Алгебра и анализ
Том 28 (2016), № 6

St. Petersburg Math. J.
Vol. 28 (2017), No. 6, Pages 825–853
http://dx.doi.org/10.1090/spmj/1476
Article electronically published on October 2, 2017

# EXTENSION OF THE NEWTON–PUISEUX ALGORITHM TO THE CASE OF A NONZERO CHARACTERISTIC GROUND FIELD. I

A. L. CHISTOV

Abstract. The Newton–Puiseux algorithm for constructing roots of polynomials in the field of fractional power series is generalized to the case of a ground field of nonzero characteristic.

## Introduction

Let $k$ be a ground field and $k((X))$ the field of power series in $X$ with coefficients in $k$. Let $f \in k((X))[Y]$ be a separable polynomial of degree $\deg_Y f = d \geq 1$. We shall assume without loss of generality that $f = \sum_{0\leq i\leq d} f_i Y^i$ where $f_i \in k[[X]]$ for all $i$ and the leading coefficient satisfies $\mathrm{lc}_Y f = f_d = 1$. So, $f \in k[[X]][Y]$. Denote by $\Delta = \mathrm{Res}(f, f'_Y)$ the discriminant of the polynomial $f$.

Denote by $\Omega = \overline{k((X))}$ the algebraic closure of the field $k((X))$ and by $\Omega_0$ the maximal weakly ramified extension of $k((X))$ contained in $\Omega$. We have

$$\Omega_0 = \bigcup_{\substack{1\leq\nu\in\mathbb{Z},\\ \mathrm{GCD}(\nu,\, \max\{1,\mathrm{char}(k)\})=1}} k_s((X^{1/\nu})), \tag{1}$$

where $k_s$ is the maximal separable extension of $k$ contained in the algebraic closure $\overline{k}$ of the field $k$ and GCD denotes the greatest common divisor. If the characteristic $\mathrm{char}(k)$ is 0, then $\Omega = \Omega_0 = \bigcup_{\nu\geq 1} \overline{k}((X^{1/\nu}))$.

In any characteristic of the ground field, there is a valuation $\mathrm{ord} : \Omega \to \mathbb{Q} \cup \{+\infty\}$ such that $\mathrm{ord}(X) = 1$. It induces the discrete valuation on each finite extension of the field $k((X))$. Notice that for any elements $x_1, x_2 \in \Omega$ conjugated over the field $k((X))$ we have $\mathrm{ord}(x_1) = \mathrm{ord}(x_2)$.

In the case of zero characteristic, the classical Newton–Puiseux algorithm can be viewed as an algorithm of factoring the polynomials from $k((X))[Y]$ over the field $\Omega_0$ by using the method of Newton broken lines. Namely, let $y = \sum_{i\geq 0} y_i X^{\alpha_i}$ be a root of $f$, where all $y_i$ are elements $\overline{k}$, $\alpha_0 < \alpha_1 < \alpha_2 < \dots$, and all $\alpha_i$ belong to $\frac{1}{e}\mathbb{Z}$ for some $1 \leq e \leq d$ (to fix $e$, we assume that it is minimal possible). Then for every $r \geq 0$ the pair $(y_r, \alpha_r)$ can be found by considering the Newton broken line of the polynomial

$$f\Big(Y + \sum_{0\leq i<r} y_i X^{\alpha_i}\Big).$$

This is the essence of the Newton–Puiseux algorithm.

One can prove easily that $K = k((X))[y] = k'((\pi))$, where $k'$ is the field of residues of the field $K$ and $\pi = \lambda X^{1/e}$ is a uniformizing element of $K$ and $0 \neq \lambda^e \in k$. The field $k'$ is a finite extension of $k$ and is generated over $k$ by all the elements $\lambda^{-e\alpha_i} y_i$ (actually by

2010 *Mathematics Subject Classification.* Primary 16W60.

*Key words and phrases.* Newton broken lines, nonzero characteristic of the ground field, generalization of the Newton–Puiseux expansions.

a finite number of them). For the degree we have $[k' : k] \le d$. The degree of the minimal polynomial of the element $y$ over $k((X))$ is equal to $e[k' : k]$.

In what follows we suppose that $\mathrm{char}(k) = p > 0$. It is natural the think that any generalization of the Newton–Puiseux algorithm to the case of nonzero characteristic of the ground field is again an algorithm of factoring polynomials from $k((X))[Y]$ over the field $\Omega_0$. This generalization must use some extension of the method of the Newton broken lines to the case of nonzero characteristic of the ground field.

But, in comparison with the case where $\mathrm{char}(k) = 0$, some difficulties arise. First, the field $\Omega = \overline{k((X))}$ cannot be described in a simple way. Moreover, let $y \in \Omega$ be a root of the polynomial $f$. Then, in general, we cannot choose an element $\pi' \in \Omega$ such that $y \in \bar{k}((\pi'))$.

However, the field $K = k((X))[y]$ has a uniformizing element $\pi$ such that $\mathrm{ord}(\pi) = 1/e$ for an integer $e \ge 1$. The residue field $k'$ of the field $K$ with respect to the restriction to $K$ of the valuation ord is a finite (not necessarily separable) extension of the field $k$. As in the case of zero characteristic, the degree of the minimal polynomial of $y$ over $k((X))$ is equal to $e[k' : k]$. There is a system of representatives $\Sigma$ of the field $k'$ in $K$. We may assume without loss of generality that $\Sigma \supset k$ and $\Sigma$ is a linear space over $k$ (in general, one cannot choose $\Sigma$ to be an algebra over $k$). Denote by $k_s$ the separable closure of the field $k$. Then $k_s \cap k' \subset K$. So, we may assume that $k_s \cap k' \subset \Sigma$. Now the root $y$ can be represented as the sum of an infinite series

$$y = \sum_{i_0 \le i \in \mathbb{Z}} y_i \pi^i, \tag{2}$$

where all $y_i$ lie in $\Sigma$, $y_{i_0} \ne 0$.

Factoring the polynomial $f$ over the field $\Omega_0$ is easily reduced to constructing, for every root $y$ of $f$, a uniformizing element $\pi$, a system of representatives $\Sigma$, and the expansion (2) (but we shall not use this in the present paper). More precisely, to obtain (2) it suffices to construct all elements $y_i \in \Sigma$ for $i_0 \le i \le 1 + \mathrm{ord}(\Delta)$ (we assume that $\mathrm{ord}(\Delta)$ is known). After that, the subsequent elements $y_i$ can be found in a simple way by using a version of the Hensel lemma, see the Appendix. Unfortunately, it is impossible to obtain at once $\Sigma$ and $\pi$ in nonzero characteristic. To overcome this difficulty, in §2 we introduce new expansions (3) with nice properties. They arise naturally and are constructed in several steps with the help of Newton broken lines, see §5. These expansions give immediately the irreducible factors of the polynomial $f$ over the field $\Omega_0$. Once expansions (3) are obtained, we can easily find $\Sigma$, $\pi$, and the expansion (2).

Actually, the construction of expansions described in §§1–3 is *canonical*. Moreover, it is natural to view the family of expansions (3) for all $q$ as a generalization to the case of nonzero characteristic of one expansion (1) for zero characteristic.

Assume that $f \in k[X, Y]$ and the field $k$ is finitely generated over a primitive subfield. It is important that in this case the complexity of the algorithm for constructing the expansions (3) is polynomial in the size of the input data and the characteristic $p$ of the field $k$ (in the sense that for every integer $N$ the approximations of order $N$, see the definition below in the Introduction, of all the coefficients of the irreducible factors of the polynomial $f$ over the field $\Omega_0$ can be found within the time polynomial in $N$, $p$ and the size of the input data). This will be proved in the second part of this paper. There we are going to establish the results in nonzero characteristic similar to those in [1] and, may be, [2] (provided this second part will not turn out to be lengthy). The main difficulty will be to estimate the size of the coefficients from $k_s$ of the factors of the polynomial $f$ that are irreducible over $\Omega_0$.

In this paper we assume that an algorithm for factoring polynomials in one variable over finite extensions of the field $k_s$ is known in advance. If the field $k$ is finitely generated over a primitive subfield, then such an algorithm can easily be obtained from the algorithm of factoring polynomials over the algebraic closure $\bar{k}$ described in [3]. We shall discuss this issue in more detail in the second part of the paper.

Now we need some notation. Let

$$\psi = \sum_{\substack{0\le i\le \deg_Y \psi,\\ j\ge j_0}} \psi_{i,j} Y^i X^{j/\nu} \in \Omega_0[Y]$$

be an arbitrary polynomial with coefficients $\psi_{i,j} \in k_s$; the integer $\nu \ge 1$ is assumed minimal possible and $j_0$ is an integer. Set

$$\operatorname{ord}(\psi) = \inf\big\{j/\nu \,:\, \psi_{i,j} \ne 0 \;\&\; 0 \le i \le \deg_Y \psi \;\&\; j \ge j_0\big\}.$$

Therefore, $j_0 \in \mathbb{Z}\cup\{+\infty\}$, and we may take $j_0 = \operatorname{ord}(\psi)\nu$ if $\psi \ne 0$. Let $N$ be an integer. We define a polynomial $\psi_{\#,N} \in k_s(X^{1/\nu})[Y]$ by the formula

$$\psi_{\#,N} = \sum_{\substack{0\le i\le \deg_Y \psi,\\ j_0\le j\le N\nu}} \psi_{i,j} Y^i X^{j/\nu}.$$

In a natural sense, $\psi_{\#,N}$ is an approximation to the polynomial $\psi$. If $N < j_0$, then $\psi_{\#,N} = 0$.

If $\psi \in k_s[X^{1/\nu}, Y]$, then, by definition,

$$\deg_X \psi = \max\big(\{-1\} \cup \{j/\nu \,:\, \psi_{i,j} \ne 0 \;\&\; 0 \le i \le \deg_Y \psi \;\&\; j \ge 0\}\big).$$

Let $x \in \overline{k((X))}$. We shall say that $\widetilde{x} \in \overline{k((X))}$ is an approximation of $x$ of order $N$ if and only if $\operatorname{ord}(x - \widetilde{x}) \ge N + 1$.

Denote by $F \in \Omega_0[Y]$ the minimal polynomial of the root $y$ over the field $\Omega_0$. We shall assume that the leading coefficient $\operatorname{lc}_Y F$ equals 1. Now we are able to formulate the main result of the first part of the paper. Put $K_0 = \Omega_0 \cap k((X))[y]$. Then $K_0$ is the maximal weakly ramified extension of the field $k((X))$ contained in $k((X))[y]$.

**Theorem 1.** *Assume that an algorithm for factoring the polynomials over finite extensions of the field $k_s$ is known. Then we suggest an algorithm for factoring the polynomials from $k[X,Y]$ over the field $\Omega_0$ by using a generalization of the Newton broken lines method. More precisely, suppose that a polynomial $f \in k[X,Y]$ with leading coefficient $\operatorname{lc}_Y f = 1$ is separable as an element of $k(X)[Y]$, see above. Then for every root $y$ of $f$ and every integer $N \ge 0$ one can construct the polynomial $F_{\#,N}$.*

*The construction of $F$ is based on the new expansions* (3) *introduced in the paper and related to the root $y$. They enjoy properties* (i)–(xviii), *see* §§1–3 (*and give a lot of information*). *These expansions are canonical. They depend only on the element $y$ and do not depend on the polynomial $f$.*

*In particular, using the expansions* (3), *one can construct a uniformizing element of the field $k((X))[y]$ over $K_0$ and a system of generators with the multiplication table of the purely inseparable extension $k' \supset k' \cap k_s$ of fields. Actually, in the notation introduced in the next sections, a uniformizing element is obtained immediately by using $g_{q_y^*}$, and the system of generators of the extension $k' \supset k' \cap k_s$ is equal to $\overline{\eta}_1, \dots, \overline{\eta}_{w(q_y^*)}$.*

Finally, we would like to distinguish the lemmas important for justification of the construction described in this paper. These are Lemma 5 and Lemma 9. Of course, what is most important in the paper is the algorithm itself described in §5. This algorithm is natural but is not so simple as it may seem at the first glance.

## §1. The main expansions

Let $f \in k[[X]][Y]$ be a polynomial from the Introduction and let $y \in \overline{k((X))}$ be a root of $f$. We fix an integer $N \geq 0$. We shall find approximations of order $N$ of some elements of $\overline{k((X))}$ (this is the meaning of $N$). We shall see that the expansions introduced in this paper and satisfying properties (i)–(xviii), see §§1–3, are stable if $N \geq \operatorname{ord}(\Delta)/2$. Starting with §3, we shall suppose that $N \geq \operatorname{ord}(\Delta)/2$. Next, one can apply the Hensel lemma, see the Appendix, to the constructed approximations to obtain irreducible factors of the polynomial $f$ over the field $\Omega_0$ if $N \geq (3/2)\operatorname{ord}(\Delta)$. Actually, in what follows we do not need the Hensel lemma. Instead, one can enlarge $N$ and use the algorithm suggested in the paper to get better approximations of the irreducible factors of $f$.

Now we are going to describe the construction of expansions related to the root $y$ of the polynomial $f$. The detailed algorithm for this construction if $f \in k[X, Y]$ will be given in §5. It employs a generalization of the method of Newton broken lines.

