ANNALES
POLONICI MATHEMATICI
LX.3 (1995)

On the approximate roots of polynomials

by Janusz Gwoździewicz and Arkadiusz Płoski (Kielce)

Abstract. We give a simplified approach to the Abhyankar–Moh theory of approximate roots. Our considerations are based on properties of the intersection multiplicity of local curves.

Introduction. In the fundamental paper [2] S. S. Abhyankar and T. T. Moh developed the theory of approximate roots of polynomials with coefficients in the meromorphic series field. In [3] they applied approximate roots to the polynomial automorphisms of the plane. Later on S. S. Abhyankar gave a simplified version [1] of [2] and T. T. Moh published generalized versions of the central theorems of [2] in [7] and [8].

Our main results are Theorems 1.1 and 1.2 presented in Section 1 of this paper. As an application we get the theorems of [2] (Theorem 1.4). To prove Theorem 1.1 which implies the main property of approximate roots (1.4(1)) we use, as in [1], the Tschirnhausen operator and some properties of the semigroup of a local analytic curve. We do not need deformations of power series which are essential for Abhyankar–Moh's method. We use Puiseux expansions only to construct "pseudoroots" (cf. [1, Ch. II] and Lemma 3.1 of this paper).

Our Theorem 1.2 is a generalization of Abhyankar's irreducibility criterion [1, Ch. V]. Its proof is based on the Max Noether formula for the intersection multiplicity of plane curves and is more intrinsic.

We restrict our considerations to the classical case of power series—the "algebroid case" according to Abhyankar [1]. We show in Section 2 that we can reduce the "pure meromorphic case" (important for polynomial automorphisms) to the algebroid case by a suitable choice of coordinates.

Throughout this paper the field $\mathbb{C}$ may be replaced by any algebraically closed field of characteristic zero.

1991 *Mathematics Subject Classification*: 32B30, 14B05.
Key words and phrases: approximate root, semigroup of an analytic curve, irreducibility criterion.

1. The main results. For any power series $f, g \in \mathbb{C}[[x, y]]$ we define the *intersection number* $(f, g)_0$ by $(f, g)_0 = \dim_{\mathbb{C}} \mathbb{C}[[x, y]]/(f, g)$. Suppose that $f = f(x, y)$ is an irreducible power series and let $n = (f, x)_0 = \operatorname{ord} f(0, y) < \infty$. Then there exists a power series $y(t) \in \mathbb{C}[[t]]$ with $\operatorname{ord} y(t) > 0$ such that $f(t^n, y(t)) = 0$. We have $(f, g)_0 = \operatorname{ord} g(t^n, y(t))$ for any $g = g(x, y) \in \mathbb{C}[[x, y]]$. The mapping $g \mapsto (f, g)_0$ induces a valuation v_f of the ring $\mathbb{C}[[x, y]]/(f)$. Let $\Gamma(f)$ be the semigroup of v_f, i.e. $\Gamma(f) = \{(f, g)_0 \in \mathbb{N} : g \not\equiv 0 \bmod f\}$.

Let us recall the well known structure theorem for the semigroup $\Gamma(f)$ ([6], [10], [2] and Section 3 of this paper).

THEOREM 1.0. *There is a sequence of positive integers* $\bar{b}_0, \bar{b}_1, \ldots, \bar{b}_h$ *such that*

(i) $\bar{b}_0 = (f, x)_0$,
(ii) $\bar{b}_k = \min(\Gamma(f) \setminus (\mathbb{N}\bar{b}_0 + \ldots + \mathbb{N}\bar{b}_{k-1}))$ *for* $k = 1, \ldots, h$,
(iii) $\Gamma(f) = \mathbb{N}\bar{b}_0 + \ldots + \mathbb{N}\bar{b}_h$, *i.e.* $\Gamma(f)$ *is generated by* $\bar{b}_0, \bar{b}_1, \ldots, \bar{b}_h$.

Moreover, if we put $B_k = \gcd(\bar{b}_0, \ldots, \bar{b}_k)$ *for* $k = 0, 1, \ldots, h$ *and* $n_k = B_{k-1}/B_k$ *for* $k = 1, \ldots, h$ *then*

(iv) $B_h = 1$, $n_k > 1$ *and* $n_k \bar{b}_k < \bar{b}_{k+1}$ *for* $k = 1, \ldots, h$ (*we put* $\bar{b}_{h+1} = \infty$).

Obviously $\bar{b}_0, \bar{b}_1, \ldots, \bar{b}_h$ are uniquely determined by $\Gamma(f)$ and $n = (f, x)_0$. If the conditions (i)–(iii) are satisfied, we write $\Gamma(f) = \langle \bar{b}_0, \ldots, \bar{b}_h \rangle$. If $n = 1$ then the sequence $\bar{b}_0, \ldots, \bar{b}_h$ reduces to $\bar{b}_0 = 1$ and we have $\Gamma(f) = \mathbb{N}$.

Let $\mathcal{O}$ be an integral domain and let d be a positive integer such that d is a unit in $\mathcal{O}$. Let $g \in \mathcal{O}[y]$ be a monic polynomial such that d divides $\deg g$. According to Abhyankar and Moh [2, Sect. 1] the *approximate* dth *root* of g, denoted by $\sqrt[d]{g}$, is defined to be the unique monic polynomial satisfying $\deg(g - (\sqrt[d]{g})^d) < \deg g - \deg \sqrt[d]{g}$. Obviously $\deg \sqrt[d]{g} = \deg g/d$. Let $1 \le k \le h$.

