta = \sup V(\omega, \beta),$$

where the supremum is taken over all zeros $\beta \in \overline{C((z))}^{m+1}$, $\beta \neq 0$, of the ideal $\mathfrak{p}^{(n-1)}$. By Lemma 6 and (10),

$$\begin{aligned} \delta &\geqslant v(\mathfrak{p}^{(n-1)}(\omega))/(m-n+2) N(\mathfrak{p}^{(n-1)}) - 2B(\mathfrak{p}^{(n-1)})/N(\mathfrak{p}^{(n-1)}) \\ &\geqslant (\lambda/(m-n+2) 4(8d)^{n-2}) d^{l_1} t^{-(n-1)l_1} N^{m-n+1} M \\ &\quad + (\lambda/(m-n+2) 4(8d)^{n-2}(n-1)\mu) t^{-(n-2)l_1} N^{m-n+2} B(\mathfrak{p}^{(n-1)})/N(\mathfrak{p}^{(n-1)}) \\ &\quad - 2B(\mathfrak{p}^{(n-1)})/N(\mathfrak{p}^{(n-1)}) \\ &\geqslant (\lambda/(m-n+2) 4(8d)^{n-2}) d^{l_1} t^{-(n-1)l_1} N^{m-n+1} M. \end{aligned}$$

Hence by (6),

$$\min(X, \delta) > 2\lambda MN^m.$$

There exists a nonnegative integer $l_n$ such that

$$2\lambda d^{l_n} MN^m < \min(X, \delta) \leqslant 2\lambda d^{l_n+1} MN^m. \tag{11}$$

Since

$$2\lambda d^{l_n} MN^m < \min(X, \delta) \leqslant X \leqslant (\lambda/2(8d)^{n-2}) d^{l_1} MN^m,$$

we have $l_n \leqslant l_1$. We apply Lemma 5 to the ideal $\mathfrak{p}^{(n-1)}$ and the polynomial $Q_{l_n}$. Put

$$\min(X, \delta) = \sigma\big(v(Q_{l_n}(\omega))\big).$$

Then $1 < \sigma \leqslant 2d$ by (4) and (11). There exists an unmixed homogeneous ideal $I^{(n)} \subset R[X]$, $h(I^{(n)}) = n$, satisfying

$$N(I^{(n)}) \leqslant t^{l_1} N \cdot N(\mathfrak{p}^{(n-1)}) \leqslant t^{nl_1} N^n,$$

$$B(I^{(n)}) \leqslant t^{l_1} N \cdot B(\mathfrak{p}^{(n-1)}) + \mu d^{l_1} M \cdot N(\mathfrak{p}^{(n-1)}) \leqslant n\mu t^{(n-1)l_1} d^{l_1} MN^{n-1},$$

$$\begin{aligned} v(I^{(n)}(\omega)) &\geqslant X/2d - B(\mathfrak{p}^{(n-1)}) t^{l_1} N - N(\mathfrak{p}^{(n-1)}) \mu d^{l_1} M \\ &\geqslant (\lambda/2(8d)^{n-1}) d^{l_1} t^{-(n-1)l_1} N^{m-n+1} M \cdot N(\mathfrak{p}^{(n-1)}) \\ &\quad + (\lambda/2(8d)^{n-1}(n-1)\mu) t^{-(n-2)l_1} N^{m-n+2} \cdot B(\mathfrak{p}^{(n-1)}), \end{aligned} \tag{12}$$

by (10). We suppose that there is no homogeneous prime ideal $\mathfrak{p}$ which satisfies the assertion for $n$. We consider the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ which are defined in Proposition 2 for the ideal $I^{(n)}$. Then for all $j$, $1 \leqslant j \leqslant s$,

$$v(\mathfrak{p}_j(\omega)) < (\lambda/4(8d)^{n-1}) d^{l_1} t^{-nl_1} N^{m-n} M \cdot N(\mathfrak{p}_j) + (\lambda/4(8d)^{n-1} n\mu) t^{-(n-1)l_1} N^{m-n+1} \cdot B(\mathfrak{p}_j).$$

By the equalities in Proposition 2, we have

$$\begin{aligned} v(I^{(n)}(\omega)) &= v(b) + \sum_{j=1}^{s} k_j v(\mathfrak{p}_j(\omega)) \\ &< v(b) + (\lambda/4(8d)^{n-1}) d^{l_1} t^{-nl_1} N^{m-n} M \cdot N(I^{(n)}) \\ &\quad + (\lambda/4(8d)^{n-1} n\mu) t^{-(n-1)l_1} N^{m-n+1} (B(I^{(n)}) - B(b)) \\ &\leqslant (\lambda/4(8d)^{n-1}) d^{l_1} t^{-(n-1)l_1} N^{m-n+1} M \cdot N(\mathfrak{p}^{(n-1)}) \\ &\quad + (\lambda/4(8d)^{n-1} n\mu) t^{-(n-2)l_1} N^{m-n+2} \cdot B(\mathfrak{p}^{(n-1)}) \\ &\quad + (\lambda/4(8d)^{n-1} n) d^{l_1} t^{-(n-1)l_1} N^{m-n+1} M \cdot N(\mathfrak{p}^{(n-1)}). \end{aligned}$$

This contradicts the inequality (12) and the assertion is proved.