We proceed to the description of this construction (it is purely mathematical; at present we do not focus on its algorithmic aspects). We shall obtain a finite number of elements $g_1, g_2, \dots, \eta_1, \eta_2, \dots$ (they depend on $y$) of the field $\Omega$ with the following properties. For every $m$, we have

$$\operatorname{ord}(\eta_m) = 0, \quad \operatorname{ord}(g_m) = a_m/(b_m p^{s_m})$$

for some integers $a_m$, $b_m$, $s_m$ with $b_m \geq 1$, $s_m \geq 0$, $\operatorname{GCD}(a_m, p) = 1$, $\operatorname{GCD}(b_m, p) = 1$, and $s_m > s_{m-1}$ (we put $s_0 = 0$). Next, for every $m$ we denote by $\bar{\eta}_m$ the residue of the element $\eta_m$. The field $k_s[\bar{\eta}_1, \dots, \bar{\eta}_m]$ is purely inseparable over the field $k_s$ and has the degree $p^{r_m}$ over $k_s$, where $1 \leq r_m \in \mathbb{Z}$ and $r_m > r_{m-1}$ (we put $r_0 = 0$).

Set $w(0) = v(0) = w(1) = v(1) = 0$, $\widetilde{y}_1 = y$. At the beginning of the $q$th step of our construction the elements $g_1, g_2, \dots, g_v$, $\eta_1, \eta_2, \dots, \eta_w$, and $\widetilde{y}_q$ from the field $\Omega$ are known. Here $1 \leq q \leq q_y^*$. So, there are $q_y^*$ steps in the construction considered. We shall write $v = v(q)$, $w = w(q)$. We have

$$v(q-1) \leq v(q) \leq v(q-1) + 1, \quad w(q-1) \leq w(q) \leq w(q-1) + 1,$$
$$(v(q-1), w(q-1)) \neq (v(q), w(q)) \quad \text{for} \quad q \geq 2.$$

Therefore, the sequences $v(0), v(1), v(2) \dots$ and $w(0), w(1), w(2), \dots$ are finite, monotone, and nondecreasing.

Put $u_q = s_{v(q)} - s_{v(q-1)} + r_{w(q)} - r_{w(q-1)}$.

We denote

$$\mathbb{Q}' = \{\beta_1/\beta_2 \in \mathbb{Q} : \beta_1, \beta_2 \in \mathbb{Z} \ \&\ \operatorname{GCD}(\beta_2, p) = 1 \ \&\ \beta_2 \geq 1\}$$

and, for integers $1 \leq v \leq v(q_y^*)$ and $1 \leq w \leq w(q_y^*)$,

$$J_w = \{(j_1, \dots, j_w) \in \mathbb{Z}^w : 0 \leq j_m < p^{r_m - r_{m-1}} \ \text{ for all } \ 1 \leq m \leq w\},$$
$$I_v = \{(i_1, \dots, i_v) \in \mathbb{Z}^v : 0 \leq i_m < p^{s_m - s_{m-1}} \ \text{ for all } \ 1 \leq m \leq v\}.$$

Set $I_0 = J_0 = \{(\ )\}$, i.e., these are singletons; here the element $(\ )$ is the 0-tuple.

**Definition 1.** Let $1 \leq w \leq w(q_y^*)$ be an integer. Suppose that $w = w(q) > w(q-1)$ for some integer $q \geq 2$ (obviously for every $w$, there is a unique integer $q$ with this property). Then we put $\rho'(w) = v(q-1)$.

Let $1 \leq m \leq v(q_y^*)$ be an integer. Then we put

$$\rho(m) = \inf\{w \in \mathbb{Z} : m \leq \rho'(w) \ \&\ 1 \leq w \leq w(q_y^*)\}.$$

Hence, if there is no integer $w$ such that $\rho'(w)$ is defined and $m \leq \rho'(w)$, then $\rho(m) = +\infty$.

The following statements can be proved easily:

- $\rho'(w) \geq 0$ for every $1 \leq w \leq w(q_y^*)$;
- the sequence $\rho'(1), \rho'(2), \ldots, \rho'(w(q_y^*))$ is monotone nondecreasing;
- the sequence $\rho(1), \rho(2), \ldots, \rho(v(q_y^*))$ is monotone nondecreasing;
- if $1 \leq m \leq v(q_y^*)$ and $1 \leq w \leq w(q_y^*)$, then the inequalities $m \leq \rho'(w)$ and $\rho(m) \leq w$ are equivalent.

**Lemma 1.** *Assume that $q \geq 2$ and only the sequences $v(0), \ldots, v(q) = v$, $w(0), \ldots, w(q) = w$ are known (these sequences are known at the beginning of the $q$th step of our construction). Let $1 \leq m \leq v$ be an integer. Then one can decide whether $\rho(m) > w$. If $\rho(m) \leq w$, then one can compute $\rho(m)$.*

*Proof.* This follows immediately from Definition 1. We leave the details to the reader. □

Our main expansion has the form

$$\widetilde{y}_q^{p^{u_q}} = \sum_{(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w) \in A_q} y_{\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w} X^\alpha g_1^{i_1} \cdot \ldots \cdot g_v^{i_v} \eta_1^{j_1} \cdot \ldots \cdot \eta_w^{j_w} + \widetilde{y}_{q+1} \tag{3}$$

and possesses the following properties (i)–(ix).

(i) $A_q$ is a finite (or empty) subset of $\mathbb{Q} \times \mathbb{Z}^{v+w}$.

(ii) $0 \leq j_m < p^{r_m - r_{m-1}}$ for all $1 \leq m \leq w$, i.e., $(j_1, \ldots, j_w) \in J_w$.

(iii) At the beginning of the $q$th step, for all $(j_1, \ldots, j_w) \in J_w$, $1 \leq m \leq v$, integral constants $c_{m, j_{\rho(m)}, \ldots, j_w}$ are computed. Each constant $c_{m, j_{\rho(m)}, \ldots, j_w}$ depends only on $m, j_{\rho(m)}, \ldots, j_w$ (if $\rho(m) > w$, then the sequence $j_{\rho(m)}, \ldots, j_w$ is empty).

(iv) For every $(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w) \in A_q$ we have

$$c_{m, j_{\rho(m)}, \ldots, j_w} \leq i_m < c_{m, j_{\rho(m)}, \ldots, j_w} + p^{s_m - s_{m-1}}$$

for all $1 \leq m \leq v$.

We shall explain the meaning of conditions (iii) and (iv) in §3. There we shall specify the constants $c_{m, j_{\rho(m)}, \ldots, j_w}$, introducing the additional condition (xviii) for them. See also Remark 1 in §3.

(v) $\alpha \in \mathbb{Q}'$, in other words $\alpha = \beta_1/\beta_2 \in \mathbb{Q}$, $\beta_1, \beta_2 \in \mathbb{Z}$, and $\mathrm{GCD}(\beta_2, p) = 1$.

(vi) Let $(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w) \in A_q$. Then $y_{\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w} \in k_s$. The element $y_{\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w}$ equals 0 if and only if $q = q_y^*$ and $(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w) = (N+1, 0, \ldots, 0)$ (notice that $(N+1, 0, \ldots, 0)$ is the last constructed element of $A_{q_y^*}$, see §2 for more detail). In all other cases $y_{\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w} \neq 0$.

(vii) For any pairwise distinct collections

$$(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w), (\alpha', i_1', \ldots, i_v', j_1', \ldots, j_w') \in A_q,$$

either $(j_1, \ldots, j_w) \neq (j_1', \ldots, j_w')$ or

$$\alpha + \sum_{1 \leq m \leq v} i_m a_m / (b_m p^{s_m}) \neq \alpha' + \sum_{1 \leq m \leq v} i_m' a_m / (b_m p^{s_m}).$$

(viii) If $q \neq q_y^*$, then $\mathrm{ord}(\widetilde{y}_{q+1}) < N+1$ and for every $(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w) \in A_q$ we have

$$\alpha + \sum_{1 \leq m \leq v} i_m a_m / (b_m p^{s_m}) < \max\big\{ \mathrm{ord}(\widetilde{y}_{q+1}), N+1 \big\}. \tag{4}$$

If $q = q_y^*$, then $\mathrm{ord}(\widetilde{y}_{q+1}) \geq N+1$. If

$$(N+1, 0, \ldots, 0) \neq (\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w) \in A_{q_y^*},$$

then inequality (4) holds true with $q = q_y^*$.

(ix) The number $\#A_q$ of elements of $A_q$ is maximal possible, i.e., there is no similar expansion with $A'$ in place of $A_q$ satisfying (i)–(viii) and such that $\#A' > \#A_q$.

If $\mathrm{ord}(\widetilde{y}_{q+1}) < N+1$, then, using the element $\widetilde{y}_{q+1}$, one can construct $g_{v+1}$ or $\eta_{w+1}$ (possibly, both of them), define $v(q+1)$, $w(q+1)$ and proceed to the next $(q+1)$st step. More precisely, for every $q \geq 1$, if $\mathrm{ord}(\widetilde{y}_{q+1}) < N+1$, then the following conditions and definitions (x)–(xiv) hold true.

(x) $g_{v+1} = \widetilde{y}_{q+1}$ if and only if $\mathrm{ord}(\widetilde{y}_{q+1}) \in \frac{1}{p^{s_{v+1}}}\mathbb{Q}'$ and $\mathrm{ord}(\widetilde{y}_q) \notin \frac{1}{p^{s_{v+1}-1}}\mathbb{Q}'$, where $s_{v+1}$ is an the integer with $s_{v+1} > s_v$.

(xi) Let $g_{v+1} = \widetilde{y}_{q+1}$. Then there is a unique $\alpha_{v+1} \in \mathbb{Q}'$ and unique $(i_{v+1,1}, \ldots, i_{v+1,v}) \in I_v$ such that

$$\mathrm{ord}\left(g_{v+1}^{p^{s_{v+1}-s_v}}/(X^{\alpha_{v+1}} g_1^{i_{v+1,1}} \cdot \ldots \cdot g_v^{i_{v+1,v}})\right) = 0.$$

Put

$$\xi_{v+1} = g_{v+1}^{p^{s_{v+1}-s_v}}/\left(X^{\alpha_{v+1}} g_1^{i_{v+1,1}} \cdot \ldots \cdot g_v^{i_{v+1,v}}\right). \tag{5}$$

Notice here that for every $0 \leq v \leq v(q^*)-1$ there is a unique $1 \leq q \leq q_y^* - 1$ such that $g_{v+1} = \widetilde{y}_{q+1}$, so that (5) is true for all such $v$.

(xii) Suppose $g_{v+1} = \widetilde{y}_{q+1}$ and the residue $\bar{\xi}_{v+1}$ belongs to $k_s[\bar{\eta}_1, \ldots, \bar{\eta}_w]$. Then $v(q+1) = v+1$, $w(q+1) = w$.

(xiii) Suppose $g_{v+1} = \widetilde{y}_{q+1}$ and the residue $\bar{\xi}_{v+1}$ does not belong to $k_s[\bar{\eta}_1, \ldots, \bar{\eta}_w]$. Then, by definition, $h_{w+1} = \widetilde{y}_{q+1}^{p^{s_{v+1}-s_v}}$ and $\eta_{w+1} = \xi_{v+1}$. So, the integer $r_{w+1} > r_w$ is defined now. Put $\beta_{w+1} = \alpha_{v+1}$, $\iota_{w+1,m} = i_{v+1,m}$ for all $1 \leq m \leq v$. In this case $v(q+1) = v+1$, $w(q+1) = w+1$.

(xiv) Let $\mathrm{ord}(\widetilde{y}_{q+1}) \in \frac{1}{p^{s_v}}\mathbb{Q}'$. Then by definition we put $h_{w+1} = \widetilde{y}_{q+1}$. Now there is a unique $\beta_{w+1} \in \mathbb{Q}'$ and unique $(\iota_{w+1,1}, \ldots, \iota_{w+1,v}) \in I_v$ such that

$$\mathrm{ord}\left(h_{w+1}/\left(X^{\beta_{w+1}} g_1^{\iota_{w+1,1}} \cdot \ldots \cdot g_v^{\iota_{w+1,v}}\right)\right) = 0.$$

Put

$$\eta_{w+1} = h_{w+1}/\left(X^{\beta_{w+1}} g_1^{\iota_{w+1,1}} \cdot \ldots \cdot g_v^{\iota_{w+1,v}}\right). \tag{6}$$

Then the residue $\bar{\eta}_{w+1}$ does not belong to $k_s[\bar{\eta}_1, \ldots, \bar{\eta}_w]$. Therefore, we see that the integer $r_{w+1} > r_w$ is defined now. In this case $v(q+1) = v$, $w(q+1) = w+1$.

Notice that (6) is satisfied if one of conditions (xiii) or (xiv) is fulfilled, i.e., if and only if $w(q+1) = w(q)+1$. Moreover, in this case $v = \rho'(w+1)$ in (6).

In either of the cases (xii) or (xiii) we represent

$$\bar{\xi}_{v+1}^{p^{r_{w(q+1)}-r_{w(q)}}} = \sum_{(j_1,\ldots,j_w)\in J_w} \xi_{v+1,j_1,\ldots,j_w} \bar{\eta}_1^{j_1} \cdot \ldots \cdot \bar{\eta}_w^{j_w} \tag{7}$$

where all $\xi_{v+1,j_1,\ldots,j_w}$ belong to $k_s$ (to avoid ambiguity, if $w = 0$ we use the notation $\xi_{v+1,}$ for $\xi_{v+1,j_1,\ldots,j_w}$).

In either of the cases (xiii) or (xiv) we represent

$$\bar{\eta}_{w+1}^{p^{r_{w(q+1)}-r_{w(q)}}} = \sum_{(j_1,\ldots,j_w)\in J_w} \eta_{w+1,j_1,\ldots,j_w} \bar{\eta}_1^{j_1} \cdot \ldots \cdot \bar{\eta}_w^{j_w} \tag{8}$$

where all $\eta_{w+1,j_1,\ldots,j_w}$ belong to $k_s$ (to avoid ambiguity, if $w = 0$ we use the notation $\eta_{w+1,}$ for $\eta_{w+1,j_1,\ldots,j_w}$).