THEOREM 1.1. *Let* $g = g(x, y) \in \mathbb{C}[[x]][y]$ *be a monic polynomial with* $\deg_y g = n/B_k$. *Suppose that* $(f, g)_0 > n_k \bar{b}_k$. *Then* $(f, \sqrt[n_k]{g})_0 = \bar{b}_k$.

The proof of 1.1 is given in Section 4 of this paper. Let $1 < k \le h + 1$.

THEOREM 1.2. *Let* $\phi = \phi(x, y) \in \mathbb{C}[[x, y]]$ *be such that* $(\phi, x)_0 = n/B_{k-1}$. *Then* $(f, \phi)_0 \le \bar{b}_k$ ($\bar{b}_{h+1} = \infty$). *If, additionally,* $(f, \phi)_0 > n_{k-1}\bar{b}_{k-1}$ *then* ϕ *is irreducible and* $\Gamma(\phi) = \langle \bar{b}_0/B_{k-1}, \ldots, \bar{b}_{k-1}/B_{k-1} \rangle$.

The proof of 1.2 is given in Section 5 of this paper. Note that for $k = h+1$ Theorem 1.2 reduces to Abhyankar's irreducibility criterion [1, Ch. V].

LEMMA 1.3. *Let* $g \in \mathcal{O}[y]$ *be a monic polynomial of degree* $m > 0$ *and let* $d, e > 0$ *be integers such that* de *divides* m. *Suppose* de *is a unit in* $\mathcal{O}$.

Then $\sqrt[e]{\sqrt[d]{g}} = \sqrt[ed]{g}$.

Proof. Let $h = \sqrt[e]{\sqrt[d]{g}}$, so $\deg h = m/(de)$. We have

$$\sqrt[d]{g} = \left(\sqrt[e]{\sqrt[d]{g}}\right)^e + R, \qquad \deg R < \frac{m}{d} - \frac{m}{de}$$

and

$$g = (\sqrt[d]{g})^d + S, \qquad \deg S < m - \frac{m}{d} \le m - \frac{m}{de}.$$

Then $g = (h^e + R)^d + S = h^{ed} + T$ where

$$T = \sum_{i=1}^{d} \binom{d}{i} (h^e)^{d-i} R^i + S.$$

Since

$$\deg\left(\binom{d}{i}(h^e)^{d-i}R^i\right) < (ed - ei)\frac{m}{de} + i\left(\frac{m}{d} - \frac{m}{de}\right) \le m - \frac{m}{de}$$

we get $\deg T < m - m/(de)$. This shows that $h = \sqrt[ed]{g}$.

Remark. The existence and uniqueness of $\sqrt[d]{g}$ can be checked directly. If $g(y) = y^m + a_1 y^{m-1} + \ldots + a_m$ and $h(y) = y^{m/d} + b_1 y^{m/d-1} + \ldots + b_{m/d}$ then $\deg(g(y) - (h(y))^d) < m - m/d$ if and only if

$$(*) \qquad a_\mu = db_\mu + \sum\nolimits^* \alpha_{i_1,\ldots,i_{\mu-1}} b_1^{i_1} \ldots b_{\mu-1}^{i_{\mu-1}}, \qquad \mu = 1, \ldots, m/d,$$

where

$$\alpha_{i_1,\ldots,i_{\mu-1}} = \binom{d}{i_1 + \ldots + i_{\mu-1}} \frac{(i_1 + \ldots + i_{\mu-1})!}{i_1! \ldots i_{\mu-1}!}$$

and $\sum^*$ denotes summation over all $i_1, \ldots, i_{\mu-1}$ such that $i_1 + 2i_2 + \ldots + (\mu-1)i_{\mu-1} = \mu$.

The system of m/d equations $(*)$ with unknowns $b_1, \ldots, b_{m/d}$ has a unique solution given by

$$(**) \qquad b_\mu = \frac{1}{d}a_\mu + \sum\nolimits^* \beta_{i_1,\ldots,i_{\mu-1}} a_1^{i_1} \ldots a_{\mu-1}^{i_{\mu-1}}, \qquad \mu = 1, \ldots, m/d,$$

where $\beta_{i_1,\ldots,i_{\mu-1}} \in \mathbb{Z}[1/d]$ depend only on m and d.

Other proofs of the existence and uniqueness of approximate roots are given in [2, Sect. 6].

Now, we can prove the Abhyankar–Moh theorem.

THEOREM 1.4 ([2]). *Let* $f = f(x,y) \in \mathbb{C}[[x]][y]$ *be an irreducible distinguished polynomial of degree* $n > 1$ *with* $\Gamma(f) = \langle \overline{b}_0, \overline{b}_1, \ldots, \overline{b}_h \rangle$ *and* $\overline{b}_0 = (f,x)_0 = n$. *Let* $1 \le k \le h+1$. *Then*:

(1) $(f, \sqrt[B_{k-1}]{f})_0 = \overline{b}_k$,

(2) $\sqrt[B_{k-1}]{f}$ *is an irreducible distinguished polynomial of degree* n/B_{k-1} *such that*

$$\Gamma(\sqrt[B_{k-1}]{f}) = \langle \overline{b}_0/B_{k-1}, \ldots, \overline{b}_{k-1}/B_{k-1}\rangle.$$