We can find a nonnegative integer $l_{m+1}$ in the same way as $l_n$ in the proof of the assertion. Applying Lemma 5 to the ideal $\mathfrak{p}^{(m)}$ and the polynomial $Q_{l_{m+1}}$, we have

$$0 \geqslant (\lambda/2(8d)^m) d^{l_1} t^{-ml_1} M \cdot N(\mathfrak{p}^{(m)}) + (\lambda/2(8d)^m m\mu) t^{-(m-1)l_1} N \cdot B(\mathfrak{p}^{(m)}).$$

This is a contradiction and completes the proof of the theorem.

### References


[1] P.-G. Becker, *Effective measures for algebraic independence of the values of Mahler type functions*, to appear.

[2] P.-G. Becker and K. Nishioka, *Measures of the algebraic independence for the values of Mahler type functions*, C. R. Math. Rep. Acad. Sci. Canada 11 (3) (1989), 89–93.

[3] Yu. V. Nesterenko, *Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers*, Izv. Akad. Nauk SSSR Ser. Mat. 41 (1977); English transl. in Math. USSR Izv. 11 (1977), 239–270.

[4] — *Estimates for the characteristic function of a prime ideal*, Mat. Sb. 123 (165) (1984); English transl. in Math. USSR Sb. 51 (1985), 9–32.

[5] — *On algebraic independence of algebraic powers of algebraic numbers*, Mat. Sb. 123 (165) (1984); English transl. in Math. USSR Sb. 51 (1985), 429–454.

[6] — *On a measure of the algebraic independence of the values of a certain functions*, Mat. Sb. 128 (170) (1985); English transl. in Math. USSR Sb. 56 (1987), 545–567.



DEPARTMENT OF MATHEMATICS
NARA WOMEN'S UNIVERSITY
Kita-Uoya Nishimachi
Nara 630, Japan


*Received on 15.3.1989* (1914)

---

ACTA ARITHMETICA
LVI (1990)

# Sous-groupes minimaux des groupes de Lie commutatifs réels, et applications arithmétiques

par

DAMIEN ROY (Paris)

**Introduction.** On dit qu'un groupe abélien est de *type fini* s'il est engendré par un nombre fini d'éléments. Alors on définit son *rang* comme le plus petit entier $r \geqslant 0$ tel que le groupe soit engendré par $r$ éléments. On convient qu'un groupe $\{e\}$, réduit à son élément neutre, est de rang 0. Cela étant posé, nous disons qu'un sous-groupe $\Gamma$ d'un groupe topologique commutatif $R$ est *minimal* s'il est de type fini, dense dans $R$, et si aucun sous-groupe de $\Gamma$ de rang inférieur au rang de $\Gamma$ n'est dense dans $R$. Dans cet article, on considère le cas où $R$ est un groupe de Lie commutatif réel. L'étude des sous-groupes minimaux d'un tel groupe $R$ est motivée par le problème suivant:

Soient $k$ une extension algébrique de $\boldsymbol{Q}$ de degré fini, et $R$ le groupe des éléments inversibles de la $\boldsymbol{R}$-algèbre $k \otimes_{\boldsymbol{Q}} \boldsymbol{R}$, déduite de la $\boldsymbol{Q}$-algèbre $k$ par extension des scalaires de $\boldsymbol{Q}$ à $\boldsymbol{R}$. C'est un groupe de Lie commutatif réel pour la structure différentielle de sous-variété ouverte de l'espace vectoriel réel $k \otimes_{\boldsymbol{Q}} \boldsymbol{R}$. Via l'injection canonique, le groupe $k^\times$ s'identifie à un sous-groupe dense de $R$. Dans ce contexte, J.-L. Colliot-Thélène demandait ([3], remarque 3.8) si $k^\times$ contient toujours un sous-groupe de type fini, dense dans $R$. Cette question a été résolue de manière affirmative, d'abord par H. W. Lenstra Jr. [6] et J.-L. Brylinski ([2], et [10], ch. I, lemme 3.18), lorsque $k$ est une extension abélienne de $\boldsymbol{Q}$, puis par M. Waldschmidt ([11], §4, et [10], ch. I, cor. 3.17), dans le cas général. Pour préciser leurs solutions, désignons par $r_1$ le nombre de plongements réels de $k$, et par $r_2$ le nombre de paires de plongements complexes conjugués de $k$. Alors le degré $d$ de $k$ sur $\boldsymbol{Q}$ s'écrit $r_1 + 2r_2$. Désignons aussi par $R_0$ la composante neutre de $R$. Chacun d'eux construit explicitement un sous-groupe de type fini de $k^\times$ qui est dense dans $R_0$, de rang $2d - r_2$ chez H. W. Lenstra Jr., de rang $2d$ chez J.-L. Brylinski, de rang $d^2 - d + 2$ chez M. Waldschmidt. Comme le quotient $R/R_0$ est un groupe fini, et que $k^\times$ est dense dans $R$, cela répond bien à la question de J.-L. Colliot-Thélène. Suite à ces résultats, J.-J. Sansuc a demandé quel est le plus petit entier $r$ tel que $k^\times$ contienne un sous-groupe de type fini, de rang $r$, dense dans $R$ ([9], remarque 4.3). Puisqu'un tel sous-groupe de $R$ est nécessairement minimal, une façon de répondre à cette question est de majorer le rang des sous-groupes minimaux de