So, in case (xiii) we have $\xi_{v+1,j_1,\ldots,j_w} = \eta_{w+1,j_1,\ldots,j_w}$ for all $(j_1, \ldots, j_w) \in J_w$, and therefore, the representations (7) and (8) coincide.

Put $k_{s,m} = k_s[\bar{\eta}_1, \ldots, \bar{\eta}_m]$ for every $1 \leq m \leq w(q_y^*)$. Then using relations (8) for $w = 0, \ldots, m-1$, one can obtain the multiplication table for the basis

$$\bar{\eta}_1^{j_1} \cdot \ldots \cdot \bar{\eta}_m^{j_m}, \quad 0 \leq j_n < p^{r_n - r_{n-1}}, \quad 1 \leq n \leq m, \tag{9}$$

of the field $k_{s,m}$ over $k_s$ (actually $(j_1,\dots,j_m)\in J_m$ in (9)). The basis (9) will be called the standard basis of the field $k_{s,m}$ over $k_s$. We put $k_{s,0}=k_s$.

Note also that if $q\ge 2$ and $A_1=\varnothing$, then $g_1=y$ or $h_1=y$.

Finally,

(xv) let $\operatorname{ord}(\widetilde{y}_{q+1})\ge N+1$. Then the $q$th step under consideration is final. We put $q_y^*=q$ in this case.

## §2. More details about the construction of the main expansion

Let us describe in more detail how to obtain the expansion (3) at the $q$th step (where $1\le q\le q_y^*$) of our construction (at present everything depends on $y$). In what follows in this section, we shall suppose that the integers $c_{m,j_{\rho(m)},\dots,j_w}$, $(j_1,\dots,j_w)\in J_w$, $1\le m\le v$, are arbitrary but fixed, where $v=v(q)$, $w=w(q)$, and $1\le q\le q^*$. We shall specify these integers $c_{m,j_{\rho(m)},\dots,j_w}$ in the next section.

For all $(j_1,\dots,j_w)\in J_w$, we put

$$I_{v,j_1,\dots,j_w}=\big\{(i_1,\dots,i_v)\in\mathbb{Z}^v\,:\,c_{m,j_{\rho(m)},\dots,j_w}\le i_m<c_{m,j_{\rho(m)},\dots,j_w}+p^{s_m-s_{m-1}}\quad\forall m\ (1\le m\le v)\big\}.$$

Set $\widetilde{A}_0=\varnothing$. We shall suppose that the finite set of multiindices (of different lengths) $\widetilde{A}_{q-1}=\bigcup_{1\le m\le q-1}A_m$ is constructed at the $(q-1)$st step of the first recursion or $q=1$. Here we need a second recursion on a set $A\supset\widetilde{A}_{q-1}$ for finding the expansion (3). We shall say that *$A$ determines the step of the second recursion at the $q$th step of the first recursion*. We shall also say that this step of the second recursion corresponds to $A$.

If $q=1$, it may happen that this second recursion has no steps. In this case $A_1=\varnothing$ and $\widetilde{A}_1=\varnothing$.

The set $A$ is also constructed recursively at the previous steps. At the first step of this second recursion we have $A=\widetilde{A}_{q-1}$. At the end of recursion we obtain the set $\widetilde{A}_q$. Actually, $A\subset\widetilde{A}_q$ and $A\ne\widetilde{A}_q$ at the beginning of any step, and $A=\widetilde{A}_q$ at the end of the final step of this recursion. We have $A_q=\widetilde{A}_q\setminus\widetilde{A}_{q-1}$, where $A_q$ is as in §1.

Let $A$ determine the step of the second recursion at the $q$th step of the first recursion, or $A=\widetilde{A}_q$. Then we put

$$\widetilde{y}_{q,A}=\widetilde{y}_q^{\,p^{u_q}}-\sum_{(\alpha,i_1,\dots,i_v,j_1,\dots,j_w)\in A\setminus\widetilde{A}_{q-1}}y_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w}X^\alpha g_1^{i_1}\cdot\ldots\cdot g_v^{i_v}\eta_1^{j_1}\cdot\ldots\cdot\eta_w^{j_w}\tag{10}$$

and $\widetilde{y}_A=\widetilde{y}_{q,A}$ if $A\setminus\widetilde{A}_{q-1}\ne\varnothing$. Set $\widetilde{y}_\varnothing=y$.

We suppose that the elements $y_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w}$ are known for all

$$(\alpha,i_1,\dots,i_v,j_1,\dots,j_w)\in A\setminus\widetilde{A}_{q-1}$$

at the beginning of the step of the second recursion corresponding to the subset $A$. At the end of that step we obtain a set $A_+\supsetneqq A$ and the expansion (10) with $A_+$ in place of $A$. If the step corresponding to $A$ is not final, then the next step of the second recursion corresponds to $A_+$ (in place of $A$).

If the step corresponding to $A$ is final, then we put $\widetilde{A}_q=A_+$ and obtain the element $\widetilde{y}_{q+1}$ by replacing $A$ with $\widetilde{A}_q$ on the right-hand side of (10). So, $\widetilde{y}_{q+1}=y_{q,\widetilde{A}_q}$. Put $y_{\widetilde{A}_q}=y_{q,\widetilde{A}_q}$.

If $q=q_y^*$, then at the final step of the second recursion we have $\operatorname{ord}(\widetilde{y}_A)\ge N+1$. There is only one step when the last inequality is true. Only in this case it may happen that $\widetilde{y}_A=0$.

If $\operatorname{ord}(\widetilde{y}_{q,A}) < N+1$ and $A$ determines the step of the second recursion at the $q$th step of the first recursion, then we assume that the conditions (xvi) and (xvii) formulated below are fulfilled.

(xvi) $a = \operatorname{ord}(\widetilde{y}_{q,A}) \in \frac{1}{p^{s_v}}\mathbb{Q}'$, where $v = v(q)$ (in particular, this automatically implies that $\widetilde{y}_{q,A} \neq 0$).

Hence, there are unique $\alpha \in \mathbb{Q}'$ and $(\iota_1, \dots, \iota_v) \in I_v$ such that

$$a = \alpha + \iota_1 \operatorname{ord} g_1 + \dots + \iota_v \operatorname{ord} g_v. \tag{11}$$

Therefore,

$$\operatorname{ord}\left(\widetilde{y}_{q,A}/(X^{\alpha} g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})\right) = 0 \tag{12}$$

(here $\alpha$, $\iota_1, \dots, \iota_v$ depend on $q, A$). Putting $\eta_{q,A} = \widetilde{y}_{q,A}/(X^{\alpha} g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})$, we denote by $\overline{\eta}_{q,A}$ the residue of the element $\eta_{q,A}$.

(xvii) The residue $\overline{\eta}_{q,A}$ belongs to $k[\overline{\eta}_1, \dots, \overline{\eta}_w]$, where $w = w(q)$.

Notice that if $A = \widetilde{A}_{q-1}$, $\operatorname{ord}(\widetilde{y}_{q,A}) < N+1$, and $q \geq 2$, then conditions (xvi) and (xvii) are fulfilled, and therefore, $\widetilde{A}_{q-1}$ determines the step of the second recursion at the $q$th step of the first recursion.

**Lemma 2.** *Let $0 \leq v \leq v(q_y^*)$ be an integer. Then (5) with $m$ in place of $v+1$ is true for every $1 \leq m \leq v$. We shall view all $s_1, \dots, s_v$ and $i_{m_1,m_2}$ as constants. Assume that $\operatorname{ord}(X^{\gamma} g_1^{n_1} \cdot \ldots \cdot g_v^{n_v}) = 0$ for some $\gamma \in \mathbb{Q}'$ and some integers $n_1, \dots, n_v$. Then there are integers $a_1, \dots, a_v$ such that*

$$X^{\gamma} g_1^{n_1} \cdot \ldots \cdot g_v^{n_v} = \xi_1^{a_1} \cdot \ldots \cdot \xi_v^{a_v}, \tag{13}$$

*and for every $1 \leq m \leq v$ the integer $a_m p^{s_m - s_{m-1}} - n_m$ depends only on $n_{m+1}, \dots, n_v$. Therefore, the integer $a_m$ depends only on $n_m, \dots, n_v$ for every $1 \leq m \leq v$.*

*Proof.* We shall suppose without loss of generality that $v \geq 1$. Since

$$\operatorname{ord}(X^{\gamma} g_1^{n_1} \cdot \ldots \cdot g_v^{n_v}) = 0,$$

we have $n_v = p^{s_v - s_{v-1}} a_v$ for an integer $a_v$. Now by (5) with $v$ in place of $v+1$ we can write $X^{\gamma} g_1^{n_1} \cdot \ldots \cdot g_v^{n_v} = X^{\gamma'} g_1^{n_1'} \cdot \ldots \cdot g_{v-1}^{n_{v-1}'} \xi_v^{a_v}$ for some $\gamma' \in \mathbb{Q}'$ and some integers $n_1', \dots, n_{v-1}'$. Here each $n_m' - n_m$, $1 \leq m \leq v-1$, depends only on $n_v$. Obviously $a_v p^{s_v - s_{v-1}} - n_v = 0$. We have $\operatorname{ord}\left(X^{\gamma'} g_1^{n_1'} \cdot \ldots \cdot g_{v-1}^{n_{v-1}'}\right) = 0$. Therefore, the required assertion is obtained by induction on $v$. □

**Corollary 1.** *Under the conditions of Lemma 2, let $0 \leq w \leq w(q_y^*)$ be an integer. Then identity (6) with $(n, \rho'(n))$ in place of $(w+1, v)$ is true for every $1 \leq n \leq w$. We view all $r_1, \dots, r_w$ and $\iota_{m_1,m_2}$ as constants. Suppose that $\operatorname{ord}(X^{\delta} g_1^{i_1} \cdot \ldots \cdot g_v^{i_v} h_1^{j_1} \cdot \ldots \cdot h_w^{j_w}) = 0$ for some $\delta \in \mathbb{Q}'$ and some integers $i_1, \dots, i_v$, $j_1, \dots, j_w$. Then there are integers $a_1, \dots, a_v$ such that*

$$X^{\delta} g_1^{i_1} \cdot \ldots \cdot g_v^{i_v} h_1^{j_1} \cdot \ldots \cdot h_w^{j_w} = \xi_1^{a_1} \cdot \ldots \cdot \xi_v^{a_v} \eta_1^{j_1} \cdot \ldots \cdot \eta_w^{j_w}, \tag{14}$$

*and for every $1 \leq m \leq v$ the integer $a_m$ depends only on $i_m, \dots, i_v$ and $j_{\rho(m)}, \dots, j_w$.*

*Proof.* Recall that the inequalities $m \leq \rho'(n)$ and $\rho(m) \leq n$ are equivalent. Hence, by (6), $\iota_{n,m} \neq 0$ only if $\rho(m) \leq n$. Thus, the required assertion follows immediately from Lemma 2 and identity (6). □

**Lemma 3.** (a) *Let $v = v(q)$, $w = w(q)$, $1 \leq q \leq q_y^*$, and let $a \in (1/p^{s_v})\mathbb{Q}'$ be an arbitrary number (not necessarily $a = \operatorname{ord}(\widetilde{y}_{q,A})$). Then for every $(j_1, \dots, j_w) \in J_w$ there are unique*

$(i_1,\dots,i_v)\in I_{v,j_1,\dots,j_w}$ *and* $\beta\in\mathbb{Q}'$ *such that* $a=\operatorname{ord}(X^\beta g_1^{i_1}\cdot\ldots\cdot g_v^{i_v})$. *More precisely, there is a function* $\varkappa:\frac{1}{p^{s_v}}\mathbb{Q}'\times J_w\to\mathbb{Q}'\times\mathbb{Z}^v$ *such that* $(\beta,i_1,\dots,i_v)=\varkappa(a,j_1,\dots,j_w)$.

(b) *Moreover, assume also that* $v\ge 1$, $(j_1,\dots,j_w)\in J_w$, *and the elements* $g_1,\dots,g_v$ *and the constants* $c_{m,j_{\rho(m)},\dots,j_w}$ *are fixed for all* $1\le m\le v$. *Then for every* $1\le m\le v$ *the integer* $i_m$ *depends only on* $\operatorname{ord}(\widetilde{y}_{q,A})$ *and* $c_{m,j_{\rho(m)},\dots,j_w},\dots,c_{v,j_{\rho(v)},\dots,j_w}$. *The integer* $\beta$ *depends only on*

$$\operatorname{ord}(\widetilde{y}_{q,A}),\quad c_{1,j_{\rho(1)},\dots,j_w},\dots,c_{v,j_{\rho(v)},\dots,j_w}.$$

*Proof.* This is straightforward by the Chinese remainder theorem applied $v$ times. □

Recall that $k_{s,0}=k_s$ and $k_{s,m}=k_s[\overline{\eta}_1,\dots,\overline{\eta}_m]$, $1\le m\le w(q_y^*)$.

**Definition 2.** Let $1\le v\le v(q_y^*)$ be an integer. Put

$$\chi(v)=\min\{m:\overline{\xi}_v\in k_{s,m}\ \&\ m\ge 0\}.$$

Then $0\le\chi(v)\in\mathbb{Z}$.

**Lemma 4.** *If* $1\le v\le v(q_y^*)$, *then* $\chi(v)<\rho(v)$.

*Proof.* The sequences $v(0),v(1),v(2)\dots$ and $w(0),w(1),w(2)\dots$ are monotone nondecreasing. We shall use this fact below.