Proof. First we check (1) using 1.1 and induction on k. If $k = h + 1$ then $B_{k-1} = B_h = 1$, $\overline{b}_k = \overline{b}_{h+1} = \infty$ and (1) is obvious. Let $k \le h$ and suppose $(f, \sqrt[B_k]{f})_0 = \overline{b}_{k+1}$. The polynomial $\sqrt[B_k]{f}$ is of degree n/B_k and $(f, \sqrt[B_k]{f})_0 = \overline{b}_{k+1} > n_k\overline{b}_k$ by 1.0(iv) so we can apply 1.1 to $g = \sqrt[B_k]{f}$ to get $(f, \sqrt[n_k]{g})_0 = \overline{b}_k$. By 1.3 we have $\sqrt[n_k]{g} = \sqrt[n_k]{\sqrt[B_k]{f}} = \sqrt[B_{k-1}]{f}$. Consequently, $(f, \sqrt[B_{k-1}]{f})_0 = \overline{b}_k$ and (1) is proved.

In order to prove (2) put $\phi = \sqrt[B_{k-1}]{f}$ and assume $k > 1$, the case $k = 1$ being obvious. Thus ϕ is a distinguished polynomial of degree n/B_{k-1}, hence $(\phi, x)_0 = n/B_{k-1}$. On the other hand, $(f, \phi)_0 = \overline{b}_k > n_{k-1}\overline{b}_{k-1}$ by (1). According to Theorem 1.2, $\phi = \sqrt[B_{k-1}]{f}$ is irreducible and $\Gamma(\phi) = \langle \overline{b}_0/B_{k-1}, \ldots, \overline{b}_{k-1}/B_{k-1}\rangle$.

2. The Abhyankar–Moh inequality. We give here a geometrical version of the Abhyankar–Moh inequality which is the basic tool for proving the Embedding Theorem [3]. Let $\mathbf{C} \subset \mathbb{P}^2$ be an irreducible projective plane curve of degree $n > 1$ and let $\mathbf{O} \in \mathbf{C}$ be its singular point. We assume that $\mathbf{C}$ is analytically irreducible at $\mathbf{O}$, i.e. the analytic germ $(\mathbf{C}, \mathbf{O})$ is irreducible, and let $\mathbf{L}$ be the unique tangent to $\mathbf{C}$ at $\mathbf{O}$. Let $\Gamma(\mathbf{C}, \mathbf{O})$ be the semigroup of the branch of $\mathbf{C}$ passing through $\mathbf{O}$ and let $\Gamma(\mathbf{C}, \mathbf{O}) = \langle \overline{b}_0, \overline{b}_1, \ldots, \overline{b}_h\rangle$ with $\overline{b}_0 = (\mathbf{C}.\mathbf{L})_{\mathbf{O}}$.

Theorem 2.1 ([3]). *Suppose that* $\mathbf{C} \cap \mathbf{L} = \{\mathbf{O}\}$, *i.e.* $\overline{b}_0 = n$. *Then* $B_{h-1}\overline{b}_h < n^2$.

Proof. Choose the line at infinity not passing through $\mathbf{O}$ and let x, y be an affine system of coordinates centered at $\mathbf{O}$ such that $\mathbf{L}$ has equation $x = 0$. Let $f(x, y) \in \mathbb{C}[x, y]$ be the irreducible equation of $\mathbf{C}$ in the coordinates x, y. It is easy to see that f is a distinguished, irreducible polynomial in $\mathbb{C}[[x, y]]$ and $\Gamma(f) = \langle \overline{b}_0, \overline{b}_1, \ldots, \overline{b}_h\rangle$.

We have $\deg f = n$ and consequently $\deg \sqrt[B_{h-1}]{f} = n/B_{h-1}$, thus 1.4(1) and Bézout's theorem imply

$$\overline{b}_h = (f, \sqrt[B_{h-1}]{f})_0 \le n\frac{n}{B_{h-1}},$$

that is, $B_{h-1}\overline{b}_h \le n^2$. In fact, $B_{h-1}\overline{b}_h < n^2$ because the equality $B_{h-1}\overline{b}_h = n^2$ implies $\overline{b}_h = n\frac{n}{B_{h-1}}$, contrary to $\overline{b}_h \not\equiv 0 \bmod B_{h-1}$.

The inequality 2.1 has an application to polar curves [4].

THEOREM 2.2 (with the assumptions as above). *Let* $(\mathbf{D},\mathbf{O})$ *be an irreducible component of the local polar of* $\mathbf{C}$ *with respect to* $\mathbf{L}$. *Then* $(\mathbf{C}.\mathbf{D})_{\mathbf{O}} < (\mathbf{C}.\mathbf{L})_{\mathbf{O}}(\mathbf{D}.\mathbf{L})_{\mathbf{O}}$.

Proof. In the coordinates x, y introduced in the proof of 2.1 the local polar is given by $\partial f/\partial y = 0$ and its irreducible component is given by $g = 0$ where g is an irreducible (in $\mathbb{C}[[x,y]]$) divisor of $\partial f/\partial y$. By the Merle formula for polar invariants [6], [4], [5] and Theorem 2.1 we get

$$\frac{(\mathbf{C}.\mathbf{D})_{\mathbf{O}}}{(\mathbf{D}.\mathbf{L})_{\mathbf{O}}} = \frac{(f,g)_0}{(g,x)_0} = \frac{B_{k-1}}{\overline{b}_0}\,\overline{b}_k \le \frac{B_{h-1}}{\overline{b}_0}\,\overline{b}_h < n = (f,x)_0 = (\mathbf{C}.\mathbf{L})_{\mathbf{O}}$$

and the theorem follows.