Let $q\ge 2$ be the smallest integer such that $v=v(q)$. By Definition 2, $\overline{\xi}_v\in k[\overline{\eta}_1,\dots,\overline{\eta}_{w(q')}]$ for some $1\le q'\le q$ with $\chi(v)=w(q')$.

On the other hand, let $\rho(v)=w<+\infty$. By Definition 1, $v\le\rho'(w)=v(q''-1)$ for an integer $q''\ge 2$ such that $w=w(q'')>w(q''-1)$. Hence, $v(q)\le v(q''-1)$. Now $q\le q''-1$ because $q$ is the smallest integer such that $v=v(q)$. Thus,

$$\chi(v)=w(q')\le w(q)\le w(q''-1)<w(q'')=w=\rho(v).$$

The lemma is proved. □

Recall that (11) and (12) hold true. In assertion (a) of the following lemma the number $a\in(1/p^{s_v})\mathbb{Q}'$ is arbitrary (not necessarily $a=\operatorname{ord}(\widetilde{y}_{q,A})$). For this $a$, there are unique $\alpha\in\mathbb{Q}'$ and $(\iota_1,\dots,\iota_v)\in I_v$ such that (11) is fulfilled (here we use the same notation $\alpha$, $\iota_1,\dots,\iota_v$ as in the case where $a=\operatorname{ord}(\widetilde{y}_{q,A})$; this will not lead to any ambiguity).

**Lemma 5.** (a) *Let* $v=v(q)$, $w=w(q)$, $1\le q\le q_y^*$. *Suppose* $a\in(1/p^{s_v})\mathbb{Q}'$ *is arbitrary and* (11) *holds true. Put*

$$B_{a,v,w}=\big\{X^{\beta-\alpha}g_1^{i_1-\iota_1}\cdot\ldots\cdot g_v^{i_v-\iota_v}\eta_1^{j_1}\cdot\ldots\cdot\eta_w^{j_w}:\ (j_1,\dots,j_w)\in J_w\ \&\ (\beta,i_1,\dots,i_v)=\varkappa(a,j_1,\dots,j_w)\big\}.$$

*Then the family of residues* $\{\overline{\eta}\}_{\eta\in B_{a,v,w}}$ *is a basis of the field* $k_s[\overline{\eta}_1,\dots,\overline{\eta}_w]$ *over* $k_s$.

(b) *Assume that conditions* (xvi) *and* (xvii) *are fulfilled. Then there are unique* $y_{\beta,i_1,\dots,i_v,j_1,\dots,j_w}\in k_s$ *with* $(\beta,i_1,\dots,i_v)=\varkappa(\operatorname{ord}(\widetilde{y}_{q,A}),j_1,\dots,j_w)$ *for all* $(j_1,\dots,j_w)\in J_w$ *such that*

$$\operatorname{ord}\Big(\widetilde{y}_{q,A}-\sum_{\substack{(j_1,\dots,j_w)\in J_w,\\(\beta,i_1,\dots,i_v)=\varkappa(a,j_1,\dots,j_w)}}y_{\beta,i_1,\dots,i_v,j_1,\dots,j_w}X^\beta g_1^{i_1}\cdot\ldots\cdot g_v^{i_v}\eta_1^{j_1}\cdot\ldots\cdot\eta_w^{j_w}\Big)>\operatorname{ord}(\widetilde{y}_{q,A}).\tag{15}$$

*Proof.* Assertion (b) follows from (a) immediately.

We prove (a). We shall suppose without loss of generality that $v\ge 1$. By Lemma 3, each $i_m-\iota_m$, $1\le m\le v$, depends only on $c_{m,j_{\rho(m)},\dots,j_w},\dots,c_{v,j_{\rho(v)},\dots,j_w}$ and $\operatorname{ord}(\widetilde{y}_{q,A})$.

We have $\operatorname{ord}(X^{\beta-\alpha}g_1^{i_1-\iota_1}\cdot\ldots\cdot g_v^{i_v-\iota_v})=0$. By Lemma 2, we can write

$$X^{\beta-\alpha}g_1^{i_1-\iota_1}\cdot\ldots\cdot g_v^{i_v-\iota_v}=\xi_1^{a_1}\cdot\ldots\cdot\xi_v^{a_v},$$

where $a_m$ is an integer depending only on $i_m - \iota_m, \dots, i_v - \iota_v$ for every $1 \le m \le v$.

Therefore, $a_m$ depends only on $c_{m,j_{\rho(m)},\dots,j_w}, \dots, c_{v,j_{\rho(v)},\dots,j_w}$ and $\operatorname{ord}(\widetilde{y}_{q,A})$ for every $1 \le m \le v$.

Set

$$\lambda_n = \prod_{\substack{\chi(m)=n,\\ 1\le m\le v}} \xi_m^{a_m}, \quad 0 \le n \le w.$$

Notice that each $a_m$ in the last product does not depend on $j_1, \dots, j_{\rho(m)-1}$. By Lemma 4, we have $\rho(m) - 1 \ge \chi(m) = n$. Hence, each $a_m$ in the last product does not depend on $j_1, \dots, j_n$. Therefore, also the product $\lambda_n$ itself does not depend on $j_1, \dots, j_n$. To specify the dependence of $\lambda_n$ on $j_{n+1}, \dots, j_w$, we shall write $\lambda_n = \lambda_n(j_{n+1}, \dots, j_w)$ ($\lambda_n$ also depends on $a$, but this does not matter at present).

Denote by $\overline{\lambda}_n(j_{n+1}, \dots, j_w)$ the residue of the element $\lambda_n(j_{n+1}, \dots, j_w)$. Then $0 \ne \overline{\lambda}_n(j_{n+1}, \dots, j_w) \in k_{s,n}$.

Now we write

$$X^{\beta-\alpha} g_1^{i_1-\iota_1} \cdot \ldots \cdot g_v^{i_v-\iota_v} \eta_1^{j_1} \cdot \ldots \cdot \eta_w^{j_w} = \lambda_0(j_1, \dots, j_w) \prod_{1\le n\le w} \left(\eta_n^{j_n} \lambda_n(j_{n+1}, \dots, j_w)\right). \tag{16}$$

Let $1 \le t \le w$ be an integer. Let $\mathcal{A}(t)$ denote the following claim. The family $\prod_{t\le n\le w} (\overline{\eta}_n^{j_n} \overline{\lambda}_n(j_{n+1}, \dots, j_w))$, $0 \le j_n < p^{r_n - r_{n-1}}$, $t \le n \le w$, is a basis of the field $k_{s,w}$ over $k_{s,t-1}$.

We are going to prove $\mathcal{A}(1)$ with the help of decreasing induction on $t$. The base $\mathcal{A}(w)$ of induction is obvious. Assume that $t \ge 1$ and that $\mathcal{A}(t+1)$ is proved. Then

$$\overline{\eta}_t^{j_{t+1}} \prod_{t+1\le n\le w} \left(\overline{\eta}_n^{j_n} \overline{\lambda}_n(j_{n+1}, \dots, j_w)\right),$$
$$0 \le j_t \le p^{r_t - r_{t-1}}, \quad 0 \le j_n < p^{r_n - r_{n-1}}, \quad t+1 \le n \le w,$$

is a basis of the field $k_{s,w}$ over $k_{s,t-1}$.

The family $\overline{\eta}_t^{j_t} \overline{\lambda}_t(j_{t+1}, \dots, j_w)$, $0 \le j_t < p^{r_t - r_{t-1}}$, is a basis of the field $k_{s,t}$ over $k_{s,t-1}$ because $0 \ne \overline{\lambda}_t(j_{t+1}, \dots, j_w) \in k_{s,t}$. Therefore, for every $(j_{t+1}, \dots, j_w)$ the linear space over $k_{s,t-1}$ generated by the family

$$\overline{\eta}_t^{j_t} \prod_{t+1\le n\le w} \left(\overline{\eta}_n^{j_n} \overline{\lambda}_n(j_{n+1}, \dots, j_w)\right), \quad 0 \le j_t \le p^{r_t - r_{t-1}},$$

coincides with the linear space over $k_{s,t-1}$ generated by the family

$$\overline{\eta}_t^{j_t} \overline{\lambda}_t(j_{t+1}, \dots, j_w) \prod_{t+1\le n\le w} \left(\overline{\eta}_n^{j_n} \overline{\lambda}_n(j_{n+1}, \dots, j_w)\right), \quad 0 \le j_t \le p^{r_t - r_{t-1}}$$

(both are subspaces of the field $k_{s,w}$). This implies $\mathcal{A}(t)$ immediately.

Thus, $\mathcal{A}(1)$ is true. Hence, the family

$$\prod_{1\le n\le w} \left(\overline{\eta}_n^{j_n} \overline{\lambda}_n(j_{n+1}, \dots, j_w)\right), \quad (j_1, \dots, j_w) \in J_w,$$

is a basis of the field $k_{s,w}$ over $k_s$. For every $(j_1, \dots, j_w) \in J_w$, multiplying the element of this basis that corresponds to $(j_1, \dots, j_w)$ by a nonzero constant $\overline{\lambda}_0(j_1, \dots, j_w)$, we obtain again a basis of $k_{s,w}$ over $k_s$. This last basis coincides with the family $\{\overline{\eta}\}_{\eta\in B_{a,v,w}}$ by (16). Assertion (a) and the lemma are proved. □

We return to the case where $A$ determines the step of the second recursion at the $q$th step of the first recursion. First, suppose that $a = \operatorname{ord}(\widetilde{y}_{q,A}) < N + 1$. Then, by our

assumption, see above, conditions (xvi) and (xvii) are fulfilled. Put

$$A' = \big\{(\beta, i_1, \dots, i_v, j_1, \dots, j_w) : (j_1, \dots, j_w) \in J_w \ \&\ (\beta, i_1, \dots, i_v) = \varkappa(a, j_1, \dots, j_w)\big\}. \tag{17}$$

Then by Lemma 5 (b), all the elements $y_{\beta,i_1,\dots,i_v,j_1,\dots,j_w} \in k_s$ with $(\beta, i_1, \dots, i_v, j_1, \dots, j_w) \in A'$ are well defined and (15) holds true. Set

$$A'' = \big\{(\beta, i_1, \dots, i_v, j_1, \dots, j_w) \in A' : y_{\beta,i_1,\dots,i_v,j_1,\dots,j_w} \neq 0\big\}. \tag{18}$$

Then $A'' \neq \varnothing$ because $\widetilde{y}_{q,A} \neq 0$. Put $A_+ = A \cup A''$. Now we have one of the following two subcases (a) and (b).

(a) Recall that the element $\widetilde{y}_{q,A_+}$ is defined, see the beginning of the section. Assume that conditions (xvi) and (xvii) are fulfilled with $\widetilde{y}_{q,A_+}$ in place of $\widetilde{y}_{q,A}$ (the residue $\overline{\eta}_{q,A_+}$ is defined by analogy with $\overline{\eta}_{q,A}$ if condition (xvi) is fulfilled with $\widetilde{y}_{q,A_+}$ in place of $\widetilde{y}_{q,A}$; in what follows we shall omit the words "in place of $\widetilde{y}_{q,A}$" for brevity). Then we replace $A$ by $A_+$ and proceed to the next step of the second recursion at the $q$th step of the first recursion. Notice that in this subcase we do not suppose that necessarily $\operatorname{ord}(\widetilde{y}_{q,A_+}) < N + 1$.

(b) Assume that it is not true that conditions (xvi) and (xvii) are fulfilled for $\widetilde{y}_{q,A_+}$. Then the step of the second recursion corresponding to $A$ is final. In this subcase we put $\widetilde{A}_q = A_+$, $A_q = \widetilde{A}_q \setminus \widetilde{A}_{q-1}$, $\widetilde{y}_{q+1} = \widetilde{y}_{q,A_+}$. Now, by items (xii), (xiii), and (xiv) in §1, we pass to the $(q+1)$st step of the first recursion.

More precisely, in subcase (b) either condition (xvi) is fulfilled for $\widetilde{y}_{q,A_+}$ and condition (xvii) is not fulfilled for $\widetilde{y}_{q,A_+}$ or condition (xvi) is not fulfilled for $\widetilde{y}_{q,A_+}$. Therefore, in subcase (b) either $\operatorname{ord}(\widetilde{y}_{q,A_+}) \in \frac{1}{p^{s_v}}\mathbb{Q}'$ and the element $\overline{\eta}_{q,A_+}$ does not lie in $k_s[\overline{\eta}_1, \dots, \overline{\eta}_w]$, or $\operatorname{ord}(\widetilde{y}_{q,A_+}) \notin \frac{1}{p^{s_v}}\mathbb{Q}'$ and $\widetilde{y}_{q,A_+} \neq 0$. Moreover, by Lemma 9 (see §3 below), in subcase (b) if additionally condition (xviii) holds true, then $\operatorname{ord}(\widetilde{y}_{q+1}) \leq \operatorname{ord}(\Delta)/2$.

Now suppose that $\operatorname{ord}(\widetilde{y}_{q,A}) \geq N + 1$ (possibly, $\widetilde{y}_{q,A} = 0$) and $A$ determines the step of the second recursion at the $q$th step of the first recursion. Then the step of the second recursion corresponding to $A$ is final. Put $A_+ = A \cup \{(N+1, 0, \dots, 0)\}$ and $y_{N+1,0,\dots,0} = 0$, where $(N+1, 0, \dots, 0) \in \mathbb{Q}' \times \mathbb{Z}^{v+w}$. Set $\widetilde{y}_{q,A_+} = \widetilde{y}_{q,A}$, $\widetilde{y}_{q+1} = \widetilde{y}_{q,A_+}$, $\widetilde{A}_q = A_+$, $A_q = \widetilde{A}_q \setminus \widetilde{A}_{q-1}$, and $q^*_y = q$, see item (xv) in §1. Here the construction is canonical, but may seem slightly artificial. However, we shall see that for $q = q^*_y$ and $\operatorname{ord}(\widetilde{y}_{q,A}) \geq N+1$ such a final step (or some similar one) will be necessary in §5 to define the leaf of the tree $T$, see §4 below, corresponding to the root $y$.

Also, it may happen that $\operatorname{ord}(\widetilde{y}_{q,A}) < N + 1$ but the conditions of Lemma 5 (b) are not fulfilled for $\widetilde{y}_{q,A}$ with $A = \widetilde{A}_{q-1}$. Then we are not able to find $A_+$ at the $q$th step. But obviously, in this case $q = 1$ and $A = \widetilde{A}_0 = \varnothing$. Then, in accordance with items (x)–(xiv), see the end of §1, we put $\widetilde{A}_1 = \varnothing$, construct $g_1$ or $\eta_1$ (maybe both of them) and proceed to step 2 of the first recursion.

Thus, we have finished the description of the construction of expansion (3) in this section. More information on this expansion will be given in §5 with the help of the method of Newton broken lines.

We need also the following definitions. Let $1 \leq q \leq q^*_y$. Denote by $S'_{y,q}$ the set of all $A$ such that the set $A$ determines the step of the second recursion at the $q$th step of the first recursion, see the beginning of the section. Therefore, $S'_{y,q_1} \cap S'_{y,q_2} = \varnothing$ for all $1 \leq q_1 \neq q_2 \leq q^*_y$.

Observe that $S'_{y,q} \neq \varnothing$ for $q \geq 2$. For every $1 \leq q \leq q^*_y$, if $S'_{y,q} \neq \varnothing$ then $\widetilde{A}_{q-1} \in S'_{y,q}$, but $\widetilde{A}_q \notin S'_{y,q}$, whence $A_q \neq \varnothing$ in this case.

For every $1 \le q \le q_y^*$ we put

$$S_{y,q} = \{\widetilde{A}_q\} \cup \bigcup_{1 \le m \le q} S'_{y,m}, \qquad S_y = \{\widetilde{A}_{q_y^*}\} \cup \bigcup_{1 \le q \le q_y^*} S'_{y,q}.$$

Set $S_{y,0} = \{\widetilde{A}_0\} = \{\varnothing\}$, $S_{y,-1} = \varnothing$ (so that $\#S_{y,0} = 1$, $\#S_{y,-1} = 0$).

Notice that also $S_y = \bigcup_{1 \le q \le q_y^*} S_{y,q}$.

For every $0 \le q \le q_y^*$ and every $A \in S_{y,q} \setminus S_{y,q-1}$ we put $s_A = s_{v(q)}$, $r_A = r_{w(q)}$.

## §3. Modified expansions

In this and the following sections we suppose that $N \ge \operatorname{ord}(\Delta)/2$. Consider the main expansion (3) obtained at the $q$th step of our construction. Recall that $v = \rho'(w+1)$ in (3). Put

$$c'_{m,j_{\rho(m)},\dots,j_w} = c_{m,j_{\rho(m)},\dots,j_w} - \sum_{\rho(m) \le n \le w} j_n \iota_{n,m}, \quad 1 \le m \le v,$$

see (6) with $(n, \rho'(n))$ in place of $(w+1, v)$ for the definition of $\iota_{n,m}$. Recall that the conditions $m \le \rho'(n)$ and $\rho(m) \le n$ are equivalent. We substitute the expressions for $\eta_n$, $1 \le n \le w$, from (6) (with $(n, \rho'(n))$ in place of $(w+1, v)$) in the expansion (3). Then we get the modified expansion

$$\widetilde{y}_q^{p^{u_q}} = \sum_{(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A'_q} y'_{\alpha, i_1, \dots, i_v, j_1, \dots, j_w} X^\alpha g_1^{i_1} \cdot \ldots \cdot g_v^{i_v} h_1^{j_1} \cdot \ldots \cdot h_w^{j_w} + \widetilde{y}_{q+1}, \tag{19}$$

where all $y'_{\alpha, i_1, \dots, i_v, j_1, \dots, j_w}$ are elements of $k_s$, and $\#A_q = \#A'_q$. More precisely, there is a bijection $A_q \to A'_q$,

$$(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \mapsto (\alpha', i'_1, \dots, i'_v, j_1, \dots, j_w),$$

$$i'_m = i_m - \sum_{\rho(m) \le n \le w} j_n \iota_{n,m}, \quad 1 \le m \le v,$$

$$\alpha' = \alpha - \sum_{1 \le n \le w} j_n \alpha_n.$$

such that $y'_{\alpha', i'_1, \dots, i'_v, j_1, \dots, j_w} = y_{\alpha, i_1, \dots, i_v, j_1, \dots, j_w}$ for every $(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A_q$. Hence,

$$c'_{m,j_{\rho(m)},\dots,j_w} \le i_m < c'_{m,j_{\rho(m)},\dots,j_w} + p^{s_m - s_{m-1}}, \quad 1 \le m \le v,$$

for every $(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A'_q$.

Thus, to obtain expansions (3) it suffices to construct the modified expansions (19), and conversely. Actually, we shall construct (3) and (19) simultaneously.

*In what follows in this paper we shall suppose that the following condition is fulfilled*:

(xviii) $c_{m,j_{\rho(m)},\dots,j_w} = \sum_{\rho(m) \le u \le w} j_u \iota_{u,m}$ for all $(j_1, \dots, j_w) \in J_w$, $1 \le m \le v$.

We shall see that condition (xviii) is convenient for applying our generalization of the method of Newton broken lines. Obviously, condition (xviii) is equivalent to

$$c'_{m,j_{\rho(m)},\dots,j_w} = 0, \quad \text{for all} \quad (j_1, \dots, j_w) \in J_w, \quad 1 \le m \le v. \tag{20}$$

*Remark* 1. Assume that the constants $c_{m,j_{\rho(m)},\dots,j_w}$ satisfy condition (iii) but may fail to satisfy (xviii) (say, in the important case where all $c_{m,j_{\rho(m)},\dots,j_w}$ are 0). Then, for example, one can modify the entire construction as follows. At the $q$th step of the first recursion, let $1 \le a_q \le \deg_Y f - 1$ be the smallest integer (it exists) such that the elements $\widetilde{y}_q^{a_q p^{u_q}}$, $g_1^{i_1} \cdot \ldots \cdot g_v^{i_v} \eta_1^{j_1} \cdot \ldots \cdot \eta_w^{j_w}$, $(i_1, \dots, i_v) \in I_{v,j_1,\dots,j_w}$, $(j_1, \dots, j_w) \in J_w$ are linearly independent over the field $\Omega_0$. Then one replaces $\widetilde{y}_q^{p^{u_q}}$ by $\widetilde{y}_q^{a_q p^{u_q}}$ in the expansion (3).

This replacement is necessary. Namely, the elements $\widetilde{y}q_q^{a_q p^{u_q}}$, $g_1^{i_1}\cdot\ldots\cdot g_v^{i_v}\eta_1^{j_1}\cdot\ldots\cdot\eta_w^{j_w}$, $(i_1,\ldots,i_v)\in I_{v,j_1,\ldots,j_w}$, $(j_1,\ldots,j_w)\in J_w$, must be linearly independent over the field $\Omega_0$ if the final aim is to construct $\Sigma$ and $\pi$, see the Introduction, cf. the proof of Lemma 9. Here we leave the details to the interested reader. We shall not use this remark in the paper.

**Lemma 6.** (a) *Let $v=v(q)$, $w=w(q)$, $1\le q\le q_y^*$, and let $a\in(1/p^{s_v})\mathbb{Q}'$ be an arbitrary number. Then for every $(j_1,\ldots,j_w)\in J_w$ there are unique $(i_1,\ldots,i_v)\in I_v$ and $\beta\in\mathbb{Q}'$ such that $a=\operatorname{ord}(X^\beta g_1^{i_1}\cdot\ldots\cdot g_v^{i_v}h_1^{j_1}\cdot\ldots\cdot h_w^{j_w})$. More precisely, there is a function $\varkappa' : \frac{1}{p^{s_v}}\mathbb{Q}'\times J_w\to\mathbb{Q}'\times\mathbb{Z}^v$ such that $(\beta,i_1,\ldots,i_v)=\varkappa'(a,j_1,\ldots,j_w)$. Assume that* (11) *is fulfilled. Then under condition* (xviii) *we have*

$$B_{a,v,w}=\big\{X^{\beta-\alpha}g_1^{i_1-\iota_1}\cdot\ldots\cdot g_v^{i_v-\iota_v}h_1^{j_1}\cdot\ldots\cdot h_w^{j_w}\ :\ (j_1,\ldots,j_w)\in J_w\ \&\ (\beta,i_1,\ldots,i_v)=\varkappa'(a,j_1,\ldots,j_w)\big\}.$$

(b) *Under the conditions of* (a) *assume additionally that $v'=v(q')$, $w'=w(q')$, $1\le q'\le q$, and $a\in(1/p^{s_{v'}})\mathbb{Q}'$. Then the family $B_{a,v,w}$ contains $B_{a,v',w'}$ (more precisely, $B_{a,v',w'}$ is a subfamily of $B_{a,v,w}$).*

*Proof.* This follows straightforwardly from the definitions (we leave the details to the reader). □

*Remark* 2. Put $\bar{B}_{a,v,w}=\{\overline{\eta}\}_{\eta\in B_{a,v,w}}$. Then the elements of the basis $\bar{B}_{a,v,w}$ can be presented as linear combinations of the elements of the standard basis (9) with $m=w$ by using Lemma 2 or Corollary 1 and relations (7), (8) with $(v(q'),w(q'))$, $1\le q'\le q-1$, in place of $(v,w)$.

Let $q\ge 1$, and let $(\mathrm{xii})_q$, $(\mathrm{xiii})_q$, $(\mathrm{xiv})_q$ denote conditions (xii), (xiii), (xiv) from §1, respectively.

Also, we need to introduce yet another modified expansion. Let $(\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w)\in A'_q$. For every $2\le m\le q$, we set

- $i''_m=i_{v(m)}$ if and only if condition $(\mathrm{xii})_{m-1}$ is fulfilled;
- $i''_m=i_{v(m)}+p^{s_m-s_{m-1}}j_{w(m)}$ if and only if condition $(\mathrm{xiii})_{m-1}$ is fulfilled;
- $i''_m=j_{w(m)}$ if and only if condition $(\mathrm{xiv})_{m-1}$ is fulfilled.

For every $1\le q\le q_y^*$, there is a bijection

$$A'_q\to A''_q,\quad(\alpha,i_1,\ldots,i_{v(q)},j_1,\ldots,j_{w(q)})\mapsto(\alpha,i''_2,\ldots,i''_q) \tag{21}$$

defining the set $A''_q$ (if $q=1$, the sequences $i_1,\ldots,i_{v(q)}$; $j_1,\ldots,j_{w(q)}$; $i''_2,\ldots,i''_q$ are empty). Put $y''_{\alpha,i''_2,\ldots,i''_q}=y_{\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w}$ for every $(\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w)\in A'_q$. Now for every $1\le q\le q_y^*$ we can use (19) to get the second modified expansion

$$\widetilde{y}_q^{p^{u_q}}=\sum_{(\alpha,i_2,\ldots,i_q)\in A''_q}y''_{\alpha,i_2,\ldots,i_q}X^\alpha\widetilde{y}_2^{i_2}\widetilde{y}_3^{i_3}\cdot\ldots\cdot\widetilde{y}_q^{i_q}+\widetilde{y}_{q+1} \tag{22}$$

(here if $q=1$, then the sequence $i_2,\ldots,i_q$ is empty and the product $\widetilde{y}_2^{i_2}\widetilde{y}_3^{i_3}\cdot\ldots\cdot\widetilde{y}_q^{i_q}$ is equal to 1). Notice that if $(\alpha,i_2,\ldots,i_q)\in A''_q$, then $0\le i_m<p^{u_m}$ for all $2\le m\le q$.

**Lemma 7.** (a) *Let $2\le q\le q_y^*$ or $q=1$ and $\widetilde{A}_1\ne\varnothing$. Then*

$$\operatorname{ord}(\widetilde{y}_{q+1})>p^{u_q}\operatorname{ord}(\widetilde{y}_q)\ge 0$$

*(if $\widetilde{A}_1=\varnothing$, then $\widetilde{y}_2=\widetilde{y}_1$, whence $\operatorname{ord}(\widetilde{y}_2)=p^{u_1}\operatorname{ord}(\widetilde{y}_1)$).*

(b) *If $(\alpha,i_2,\ldots,i_q)\in A''_q$ and $1\le q\le q_y^*$, then $\alpha\ge 0$.*

(c) *If* $(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A'_q$ *and* $1 \le q \le q^*_y$, *then* $\alpha \ge 0$.

*Proof.* We have $\mathrm{lc}_Y f = 1$. Hence, $y$ is integral over $k[[X]]$. Therefore, $\mathrm{ord}(y_1) \ge 0$. Now assertion (a) follows from (3) and the described construction immediately. Assertion (c) follows from (b) and the existence of the bijection (21).

It remains to prove (b). We shall suppose without loss of generality that $q \ge 2$. By (22), for every $(\alpha, i_2, \dots, i_q) \in A''_q$ we have $p^{u_q} \mathrm{ord}(\widetilde{y}_q) \le \mathrm{ord}(X^\alpha \widetilde{y}_2^{i_2} \widetilde{y}_3^{i_3} \cdot \ldots \cdot \widetilde{y}_q^{i_q})$.