3. The characteristic and the semigroup of an analytic curve and the Noether formula. In this section we recall some well-known notions of the theory of analytic curves. Our main references are [10] and [6]. Let $f = f(x,y)$ be an irreducible power series y-regular of order $n = \operatorname{ord} f(0,y)$. There exists a power series $y(t) \in \mathbb{C}[[t]]$ with $\operatorname{ord} y(t) > 0$ such that $f(t^n, y(t)) = 0$. Moreover, every solution of the equation $f(t^n, y) = 0$ is of the form $y(\varepsilon t)$ for some ε such that $\varepsilon^n = 1$. Let $y(t) = \sum a_j t^j$. We put $S(f) = \{j \in \mathbb{N} : a_j \ne 0\}$. Note that $S(f)$ depends only on f and $\gcd S(f) = 1$. The *characteristic* $b_0, b_1, \ldots, b_h$ of f is the unique sequence of positive integers satisfying

(i′) $b_0 = n$,
(ii′) $b_{k+1} = \min\{j \in S(f) : \gcd(b_0,\ldots,b_k,j) < \gcd(b_0,\ldots,b_k)\}$,
(iii′) $\gcd(b_0,\ldots,b_h) = 1$.

We put $B_k = \gcd(b_0,\ldots,b_k)$ for $k = 0,1,\ldots,h$ and

$$\overline{b}_k = b_k + \frac{1}{B_{k-1}}\sum_{i=1}^{k-1}(B_{i-1}-B_i)b_i \quad \text{for } k = 1,\ldots,h.$$

We assume that the sum of an empty family is equal to zero. Thus we have $\overline{b}_1 = b_1$. We put $\overline{b}_0 = b_0$. One checks easily that $\gcd(\overline{b}_0,\ldots,\overline{b}_k) = B_k$ for $k = 0,\ldots,h$ and

$$b_k = \overline{b}_k - \sum_{i=1}^{k-1}\left(\frac{B_{i-1}}{B_i} - 1\right)\overline{b}_i \quad \text{for } k = 0,1,\ldots,h.$$

Therefore the sequence $\overline{b}_0,\ldots,\overline{b}_k$ determines $B_0,\ldots,B_k$ and $b_0,\ldots,b_k$ for any $k = 0,\ldots,h$.

Remark ([10]). Let $u(n)$ be the group of nth roots of unity in $\mathbb{C}$. The sequence $B_0 = n$, $B_1,\ldots,B_h = 1$ of divisors of n determines the filtration of groups: $u(n) = u(B_0) \supset u(B_1) \supset \ldots \supset u(B_{h-1}) \supset u(B_h) = \{1\}$. We have $\operatorname{ord}(y(t) - y(\varepsilon t)) = b_k$ for $\varepsilon \in u(B_{k-1}) \setminus u(B_k)$.

Let $n_k = B_{k-1}/B_k$ for $k = 1, \ldots, h$. We have $\bar{b}_{k+1} - n_k \bar{b}_k = b_{k+1} - b_k > 0$ for $k = 1, \ldots, h-1$. For any k with $0 \le k \le h$ we set $S_k = \{j \in S(f) : j < b_{k+1}\}$. We put $b_{h+1} = \bar{b}_{h+1} = \infty$, so $S_h = S(f)$. Let $y_k(t) = \sum_{j \in S_k} a_j t^j$. For the sake of completeness we give here the proofs of two known facts (Lemma 3.1 and Proposition 3.2) which are basic for us.

LEMMA 3.1. *There exists a monic polynomial* $f_k = f_k(x,y) \in \mathbb{C}[[x]][y]$ *such that* $\deg_y f_k = n/B_k$ *and* $(f, f_k)_0 = \bar{b}_{k+1}$ *for* $k = 0, 1, \ldots, h$.

Proof. We can write $y_k(t) = Y_k(t^{B_k})$ with $Y_k(s) \in \mathbb{C}[[s]]$. There exists a polynomial $f_k(x,y) \in \mathbb{C}[[x]][y]$ such that

$$f_k(s^{n/B_k}, y) = \prod_{\mu \in u(n/B_k)} (y - Y_k(\mu s)).$$

Indeed, the product on the right side does not change when we replace s by θs with $\theta \in u(n/B_k)$. We can easily see that $f_k(x,y)$ is monic of degree n/B_k. Note that f_h is the distinguished polynomial associated with f, so $(f, f_h)_0 = \infty = \bar{b}_{h+1}$. Let $k < h$. We have

$$\begin{aligned}(f, f_k)_0 &= \operatorname{ord} f_k(t^n, y(t)) = \operatorname{ord} \prod (y(t) - Y_k(\mu t^{B_k})) \\ &= \sum \operatorname{ord}(y(t) - Y_k(\mu t^{B_k})) = b_{k+1} + \sum_{i=1}^{k} \left(\frac{B_{i-1}}{B_k} - \frac{B_i}{B_k}\right) b_i = \bar{b}_{k+1}\end{aligned}$$

since $\operatorname{ord}(y(t) - Y_k(t^{B_k})) = \operatorname{ord}(y(t) - y_k(t)) = b_{k+1}$ and $\operatorname{ord}(y(t) - Y_k(\mu t^{B_k})) = \operatorname{ord}(Y_k(t^{B_k}) - Y_k(\mu t^{B_k})) = B_k \operatorname{ord}(Y_k(s) - Y_k(\mu s)) = B_k b_i / B_k$ for $\mu \in u(B_{i-1}/B_k) \setminus u(B_i/B_k)$.

PROPOSITION 3.2. *If* $\psi(x,y) \in \mathbb{C}[[x]][y]$, $\psi(x,y) \neq 0$ *and* $\deg_y \psi(x,y) < n/B_k$ *then* $(f, \psi)_0 \in \mathbb{N}\bar{b}_0 + \ldots + \mathbb{N}\bar{b}_k$ *for* $k = 0, 1, \ldots, h$.

Proof. By induction on k, the case $k = 0$ being obvious. Let $k > 0$ and suppose Proposition 3.2 holds true for polynomials of degree $< n/B_{k-1}$. Fix $\psi \in \mathbb{C}[[x]][y]$ with $\deg_y \psi < n/B_k$ and consider the f_{k-1}-adic expansion of ψ:

$$\begin{aligned}(1)\qquad \psi = \psi_0 f_{k-1}^s + \psi_1 f_{k-1}^{s-1} + \ldots + \psi_s,& \\ \psi_0 \neq 0,\ \deg_y \psi_i < \deg_y f_{k-1} = n/B_{k-1}.&\end{aligned}$$

Note that $s \le \deg \psi / \deg f_{k-1} < n_k$. Let I be the set of all $i \in \{0, \ldots, s\}$ such that $\psi_i \neq 0$. Therefore, by the induction hypothesis we get $(f, \psi_i)_0 \in \mathbb{N}\bar{b}_0 + \ldots + \mathbb{N}\bar{b}_{k-1}$, and

$$(2)\qquad (f, \psi_i)_0 \equiv 0 \bmod B_{k-1} \quad \text{for } i \in I.$$

Moreover,

$$(f, \psi_i f_{k-1}^{s-i})_0 \neq (f, \psi_j f_{k-1}^{s-j})_0 \quad \text{for } i \neq j \in I. \tag{3}$$

Indeed, suppose that (3) is not true, so there exist $i, j \in I$ such that $i < j$ and $(f, \psi_i f_{k-1}^{s-i})_0 = (f, \psi_j f_{k-1}^{s-j})_0$. Therefore $(f, \psi_i)_0 + (s - i)(f, f_{k-1})_0 = (f, \psi_j)_0 + (s - j)(f, f_{k-1})_0$ and $(j - i)\overline{b}_k = (f, \psi_j)_0 - (f, \psi_i)_0 \equiv 0 \bmod B_{k-1}$ by (2). The last relation implies $(j - i)\overline{b}_k/B_k \equiv 0 \bmod n_k$ and consequently $j - i \equiv 0 \bmod n_k$ because $\overline{b}_k/B_k$ and n_k are coprime. We get a contradiction because $0 < j - i \leq s < n_k$. Now, by (1) and (3) we get

$$\begin{aligned}(f, \psi)_0 &= \min_{i=0}^{s}(f, \psi_i f_{k-1}^{s-i})_0 = (f, \psi_i f_{k-1}^{s-i})_0 \\ &= (f, \psi_i)_0 + (s - i)\overline{b}_k \in \mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_k.\end{aligned}$$

Proof of Theorem 1.0. By Lemma 3.1, $\overline{b}_0, \ldots, \overline{b}_h \in \Gamma(f)$, thus $\mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_h \subset \Gamma(f)$. On the other hand, by the Weierstrass Division Theorem any element of $\Gamma(f)$ can be written in the form $(f, \psi)_0$ with $\psi \in \mathbb{C}[[x]][y]$, $\deg_y \psi < n = n/B_h$. Proposition 3.2 gives $\mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_h = \Gamma(f)$. Properties (i) and (iv) follow from the construction of the sequence $\overline{b}_0, \ldots, \overline{b}_h$. Property (ii) follows from (iii) established above and from (iv).

Now, let $g = g(x, y)$ be an irreducible power series y-regular of order $p = \operatorname{ord} g(0, y) < \infty$. Suppose that f and g are coprime. Let $z(t) \in \mathbb{C}[[t]]$ with $\operatorname{ord} z(t) > 0$ be such that $g(t^p, z(t)) = 0$. We put

$$o_f(g) = \max\{\operatorname{ord}(y(\varepsilon x^{1/n}) - z(\nu x^{1/p})) : \varepsilon^n = 1,\ \nu^p = 1\}.$$

It is easy to check that

$$\begin{aligned}o_f(g) &= \max\{\operatorname{ord}(y(x^{1/n}) - z(\nu x^{1/p})) : \nu^p = 1\} \\ &= \max\{\operatorname{ord}(y(\varepsilon x^{1/n}) - z(x^{1/p})) : \varepsilon^n = 1\}.\end{aligned}$$

In particular, $o_f(g) = o_g(f)$.