Applying (a) und using induction on $2 \le n \le q$, we prove that

$$\sum_{1 \le m \le n-1} (p^{u_m} - 1) \mathrm{ord}(\widetilde{y}_m) \le \mathrm{ord}(\widetilde{y}_n) - \mathrm{ord}(\widetilde{y}_1).$$

Notice that $p^{u_1} - 1 = 0$. Hence,

$$(p^{u_q} - i_q) \mathrm{ord}(\widetilde{y}_q) \le \alpha + \sum_{1 \le m \le q-1} (p^{u_m} - 1) \mathrm{ord}(\widetilde{y}_m) \le \alpha + \mathrm{ord}(\widetilde{y}_q) - \mathrm{ord}(\widetilde{y}_1).$$

Thus, $\alpha \ge \mathrm{ord}(\widetilde{y}_1) \ge 0$ because $p^{u_q} - i_q \ge 1$. The lemma is proved. □

Recall that the last step $q^*_y$ of the construction of our expansions was defined at the end of §1. Now we are going to introduce the polynomials $P_q \in \Omega_0[Y]$, $1 \le q \le q^*_y + 1$, and $G_{v(q)}, H_{w(q)} \in \Omega_0[Y]$, $2 \le q \le q^*_y$, associated with the modified expansions (19). These polynomials will be such that

$$\widetilde{y}_q = P_q(y), \quad g_{v(q)} = G_{v(q)}(y), \quad h_{w(q)} = H_{w(q)}(y). \tag{23}$$

**Definition 3.** This definition is recursive in $q \ge 1$. Put $P_1 = Y$. Suppose that $1 \le q \le q^*_y$ and the polynomials $P_a \in \Omega_0[Y]$, $1 \le a \le q$, and $G_{v(a)}, H_{w(a)} \in \Omega_0[Y]$, $2 \le a \le q$, have already been defined. Then we put

$$P_{q+1} = P_q^{p^{u_q}} - \sum_{(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A'_q} y'_{\alpha, i_1, \dots, i_v, j_1, \dots, j_w} X^\alpha G_1^{i_1} \cdot \ldots \cdot G_v^{i_v} H_1^{j_1} \cdot \ldots \cdot H_w^{j_w}, \tag{24}$$

where $u_q = s_{v(q)} - s_{v(q-1)} + r_{w(q)} - r_{w(q-1)}$, $v = v(q)$, $w = w(q)$.

Suppose that $1 \le q < q^*_y$ and that (xii), see §1, holds true (recall that in this case we have $v(q+1) = v(q) + 1$, $w(q+1) = w(q)$). Then we put $G_{v(q+1)} = P_{q+1}$.

Suppose that $1 \le q < q^*_y$ and that (xiii) holds true (recall that $v(q+1) = v(q) + 1$, $w(q+1) = w(q) + 1$ in this case). Then we put $G_{v(q+1)} = P_{q+1}$ and $H_{w(q+1)} = P_{q+1}^{p^{s_{v+1} - s_v}}$, where $v = v(q)$.

Suppose that $1 \le q < q^*_y$ and that (xiv) holds true (recall that $v(q+1) = v(q)$, $w(q+1) = w(q) + 1$ in this case). Then we put $H_{w(q+1)} = P_{q+1}$.

Comparing (24) and (19), we see that (23) is satisfied. Note that the leading coefficients with respect to $Y$ of all the introduced polynomials $P_q$ and $G_{v(q)}, H_{w(q)}$, $q \ge 2$, are equal to 1. Next, if $q \ge 2$, then $\deg_Y G_1 = 1$ or $\deg_Y H_1 = 1$, and if additionally $\widetilde{A}_1 = \varnothing$, then $G_1 = Y$ or $H_1 = Y$, see the end of §1. Similarly, $\deg_Y P_2 = 1$, and if $\widetilde{A}_1 = \varnothing$, then $P_2 = Y$.

The definitions and (24) imply

$$P_{q+1} = P_q^{p^{u_q}} - \sum_{(\alpha, i_1, \dots, i_q) \in A''_q} y''_{\alpha, i_1, \dots, i_q} X^\alpha P_1^{i_1} \cdot \ldots \cdot P_q^{i_q} \tag{25}$$

for every $1 \le q \le q^*_y$, cf. (22).

**Lemma 8.** (a) *Suppose that* $q$ *an integer,* $1 \le q \le q^*_y$, *and* $v = v(q)$, $w = w(q)$. *Then* $\deg_Y P_{q+1} = p^{s_v + r_w}$.

(b) *Suppose that* $1 \le q < q_y^*$, $v = v(q)$, $w = w(q)$, *and* (xii) *holds true. Then* $\deg_Y G_{v+1} = p^{s_v + r_w}$.
(c) *Suppose that* $1 \le q < q_y^*$, $v = v(q)$, $w = w(q)$, *and* (xiii) *holds true. Then* $\deg_Y G_{v+1} = p^{s_v + r_w}$ *and* $\deg_Y H_{w+1} = p^{s_{v+1} + r_w}$.
(d) *Suppose that* $1 \le q < q_y^*$, $v = v(q)$, $w = w(q)$, *and* (xiv) *holds true. Then* $\deg_Y H_{w+1} = p^{s_v + r_w}$.

*Proof.* This follows straightforwardly from Definition 3. □

**Lemma 9.** (a) $\operatorname{ord}(\widetilde{y}_1) \le \operatorname{ord}(f(0))$. *If, moreover,* $y \ne 0$ *and* $f(0) = 0$, *then* $f'(0) = (\frac{d}{dY} f)(0) \ne 0$ *and* $\operatorname{ord}(\widetilde{y}_1) \le \operatorname{ord}(f'(0))$.
(b) *Let* $q_y^* \ge 2$. *Then for every* $1 \le q \le q_y^*$ *we have* $\operatorname{ord}(\widetilde{y}_q) \le \operatorname{ord}(\Delta)/2$.
(c) *If* $1 \le q < q_y^*$, *then*

$$\operatorname{ord}(\widetilde{y}_q) \le p^{-\mu_q} \operatorname{ord}(\Delta)/2, \tag{26}$$

*where*

$$\mu_q = u_q + u_{q+1} + \cdots + u_{q_y^*-1} = s_{v(q_y^*-1)} + r_{w(q_y^*-1)} - s_{v(q-1)} - r_{w(q-1)}.$$

*Inequality* (26) *is strict whenever* $q_y^* \ge 3$ *or* $\widetilde{A}_1 \ne \varnothing$.
(d) *Let* $q = q_y^*$. *Then the degree of the extension of fields satisfies*

$$[\Omega_0[y] : \Omega_0] = p^{s_{v(q)} + r_{w(q)}} = \deg_Y P_{q_y^*+1}.$$

*Proof.* Assertion (a) is obvious. Assertion (c) follows from (b) with $q = q_y^*$ and Lemma 7 (a). Therefore, it suffices to prove (b) and (d) with $q \ge 2$.

Suppose that $q_y^* \ge 2$ and $2 \le q \le q_y^* + 1$. Let $a = s_{v(q-1)} + r_{w(q-1)}$. Then $P_q = Y^{p^a} + \sum_{0 \le j < p^a} P_{q,j} Y^j$, where all the coefficients $P_{q,j}$ lie in $\Omega_0$. Let $K'$ be the maximal weakly ramified extension of the field $k((X))$ contained in the field $k((X))[y]$. Put $K = K'[P_{q,0}, \dots, P_{q,p^a-1}]$. Hence, $K$ is a finite weakly ramified extension of the field $k((X))$. Therefore, the ramification index of the extension $K[y] \supset K$ is at least $p^{s_{v(q)}}$ and the degree of inertia of this extension is at least $p^{r_{w(q)}}$. Hence, $[K[y] : K] \ge p^{s_{v(q)} + r_{w(q)}}$. The extensions $\Omega_0 \supset K$ and $K[y] \supset K$ are linearly disjoint over $K$, because $K$ is the maximal weakly ramified extension of the field $k((X))$ contained in $K[y]$. Therefore, $[\Omega_0[y] : \Omega_0] = [K[y] : K]$. Let $b = [K[y] : K]$.

Let $q \le q_y^*$. In this case $q_y^* \ge q \ge 2$. Hence, $s_{v(q)} + r_{w(q)} > s_{v(q-1)} + r_{w(q-1)}$. Thus, $p^a < p^{s_{v(q)} + r_{w(q)}}$ and $b > p^a$.

Let $q = q_y^* + 1$. In this case, assuming that $[\Omega_0[y] : \Omega_0] > p^{s_{v(q-1)} + r_{w(q-1)}}$, we also get $b > p^a$.

It remains to show that for every $2 \le q \le q_y^* + 1$ the inequality $b > p^a$ implies that $\operatorname{ord}(\widetilde{y}_q) \le \operatorname{ord}(\Delta)/2$. Indeed, then (a) follows immediately, and the contradiction $\operatorname{ord}(\widetilde{y}_{q_y^*+1}) \le \operatorname{ord}(\Delta)/2$ proves also (c).

Therefore, in the sequel in the proof we shall suppose that $b > p^a$ and $2 \le q \le q_y^* + 1$. Let $\sigma_1, \dots, \sigma_b$ be the family of all the embeddings of the field $K[y] \to \overline{k((X))}$ over the field $K$. Consider the linear system

$$\sum_{0 \le j \le b-1} \sigma_i(y)^j X_j = \sigma_i(\widetilde{y}_q), \quad 1 \le i \le b, \tag{27}$$

for the unknowns $X_i$, $0 \le i \le b-1$. It is a system with square matrix. The determinant $\delta$ of this matrix is $\prod_{1 \le i < j \le b} (\sigma_j(y) - \sigma_i(y))$. Hence, $\operatorname{ord}(\delta) \le \operatorname{ord}(\Delta)/2$. By the Cramer rule, system (27) has a unique solution $X_i = \delta_i/\delta$, and $\operatorname{ord}(\delta_i) \ge \operatorname{ord}(\widetilde{y}_q)$, $0 \le i \le b-1$.

On the other hand, since $P_q(y) = \widetilde{y}_q$ and $b > p^a$, the solution of system (27) is $X_j = P_{q,j}$, $0 \le j \le p^a - 1$, $X_{p^a} = 1$ and $X_j = 0$, $p^a < j \le b-1$. In particular, this implies that $\delta_{p^a}/\delta = 1$. Consequently,

$$\operatorname{ord}(\Delta)/2 \ge \operatorname{ord}(\delta) = \operatorname{ord}(\delta_{p^a}) \ge \operatorname{ord}(\widetilde{y}_q).$$

The lemma is proved. □

**Lemma 10.** *Let $F \in \Omega_0[Y]$ be the minimal polynomial of the root $y$ with the leading coefficient $\operatorname{lc}_Y F = 1$. Then $\operatorname{ord}(F - P_{q_y^*+1}) \ge N + 1 - \operatorname{ord}(\Delta)/2$.*

*Proof.* Let $F - P_{q_y^*+1} = \sum_{0 \le i \le b-1} \varphi_i Y^i$ where all $\varphi_i$ lie in $\Omega_0$ and $b = [\Omega_0[y] : \Omega_0]$, see Lemma 9 (d). We use the notation of the proof of Lemma 9. Put $q = q_y^* + 1$. Then system (27) has the solution $X_i = \varphi_i$, $0 \le i \le b-1$, because $F(y) = 0$ and $P_q(y) = \widetilde{y}_q$. We have $\operatorname{ord}(\delta) \le \operatorname{ord}(\Delta)/2$ (even if $q_y^* = 1$). By the Cramer rule, system (27) has a unique solution $X_i = \delta_i/\delta$, and now $\operatorname{ord}(\delta_i) \ge \operatorname{ord}(\widetilde{y}_q) \ge N + 1$, $0 \le i \le b-1$. This implies the required assertion. □

Let $A \in S_y \setminus \{\widetilde{A}_{q_y^*}\}$, see the end of §2. Then $A \in S'_{y,q}$ for some $1 \le q \le q_y^*$. Hence, the set $A_+ \in S_{y,q}$ is defined, see §2. Recall that $A_+ \setminus A = A''$, where the set $A''$ is given by (17) and (18).

The mapping $S_y \setminus \{\widetilde{A}_{q_y^*}\} \to S_y \setminus \{\varnothing\}$, $A \mapsto A_+$ is injective (recall here that $\widetilde{A}_0 = \varnothing$ and, possibly, $\widetilde{A}_1 = \varnothing$). Hence, for every set $A \in S_y \setminus \{\varnothing\}$ there is a unique set $A_- \in S_y \setminus \{\widetilde{A}_{q_y^*}\}$ such that $(A_-)_+ = A$.

Now for every set $A \in S_y \setminus \{\varnothing\}$ we are going to define polynomials $Q_A$ and $P_A$. Namely, there is a unique $1 \le q \le q_y^*$ such that $A \in S_{y,q} \setminus S_{y,q-1} = S'_{y,q} \cup \{\widetilde{A}_q\} \setminus \{\widetilde{A}_{q-1}\}$. Then $Q_A$ and $P_A$ are given by the formulas

$$Q_A = \sum_{(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A \setminus A_-} y_{\alpha, i_1, \dots, i_v, j_1, \dots, j_w} X^{\alpha'} G_1^{i'_1} \cdot \ldots \cdot G_v^{i'_v} H_1^{j_1} \cdot \ldots \cdot H_w^{j_w}, \tag{28}$$

$$P_A = P_q^{p^{u_q}} - \sum_{(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A \setminus \widetilde{A}_{q-1}} y_{\alpha, i_1, \dots, i_v, j_1, \dots, j_w} X^{\alpha'} G_1^{i'_1} \cdot \ldots \cdot G_v^{i'_v} H_1^{j_1} \cdot \ldots \cdot H_w^{j_w} \tag{29}$$

where $v = v(q)$, $w = w(q)$ and (see the beginning of this section for the definition of $\iota_{n,m}$ and $\alpha_n$)

$$i'_m = i_m - \sum_{\rho(m) \le n \le w} j_n \iota_{n,m}, \quad 1 \le m \le v, \quad \alpha' = \alpha - \sum_{1 \le n \le w} j_n \alpha_n. \tag{30}$$

Hence, also

$$P_A = P_q^{p^{u_q}} - \sum_{\{A' \in S_{y,q} \setminus S_{y,q-1} \,:\, A' \subset A\}} Q_{A'}, \tag{31}$$

and if $A_+ \in S_{y,q} \setminus S_{y,q-1}$, then $P_{A_+} = P_A - Q_{A_+}$.