The classical computation leads to the following formula due to Max Noether:

PROPOSITION 3.3 ([6], [5]). *Suppose that f and g are irreducible, y-regular power series with f of characteristic $(b_0, b_1, \ldots, b_h)$, and let k be the smallest strictly positive integer such that $o_f(g) \leq b_k/b_0$ $(b_{h+1}/b_0 = \infty)$. Then*

$$\frac{(f, g)_0}{(g, x)_0} = \sum_{i=1}^{k-1}(B_{i-1} - B_i)\frac{b_i}{b_0} + B_{k-1}o_f(g).$$

Remark ([9]). The Noether formula is really symmetric. Let $(c_0, c_1, \ldots, c_m)$ be the characteristic of g. Then $k \leq m + 1$, $c_i/c_0 = b_i/b_0$ for $i = 1, \ldots, k - 1$ and $o_f(g) \leq c_k/c_0$ $(c_{m+1}/c_0 = \infty)$. If $C_i = \gcd(c_0, \ldots, c_i)$

then the formula can be rewritten in the form
$$\frac{(f,g)_0}{(f,x)_0}=\sum_{i=1}^{k-1}(C_{i-1}-C_i)\frac{c_i}{c_0}+C_{k-1}o_g(f).$$

Using 3.3 we check easily

LEMMA 3.4. *Let $l>0$ be an integer. Then*
$$o_f(g)\le\frac{b_l}{b_0}\quad\text{iff}\quad\frac{(f,g)_0}{(g,x)_0}\le B_{l-1}\frac{\overline{b}_l}{\overline{b}_0}.$$
Moreover, $o_f(g)=b_l/b_0$ *is equivalent to* $(f,g)_0/(g,x)_0=B_{l-1}\overline{b}_l/\overline{b}_0$.

Finally, let us note

COROLLARY 3.5 (to Theorem 1.4). *If* $f=f(x,y)\in\mathbb{C}[[x]][y]$ *is an irreducible distinguished polynomial*, *then* $o_f(\sqrt[B_{k-1}]{f})=b_k/b_0$ *for* $k=1,\ldots,h$.

Proof. We have $(\sqrt[B_{k-1}]{f},x)_0=\deg_y\sqrt[B_{k-1}]{f}=n/B_{k-1}$ and $(f,\sqrt[B_{k-1}]{f})_0=\overline{b}_k$ by 1.4(1). Hence
$$\frac{(f,\sqrt[B_{k-1}]{f})_0}{(\sqrt[B_{k-1}]{f},x)_0}=B_{k-1}\frac{\overline{b}_k}{\overline{b}_0}.$$
The power series $\sqrt[B_{k-1}]{f}$ is irreducible by 1.4(2), thus by 3.4 we get $o_f(\sqrt[B_{k-1}]{f})=b_k/b_0$.

4. Proof of Theorem 1.1. Let $g\in\mathcal{O}[y]$ be a monic polynomial with coefficients in the integral domain $\mathcal{O}$ of characteristic zero and let d be a positive divisor of $\deg g$. Given any monic polynomial $h\in\mathcal{O}[y]$ of degree $\deg g/d$ we have the h-adic expansion of g, namely
$$g=h^d+a_1h^{d-1}+\ldots+a_d,\qquad a_i\in\mathcal{O}[y],\ \deg a_i<\deg h.$$
The polynomials a_i are uniquely determined by g, h. The *Tschirnhausen operator* $\tau_g(h)=h+\frac{1}{d}a_1$ maps h to $\tau_g(h)$ which is again monic of degree $\deg g/d$. One checks easily [2, Sect. 1 and Sect. 6, Remark 6.4] that:

1) $a_1=0$ if and only if $h=\sqrt[d]{g}$,

2) if $g=[\tau_g(h)]^d+\overline{a}_1[\tau_g(h)]^{d-1}+\ldots+\overline{a}_d$ is the $\tau_g(h)$-expansion of g then $\deg\overline{a}_1<\deg a_1$ or $\overline{a}_1=0$.

Therefore we get

LEMMA 4.1 ([2]). $\sqrt[d]{g}=\tau_g(\tau_g\ldots(\tau_g(h))\ldots)$ *with* τ_g *repeated* $\deg g/d$ *times.*

To prove 1.1 it suffices to check the following:

(∗) if $h(x,y)\in\mathbb{C}[[x]][y]$ is a monic polynomial of degree n/B_{k-1} such that $(f,h)_0=\overline{b}_k$, then $(f,\tau_g(h))_0=\overline{b}_k$.

Indeed, to get the relation $(f, \sqrt[n_k]{g})_0 = \overline{b}_k$ we take $h = f_{k-1}$ (cf. Lemma 3.1) and apply the Tschirnhausen operator τ_g to h $\deg g/n_k = n/B_{k-1}$ times.

To prove $(*)$ fix a monic polynomial $h(x,y) \in \mathbb{C}[[x]][y]$ such that $\deg h = n/B_{k-1}$ and $(f,h)_0 = \overline{b}_k$ and consider the h-adic expansion of g:

$$(4)\qquad g = h^{n_k} + a_1 h^{n_k-1} + \ldots + a_{n_k}, \qquad \deg_y a_i < \deg_y h = n/B_{k-1}.$$

Let I be the set of all $i \in \{1,\ldots,n_k\}$ such that $a_i \neq 0$. Therefore $(f,a_i)_0 < \infty$ for $i \in I$ and by Proposition 3.2 we have $(f,a_i)_0 \in \mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_{k-1}$ and hence $(f,a_i)_0 \equiv 0 \bmod B_{k-1}$ for $i \in I$.

We have

$$(5)\qquad (f, a_i h^{n_k-i})_0 \neq (f, a_j h^{n_k-j})_0 \quad \text{for } i \neq j \in I.$$

Indeed, $(f, a_i h^{n_k-i})_0 = (f, a_j h^{n_k-j})_0$ with $i < j$ implies, as in the proof of (2), the congruence $(j-i)\overline{b}_k/B_k \equiv 0 \bmod n_k$, which leads to a contradiction for $0 < j-i < n_k$.

From (4) and (5) we have

$$(6)\qquad (f, g - h^{n_k})_0 = \min_{i=1}^{n_k} (f, a_i h^{n_k-i})_0.$$

By assumption $(f,g)_0 > n_k\overline{b}_k = (f,h^{n_k})_0$, so $(f, g-h^{n_k})_0 = n_k\overline{b}_k$ and (6) implies $n_k\overline{b}_k \le (f, a_i h^{n_k-i})_0 = (f,a_i)_0 + (n_k - i)\overline{b}_k$ for $i = 1,\ldots,n_k$. Therefore we get

$$(7)\qquad (f,a_i)_0 \ge i\overline{b}_k \quad \text{for } i = 1,\ldots,n_k.$$

Moreover, we have

$$(8)\qquad \text{if } (f,a_i)_0 = i\overline{b}_k,\ 1 \le i \le n_k,\ \text{then } i = n_k.$$

Indeed, from $(f,a_i)_0 = i\overline{b}_k$ it follows that $i\overline{b}_k \equiv 0 \bmod B_{k-1}$ and $i\overline{b}_k/B_k \equiv 0 \bmod n_k$, so $i \equiv 0 \bmod n_k$ because $\overline{b}_k/B_k$ and n_k are coprime. Hence we get $i = n_k$.

By (8) we get (because $n_k > 1$)

$$(9)\qquad (f,a_1)_0 > \overline{b}_k.$$

Therefore $(f, \tau_g(h))_0 = (f, h + (1/n_k)a_1)_0 = (f,h)_0 = \overline{b}_k$.

5. Proof of Theorem 1.2.

The proof is based on the following:

LEMMA 5.1. *Let $g = g(x,y)$ be an irreducible power series, $p = (g,x)_0 < \infty$ and let $1 < k \le h+1$. If $(f,g)_0/(g,x)_0 > B_{k-2}\overline{b}_{k-1}/b_0$, then $(g,x)_0 \equiv 0 \bmod (b_0/B_{k-1})$. If, additionally, $(g,x)_0 = b_0/B_{k-1}$, then $\Gamma(g) = \langle \overline{b}_1/B_{k-1}, \ldots, \overline{b}_{k-1}/B_{k-1}\rangle$.*

Proof. Let $(c_0, c_1, \ldots, c_m)$ with $c_0 = p$ be the characteristic of g. By Lemma 3.4 we have $o_f(g) > b_{k-1}/b_0$, so there exist Puiseux expansions determined by $f(x,y) = 0$ and $g(x,y) = 0$ respectively which coincide up to "monomials" of degree b_{k-1}/n. Therefore $k-1 \le m$ and $b_1/n = c_1/p, \ldots, b_{k-1}/n = c_{k-1}/p$. There exist integers $a_0, \ldots, a_{k-1}$ such that $B_{k-1} = a_0 b_0 + a_1 b_1 + \ldots + a_{k-1} b_{k-1}$, and consequently

$$pB_{k-1} = (a_0 p)n + a_1(nc_1) + \ldots + a_{k-1}(nc_{k-1}) \equiv 0 \bmod n$$

and $p \equiv 0 \bmod (n/B_{k-1})$, which proves the first part of 5.1.

Suppose now that $p = n/B_{k-1}$. We have $c_i = pb_i/n = b_i/B_{k-1}$ for $i = 1, \ldots, k-1$, hence $\Gamma(g) = \langle \overline{b}_1/B_{k-1}, \ldots, \overline{b}_{k-1}/B_{k-1} \rangle$.

Now, we can pass to the proof of 1.2.

Let $\phi = \phi(x,y) \in \mathbb{C}[[x,y]]$ be y-regular, $(\phi, x)_0 = n/B_{k-1}$. We shall check that $(f,\phi)_0 \le \overline{b}_k$. If $k = h+1$ this is obvious ($\overline{b}_{h+1} = \infty$), so we assume $k \le h$. Write

$$\phi = g_1 \cdot \ldots \cdot g_s, \qquad g_j \in \mathbb{C}[[x,y]] \text{ irreducible.}$$

We have

$$\frac{(f, g_j)_0}{(g_j, x)_0} \le \frac{B_{k-1}\overline{b}_k}{n} \qquad \text{for all } j = 1, \ldots, s. \tag{10}$$

Indeed, if $(f,g_j)_0/(g_j,x)_0 > B_{k-1}\overline{b}_k/n$ for some j then, by Lemma 5.1, $(g_j, x)_0 \equiv 0 \bmod (n/B_k)$ and consequently $(g_j,x)_0 \ge n/B_k$. This is impossible, because $(g_j,x)_0 \le (\phi,x)_0 = n/B_{k-1}$.

Now, from (10) we get

$$(f,\phi)_0 = \sum_j (f,g_j)_0 \le \sum_j \frac{B_{k-1}\overline{b}_k}{n}(g_j,x)_0 = \frac{B_{k-1}\overline{b}_k}{n}(\phi,x)_0 = \overline{b}_k.$$

Having proved the first part of 1.2, assume that $(f,\phi)_0 > n_{k-1}\overline{b}_{k-1}$. We claim that there exists a $j \in \{1, \ldots, s\}$ such that

$$\frac{(f,g_j)_0}{(g_j,x)_0} > \frac{B_{k-2}\overline{b}_{k-1}}{n}. \tag{11}$$

Suppose, contrary to our claim, that $(f,g_j)_0/(g_j,x)_0 \le B_{k-2}\overline{b}_{k-1}/n$ for all $j = 1, \ldots, s$. Thus we would have

$$\begin{aligned}(f,\phi)_0 &= \sum_j (f,g_j)_0 \le \frac{B_{k-2}\overline{b}_{k-1}}{n}\sum_j (g_j,x)_0 \\ &= \frac{B_{k-2}\overline{b}_{k-1}}{n}(\phi,x)_0 = n_{k-1}\overline{b}_{k-1},\end{aligned}$$

which contradicts our assumption.