Let $A \in S'_q \cup \{\widetilde{A}_q\}$. Then we set $P_{q,A} = P_A$ if $A \ne \widetilde{A}_{q-1}$ and $P_{q,A} = P_q^{p^{u_q}}$ if $A = \widetilde{A}_{q-1}$.

Put $P_\varnothing = Y$, $Q_\varnothing = 0$. Now the polynomials $P_A$, $Q_A$ are defined for all $A \in S_y$. The definitions imply that $\widetilde{y}_A = P_A(y)$ for every $A \in S_y$ and $\widetilde{y}_{q,A} = P_{q,A}(y)$ for every $A \in S'_q \cup \{\widetilde{A}_q\}$ and every $1 \le q \le q_y^*$.

Notice that if the polynomial $Q_A$ (respectively, $P_A$), $G_1, \dots, G_v$, $H_1, \dots, H_w$, and all integers $\iota_{u,m}, \alpha_u$ are known, then we can find all the coefficients $y_{\beta, i_1, \dots, i_v, j_1, \dots, j_w}$ on the right-hand side of (28) (respectively, (29)) with the help of Lemma 13, see below, and solving a linear system over the field $k''(X^{1/\nu})$.

**Lemma 11.** *Let $A \in S'_q \cup \{\widetilde{A}_q\}$, $1 \le q \le q^*_y$. Let $1 \le \nu \le d$ be the smallest integer and $k'' \subset k_s$ the smallest finite extension of $k$ such that all the polynomials $P_{q,A}, G_1, \dots, G_v, H_1, \dots, H_w$ belong to $k''((X^{1/\nu}))[Y]$. Then all these polynomials belong to the ring $k''[X^{1/\nu}, Y]$. Therefore, all the polynomials $P_1, \dots, P_q$ belong to the ring $k''[X^{1/\nu}, Y]$.*

*Proof.* This follows from Lemma 7 immediately. □

**Lemma 12.** (a) *For every $1 \le q \le q^*_y$, we have $\deg_X P_q \le p^{s_{v(q-1)}+r_{w(q-1)}} \operatorname{ord}(\Delta)/2$.*
(b) *If $q = q^*_y + 1$, then*

$$\deg_X P_q \le N + 1 + (p^{s_{v(q-1)}+r_{w(q-1)}} - 1)\operatorname{ord}(\Delta)/2.$$

*Proof.* We shall use induction on $q$ and (22), (25). If $q = 1$, then $\deg_X P_q = 0$ and the claim is trivial. If $q = 2$, then everything follows from Lemma 9 with $q = 2$ and (22), (25) with $q = 1$.

Assume that $q \ge 3$ and the lemma is proved for $q - 1$. Consider identity (25) with $q-1$ in place of $q$. Then $0 \le \alpha$ by Lemma 7 (b) and $\alpha \le \operatorname{ord}(\Delta)/2$ by Lemma 9 for every $(\alpha, i_1, \dots, i_{q-1}) \in A''_{q-1}$. Recall that $0 \le i_m \le p^{u_m} - 1$ for every $1 \le m \le q-1$ and every $(\alpha, i_1, \dots, i_{q-1}) \in A''_{q-1}$. Write $\alpha' = \alpha - \operatorname{ord}(\Delta)/2$. Now by the inductive assumption for every $(\alpha, i_1, \dots, i_{q-1}) \in A''_{q-1}$ we have

$$\begin{aligned}
\deg_X(X^\alpha P_2^{i_2} \cdot \ldots \cdot P_{q-1}^{i_{q-1}}) &= \alpha + \sum_{2 \le m \le q-1} i_m \deg_X P_m \\
&\le \alpha' + \operatorname{ord}(\Delta)/2 + \sum_{2 \le m \le q-1} (p^{u_m} - 1) p^{s_{v(m-1)}+r_{w(m-1)}} \operatorname{ord}(\Delta)/2 \\
&= \alpha' + \Big(p^{s_{v(1)}+r_{w(1)}} + \sum_{2 \le m \le q-1} (p^{s_{v(m)}+r_{w(m)}} - p^{s_{v(m-1)}+r_{w(m-1)}})\Big)\operatorname{ord}(\Delta)/2 \\
&= \alpha' + p^{s_{v(q-1)}+r_{w(q-1)}} \operatorname{ord}(\Delta)/2.
\end{aligned}$$

Notice that $\alpha' \le 0$ if $3 \le q \le q^*_y$ and $\alpha' \le N + 1 - \operatorname{ord}(\Delta)/2$ if $q = q^*_y + 1$. Similarly, the inductive assumption implies

$$\deg_X(P_{q-1}^{p^{u_{q-1}}}) \le p^{s_{v(q-1)}+r_{w(q-1)}} \operatorname{ord}(\Delta)/2,$$

and the required assertions follow. The lemma is proved. □

**Lemma 13.** *Let $1 \le q \le q^*_y$ be an integer, and let $v = v(q)$, $w = w(q)$. Let $A \in S'_{y,q} \cup \{\widetilde{A}_q\}$, see the end of §2. Let $k'' \subset k_s$ be the least finite extension of the field $k$ and $\nu \ge 1$, $\operatorname{GCD}(\nu, p) = 1$, the smallest integer such that all the polynomials $P_{q,A}$, $G_1, \dots, G_v, H_1, \dots, H_w$ lie in $k''[X^{1/\nu}, Y]$, see Lemma 11. Then for every integer $b \ge 0$ the family*

$$\begin{aligned}
&G_1^{i_1} G_2^{i_2} \cdot \ldots \cdot G_v^{i_v} H_1^{j_1} H_2^{j_2} \cdot \ldots \cdot H_w^{j_w} P_{q,A}^a, \\
&0 \le i_m < p^{s_m - s_{m-1}}, \quad 1 \le m \le v; \quad 0 \le j_m < p^{r_m - r_{m-1}}, \quad 1 \le m \le w; \\
&0 \le a \le b/p^{s_v + r_w}, \quad a \in \mathbb{Z},
\end{aligned} \tag{32}$$

*is a basis of the $k''[X^{1/\nu}]$-module of polynomials $\psi \in k''[X^{1/\nu}, Y]$ of degree $\deg_Y \psi \le b$ (this module is free over $k''[X^{1/\nu}]$). Moreover, for every integer $0 \le b' \le b$ there is a unique element of the family (32) such that*

$$b' = a \deg_Y P_{q,A} + \sum_{1 \le m \le v} i_m \deg_Y G_m + \sum_{1 \le m \le w} j_m \deg_Y H_m.$$

*Proof.* The leading coefficient with respect to $Y$ of each polynomial in the family (32) is equal to 1. Hence, it suffices to prove the last assertion of the lemma. Moreover, let $\mathcal{A}_q$ denote the following assertion. For every integer $0 \le b' < p^{s_{v(q)}+r_{w(q)}}$ there is a unique element of the family (32) with $a = 0$ such that

$$b' = \sum_{1\le m\le v} i_m \deg_Y G_m + \sum_{1\le m\le w} j_m \deg_Y H_m.$$

Obviously, the last assertion of the lemma is equivalent to $\mathcal{A}_q$. We shall prove $\mathcal{A}_q$ using induction on $q$. The base $q = 1$ is obvious. Note also that the uniqueness of the required element in $\mathcal{A}_q$ follows automatically from its existence, because the number of elements of the family (32) with $a = 0$ is equal to $p^{s_{v(q)}+r_{w(q)}}$.

Assume that $q \ge 2$ and assertion $\mathcal{A}_{q-1}$ is proved. We prove $\mathcal{A}_q$. Observe that now one of conditions $(\mathrm{xii})_{q-1}$, $(\mathrm{xiii})_{q-1}$, and $(\mathrm{xiv})_{q-1}$ is fulfilled. Suppose that condition $(\mathrm{xii})_{q-1}$ is fulfilled. Then $v(q) = v(q-1)+1$, $w(q) = w(q-1)$, $u_q = p^{s_{v(q)}-s_{v(q-1)}}$, and by Lemma 8 we have $\deg_Y G_{v(q)} = p^{s_{v(q-1)}+r_{w(q-1)}}$. Now it suffices to prove the following claim. Assume that

$$0 \le \lambda(p^{s_{v(q-1)}+r_{w(q-1)}}) < p^{s_{v(q)}+r_{w(q)}} \tag{33}$$

for an integer $\lambda$. Then there is an integer $0 \le i < p^{s_{v(q)}-s_{v(q-1)}}$ such that

$$\lambda(p^{s_{v(q-1)}+r_{w(q-1)}}) = i \deg G_{v(q)}.$$

But this follows immediately from the relations $u_q = p^{s_{v(q)}-s_{v(q-1)}}$ and $\deg_Y G_{v(q)} = p^{s_{v(q-1)}+r_{w(q-1)}}$.

Suppose that condition $(\mathrm{xiii})_{q-1}$ is fulfilled. Hence, $v(q) = v(q-1)+1$, $w(q) = w(q-1)+1$, and by Lemma 8 we have $\deg_Y G_{v(q)} = p^{s_{v(q-1)}+r_{w(q-1)}}$ and $\deg_Y H_{w(q)} = p^{s_{v(q)}+r_{w(q-1)}}$. Now it suffices to prove the following claim. Under condition (33), there are integers $0 \le i < p^{s_{v(q)}-s_{v(q-1)}}$ and $0 \le j < p^{r_{w(q)}-r_{w(q-1)}}$ such that $\lambda(p^{s_{v(q-1)}+r_{w(q-1)}}) = i \deg_Y G_{v(q)} + j \deg_Y H_{v(q)}$. Again, this is straightforward.

Finally, suppose that condition $(\mathrm{xiv})_{q-1}$ is fulfilled. Hence, $v(q) = v(q-1)$, $w(q) = w(q-1)+1$, $u_q = p^{r_{w(q)}-r_{w(q-1)}}$, and by Lemma 8 we have $\deg_Y H_{w(q)} = p^{s_{v(q-1)}+r_{w(q-1)}}$. Now it suffices to prove the following claim. Under condition (33), there is an integer $0 \le j < p^{r_{w(q)}-r_{w(q-1)}}$ such that $\lambda(p^{s_{v(q-1)}+r_{w(q-1)}}) = j \deg_Y H_{v(q)}$. Again, this is straightforward. The lemma is proved. □

Under the conditions of Lemma 11, we are going to describe the ideal of relations between $G_1, \dots, G_v$, $H_1, \dots, H_w$ and $P_{q,A}$. Let $Z_1, \dots, Z_v$, $Y_1, \dots, Y_w$, $Z$ be new variables, where $v = v(q)$, $w = w(q)$. Then the ring $R = k''[X^{1/\nu}][Z_1, \dots, Z_v, Y_1, \dots, Y_w, Z]$ is defined. We introduce the $k''[X^{1/\nu}]$-algebra $R/\mathcal{J}_q$, where $\mathcal{J}_q$ is an ideal of $R$. We shall describe the generators of $\mathcal{J}_q$. We put $X_{m+1} = Z_{v(m+1)}$ if and only if condition $(\mathrm{xii})_m$ or condition $(\mathrm{xiii})_m$ is fulfilled and $1 \le m \le q-1$. Put $X_{m+1} = Y_{w(m+1)}$ if and only if condition $(\mathrm{xiv})_m$ is fulfilled and $1 \le m \le q-1$. Let $J_{\mathrm{xiii}}$ denote the set of all $2 \le m \le q$ such that condition $(\mathrm{xiii})_{m-1}$ is fulfilled. Then the ideal $\mathcal{J}_q$ has the following family of generators:

$$\sum_{\substack{(\alpha,i_1,\dots,i_{v(m)},\\ j_1,\dots,j_{w(m)})\in A'_m}} y_{\alpha,i_1,\dots,i_{v(m)},j_1,\dots,j_{w(m)}} X^\alpha Z_1^{i_1} \cdot \ldots \cdot Z_{v(m)}^{i_{v(m)}} \cdot Y_1^{j_1} \cdot \ldots \cdot Y_{w(m)}^{j_{w(m)}} + X_{m+1} - X_m^{p^{u_m}}, \quad 2 \le m \le q-1, \tag{34}$$

$$Y_{w(m)} - Z_{v(m)}^{p^{s_{v(m)}-s_{v(m-1)}}}, \quad m \in J_{\mathrm{xiii}}, \tag{35}$$

$$\sum_{(\alpha,i_1,\dots,i_v,j_1,\dots,j_w)\in A\setminus\widetilde{A}_{q-1}} y_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w} X^{\alpha'} Z_1^{i'_1} \cdot \ldots \cdot Z_v^{i'_v} \cdot Y_1^{j_1} \cdot \ldots \cdot Y_w^{j_w} + Z - X_q^{p^{u_q}}. \tag{36}$$

where $\alpha'$, $i'_1, \dots, i'_v$ are defined by (30).