From (11) it follows, by Lemma 5.1, that $(g_j,x)_0 = qn/B_{k-1}$ for some integer $q \ge 1$. On the other hand, $(g_j,x)_0 \le (\phi,x)_0 = n/B_{k-1}$. Therefore $q = 1$ and $(g_j,x)_0 = (\phi,x)_0$. Recall that g_j divides ϕ, g_j is irreducible and ord $g_j(0, y) = \text{ord}\, \phi(0, y)$, thus g_j is associated to ϕ, which proves irreducibility of ϕ.

6. Irreducibility criterion. The aim of this section is to prove a version of 1.2 (Proposition 6.1) without using the Max Noether formula. Theorem 1.4(1) and the second part of 6.1 imply irreducibility of approximate roots. Let $1 \le k \le h$.

PROPOSITION 6.1. *Let $\phi = \phi(x, y) \in \mathbb{C}[[x]][y]$ be a monic polynomial with $\deg_y \phi = n/B_{k-1}$. Then $(f, \phi)_0 \le \overline{b}_k$. If $(f, \phi)_0 = \overline{b}_k$ then ϕ is irreducible in $\mathbb{C}[[x]][y]$.*

Proof. Let $f_{k-1} = f_{k-1}(x, y) \in \mathbb{C}[[x]][y]$ be as in Lemma 3.1. Then $\deg_y(\phi - f_{k-1}) < n/B_{k-1}$ and by Proposition 3.2 we get $(f, \phi - f_{k-1})_0 \in \mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_{k-1}$. Therefore $(f, f_{k-1})_0 = \overline{b}_k \ne (f, \phi - f_{k-1})_0$ by Theorem 1.0(ii) and we get $(f, \phi)_0 = \min((f, f_{k-1})_0, (f, \phi - f_{k-1})_0) \le (f, f_{k-1})_0 = \overline{b}_k$.

Let $(f, \phi)_0 = \overline{b}_k$ and suppose that ϕ is not irreducible. Then $\phi = \phi_1\phi_2$ in $\mathbb{C}[[x]][y]$ with monic polynomials ϕ_1, ϕ_2 of positive degrees. Consequently, $\deg_y \phi_1$, $\deg_y \phi_2 < \deg_y \phi = n/B_{k-1}$ and by Proposition 3.2 we get $(f, \phi_1)_0$, $(f, \phi_2)_0 \in \mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_{k-1}$ and $\overline{b}_k = (f, \phi)_0 = (f, \phi_1)_0 + (f, \phi_2)_0 \in \mathbb{N}\overline{b}_0 + \ldots + \mathbb{N}\overline{b}_{k-1}$. But this contradicts 1.0(ii). Therefore ϕ is irreducible in $\mathbb{C}[[x]][y]$.

Note. We thank the referee for his pointing out the article by H.-C. Chang and L.-Ch. Wang, *An intersection theoretical proof of the embedding line theorem*, J. Algebra 161 (1993), 467–479. The authors prove there a weak version of the main property of approximate roots and the Abhyankar–Moh inequality. Their considerations are based on Zariski's analysis of the semigroup of intersection numbers and on Bézout's theorem.

References

[1] S. S. Abhyankar, *Expansion Techniques in Algebraic Geometry*, Tata Inst. Fund. Research, Bombay, 1977.

[2] S. S. Abhyankar and T. Moh, *Newton–Puiseux expansion and generalized Tschirnhausen transformation*, J. Reine Angew. Math. 260 (1973), 47–83; 261 (1973), 29–54.

[3] —, —, *Embeddings of the line in the plane*, ibid. 276 (1975), 148–166.

[4] R. Ephraim, *Special polars and curves with one place at infinity*, in: Proc. Sympos. Pure Math. 40, Part I, Amer. Math. Soc., 1985, 353–359.

[5] J. Gwoździewicz and A. Płoski, *On the Merle formula for polar invariants*, Bull. Soc. Sci. Lettres Łódź 41 (7) (1991), 61–67.

[6] M. Merle, *Invariants polaires des courbes planes*, Invent. Math. 41 (1977), 103–111.

[7] T. T. Moh, *On the concept of approximate roots for algebra*, J. Algebra 65 (1980), 347–360.

[8] T. T. Moh, *On two fundamental theorems for the concept of approximate roots*, J. Math. Soc. Japan 34 (1982), 637–652.
[9] A. Płoski, *Bézout's theorem for affine curves with one branch at infinity*, Univ. Iagell. Acta Math. 28 (1991), 77–80.
[10] O. Zariski, *Le problème des modules pour les branches planes*, Centre de Mathématiques de l'Ecole Polytechnique, 1973.

DEPARTMENT OF MATHEMATICS
TECHNICAL UNIVERSITY
AL. TYSIĄCLECIA 7
25-314 KIELCE, POLAND
E-mail: MAT-JG@SRV1.TU.KIELCE.PL

Reçu par la Rédaction le 17.5.1993