**Corollary 2.** *Under the previous conditions, there is an isomorphism of $k''[X^{1/\nu}]$-algebras*

$$k''[X^{1/\nu}][Z_1, \dots, Z_v, Y_1, \dots, Y_w, Z]/\mathcal{J}_q \to k''[X^{1/\nu}, Y] \tag{37}$$

*induced by the the homomorphism of rings of polynomials*

$$R \to k''[X^{1/\nu}, Y], \quad Z_i \mapsto G_i, \ \ 1 \le i \le v, \quad Y_j \mapsto H_j, \ \ 1 \le j \le w, \quad Z \mapsto P_{q,A}.$$

*Proof.* This is straightforward. □

## §4. Trees corresponding to expansions of roots of the polynomial $f$

Put $q^* = \max\{q^*_y : y \text{ is a root of } f\}$. Recall that the sets of multiindices $S_{y,q}$, $S_y$ and, for every $A \in S_y$, the integers $s_A$ and $r_A$ were defined at the end of §2. Put

$$S_{y,A} = \big\{A' \in S_y \,:\, A' \subset A\big\} \ \text{ for every } \ A \in S_y,$$
$$V_{y,A} = \big\{(A', Q, a) \,:\, A' \in S_{y,A} \,\&\, Q = Q_{A'} \,\&\, a = s_{A'} + r_{A'},\big\} \ \text{ for every } \ A \in S_y,$$

where $Q_{A'}$, $s_{A'}$, $r_{A'}$ correspond to the root $y$ in accordance with our construction. Notice that $S_{y,A}$ is a linearly ordered set with respect to the inclusion of sets. Namely, for arbitrary $A', A'' \in S_{y,A}$ we put $A' \le A''$ if and only if $A' \subset A''$. The element $A$ is maximal in $S_{y,A}$ with respect to this order.

Similarly $V_{y,A}$ is a linearly ordered set. Namely, for arbitrary $(A', Q, a), (A'', Q', a') \in V_{y,A}$ we put $(A', Q, a) \le (A'', Q', a')$ if and only if $A' \subset A''$. The element $(A, Q_A, a) \in V_{y,A}$ is maximal in $V_{y,A}$ with respect to this order.

Set

$$T_{y,q} = \{V_{y,A} \,:\, A \in S_{y,q}\}, \qquad 1 \le q \le q^*_y,$$
$$T_y = \{V_{y,A} \,:\, A \in S_y\},$$
$$T_q = \bigcup_{y \text{ is a root of } f} T_{y,\min\{q^*_y, q\}}, \qquad 1 \le q \le q^*,$$
$$T = \bigcup_{y \text{ is a root of } f} T_y.$$

Observe that if $A \in S_{y,q}$, then $S_A \subset S_{y,q}$. Hence,

$$T_y = \bigcup_{1 \le q \le q^*_y} T_{y,q} \ \text{ and } \ T = \bigcup_{1 \le q \le q^*} T_q.$$

We shall view each $T_q$, $1 \le q \le q^*$, and, respectively, $T$ as the set of vertices of a tree. Namely, if $\tau_1, \tau_2 \in T_q$ (respectively, $\tau_1, \tau_2 \in T$), then $\tau_2$ is a son of $\tau_1$ if and only if the number of elements $\#(\tau_2 \setminus \tau_1)$ is equal to 1, i.e., if and only if the difference $\tau_2 \setminus \tau_1$ is a singleton.

Thus, *par abuse de langage*, in what follows we shall call each $T_q$ (respectively, $T$) a tree. More generally, we shall identify other trees with the sets of their vertices if this will not lead to ambiguity.

The root $\tau_0$ of each tree $T_q$ and $T$ is equal to $\{(\varnothing, 0, 0)\}$ (recall that $\widetilde{A}_0 = \varnothing$ and, possibly, $\widetilde{A}_1 = \varnothing$ for every root $y$ of the polynomial $f$).

Denote by $L(T)$ the set of all leaves of the tree $T$.

In the next lemma we prove auxiliary assertions. In fact, they are straightforward, and the reader may skip the detailed proof of this lemma.

**Lemma 14.** (a) *Let $\tau \in T$, $\tau \neq \tau_0$, so that $\tau = V_{y,A}$, where $A \in S_{y,q} \setminus S_{y,q-1}$ for some root $y$ of the polynomial $f$ and an integer $1 \leq q \leq q^*_y$.*

*We claim that the following objects depend only on $\tau$ and do not depend on the choice of the root $y$ and the set $A$. These are the sets $A$, $S_{y,A}$, the integers $q$ and*

$$v(1), \dots, v(q), \quad w(1), \dots, w(q), \quad s_1, \dots, s_{v(q)}, \quad r_1, \dots, r_{w(q)},$$

*the polynomials*

$$P_1, \dots, P_q, \quad G_1, \dots, G_{v(q)}, \quad H_1, \dots, H_{w(q)}, \quad Q_{A'}, \quad A' \in S_{y,A},$$

*the rational numbers*

$$\begin{aligned} &\operatorname{ord}(P_m(y)), \ 1 \leq m \leq q, \qquad \operatorname{ord}(Q_{A'}(y)), \quad A' \in S_{y,A}, \\ &\operatorname{ord}(g_m), \ 1 \leq m \leq v(q), \qquad \operatorname{ord}(h_m), \ 1 \leq m \leq w(q), \end{aligned}$$

*the elements*

$$(\alpha_m, i_{m,1}, \dots, i_{m,m-1}), \quad 1 \leq m \leq v(q), \tag{38}$$

$$(\beta_m, \iota_{m,1}, \dots, \iota_{m,\rho'(q)}), \quad 1 \leq m \leq w(q), \tag{39}$$

*the families of coefficients*

$$y_{\alpha,i_1,\dots,i_{v(q)},j_1,\dots,j_{w(m)}}, \ (\alpha, i_1, \dots, i_{v(q)}, j_1, \dots, j_{w(m)}) \in A \setminus \widetilde{A}_{q-1}, \tag{40}$$

$$y_{\alpha,i_1,\dots,i_{v(m)},j_1,\dots,j_{w(m)}}, \ (\alpha, i_1, \dots, i_{v(m)}, j_1, \dots, j_{w(m)}) \in A_m, \quad 1 \leq m \leq q-1, \tag{41}$$

$$y_{\alpha,i_1,\dots,i_{v(m)},j_1,\dots,j_{w(m)}}, \ (\alpha, i_1, \dots, i_{v(m)}, j_1, \dots, j_{w(m)}) \in A' \setminus (A')_-, \quad A' \subset A, \quad A' \in S_{y,m} \setminus S_{y,m-1}, \quad 1 \leq m \leq q, \tag{42}$$

*and the residues*

$$\overline{\xi}_1, \dots, \overline{\xi}_{v(q)}, \qquad \overline{\eta}_1, \dots, \overline{\eta}_{w(q)}. \tag{43}$$

*Moreover, the residues* (43) *are given by the corresponding recursive relations* (7) *and* (8)*, and these relations depend only on $\tau$ and do not depend on the choice of the root $y$ and the set $A$.*

(b) *An element $\tau \in T$ is a leaf of the tree $T$ if and only if we have $A = \widetilde{A}_q \in S_y$ and $q = q^*_y$ for some choice of the root $(y, A)$ corresponding to $\tau$ (see the beginning of the statement of the lemma). If $\tau$ is a leaf of the tree $T$, then the above relations are fulfilled also for any other similar choice of these elements. In this case, the polynomial $P_{q^*_y+1}$ is defined. Again, it does not depend on the choice of $(y, A)$.*

*Proof.* We prove (a). We have the natural mapping $\pi : \tau \to \pi(\tau)$, $(A', P, a) \mapsto A'$. Therefore, the set $S_{y,A} = \pi(\tau)$ does not depend on the choice of $(y, A)$. The set $A$ is a maximal element of $S_{y,A}$ with respect to inclusion of sets, see above, and hence $A$ depends only on $\tau$ and does not depend on the choice of $(y, A)$.

For every $A' \in S_{y,A}$ and every $x \in A'$ the element $x$ belongs to $\mathbb{Q}' \times \mathbb{Z}^{m-1}$ for an integer $m \geq 1$. Put $\sigma'(x) = m$. Set $\sigma(A') = \max(\{\sigma'(x) : x \in A'\} \cup \{0\})$. In accordance with our construction and the definitions, the number of elements $\#\sigma(S_{y,A})$ is equal to $q+1$ if and only if $\widetilde{A}_1 \neq \varnothing$. Otherwise, $\#\sigma(S_{y,A}) = q$. Notice that $\widetilde{A}_1 \neq \varnothing$ if and only if $(\varnothing, Q, 0) \in \tau$ for some nonzero $Q$. Therefore, $q$ depends only on $\tau$.

Let $\sigma(S_{y,A}) = \{\sigma_0, \sigma_1 \dots, \sigma_q\}$, where $0 = \sigma_0 \leq \sigma_1 < \sigma_2 < \dots < \sigma_q$ ($\sigma_0 = \sigma_1$ if $\#\sigma(S_{y,A}) = q$). Then $\widetilde{A}_m$, $0 \leq m \leq q-1$, is the maximal element (with respect to inclusion) of the set $\{A' \in S_{y,A} : \sigma(A') = m\}$. Hence, each set $\widetilde{A}_m$, $0 \leq m \leq q-1$, does not depend on the choice of $(y, A)$.

Using induction on $q$, we may assume that assertion (a) of the lemma holds true for $q-1$ in place of $q$ or $q=1$ ($q=1$ is the base of induction). Now, if $q\ge 2$, we can apply the inductive assumption to the set $\widetilde{A}_{q-1}$, which does not depend on the choice of $(y,A)$. Therefore, the set $S_{y,\widetilde{A}_{q-1}}=S_{y,q-1}$ does not depend on the choice of $(y,A)$. If $q\ge 3$, then, similarly, the set $S_{y,\widetilde{A}_{q-2}}=S_{y,q-2}$ does not depend on the choice of $(y,A)$. If $q=2$, the set $S_{y,q-2}=\{\varnothing\}$ also does not depend on the choice of $(y,A)$.

We have $P_1=Y$. Let $u_{q-1}=s_{v(q-1)}-s_{v(q-2)}+r_{w(q-1)}-r_{w(q-2)}$, $2\le q\le q_y^*$. Then

$$P_q=P_{q-1}^{p^{u_{q-1}}}-\sum_{A'\in S_{y,q-1}\setminus S_{y,q-2}}Q_{A'},\quad 2\le q\le q_y^*,$$

see (31) with $A=\widetilde{A}_{q-1}$. Hence, by the inductive assumption, the polynomial $P_q$ does not depend on the choice of $(y,A)$.

Let $q_1$ be an integer such that $2\le q_1\le q$ or $1\le q_1\le q$ and $\widetilde{A}_1\ne\varnothing$. Then by the conditions of the lemma we have $A\supset(\widetilde{A}_{q_1-1})_+\supsetneqq\widetilde{A}_{q_1-1}$. Hence, the element $(\widetilde{A}_{q_1-1})_+$ is minimal in $S_{y,A}\setminus S_{y,q_1-1}$, and therefore, it depends only on $\tau$ and does not depend on the choice of $(y,A)$.

Let $(\alpha,i_1,\dots,i_v,j_1,\dots,j_w)\in(\widetilde{A}_{q_1-1})_+\setminus\widetilde{A}_{q_1-1}$. Notice here that if $v=v(q)>v(q-1)$, then $i_v=0$ because $\operatorname{ord}(P_{q_1}^{p^{u_{q_1}}}(y))\in(1/p^{s_{v(q_1-1)}})\mathbb{Q}'$, see (23) and the end of §1. Next, $s_{v(q_1)}+r_{w(q_1)}=s_{A'}+r_{A'}$, where $A'=\widetilde{A}_{q_1}$ if $q_1<q$ and $A'=A$ if $q_1=q$. Therefore, $s_{v(q_1)}+r_{w(q_1)}$ does not depend on the choice of $(y,A)$. Consequently, $u_q$ does not depend on the choice of $(y,A)$. Now, see the end of §2, by Lemma 5 (b) we have

$$\operatorname{ord}(P_{q_1}^{p^{u_{q_1}}}(y))=\alpha+\sum_{1\le m\le v(q_1-1)}i_m\operatorname{ord}(g_m),$$

which does not depend on on the choice of $(y,A)$ by the inductive assumption. Therefore, $\operatorname{ord}(P_{q_1}(y))$ does not depend on on the choice of $(y,A)$.

We show that also $\operatorname{ord}(P_1(y))$ does not depend on on the choice of $(y,A)$. Indeed, it suffices to consider the case where $\widetilde{A}_1=\varnothing$. Then $q\ge 2$, $P_1=Y$, and $P_2=Y^{p^{u_1}}=Y$, $\operatorname{ord}(P_1(y))$ does not depend on the choice of $(y,A)$.

On the other hand, our construction shows that

$$\operatorname{ord}(P_q^{p^{u_q}}(y))\in p^{-s_{v(q-1)}+r_{w(q)}-r_{w(q-1)}}\mathbb{Q}',$$
$$\operatorname{ord}(P_q^{p^{u_q}}(y))\notin p^{-s_{v(q-1)}+r_{w(q)}-r_{w(q-1)}+1}\mathbb{Q}'.$$

Therefore, using the inductive assumption, we see that $r_{w(q)}$ does not depend on the choice of $(y,A)$. Hence, also $s_{v(q)}$ does not depend on the choice of $(y,A)$.

Now we use the definitions to prove that $\operatorname{ord}(g_m)$, $1\le m\le v(q)$, and $\operatorname{ord}(h_m)$, $1\le m\le w(q)$, do not depend on the choice of $(y,A)$. By the construction described in §1 and §2 this implies that the elements (38), (39) do not depend on the choice of $(y,A)$.

To obtain relations (7) and (8), we use the polynomials $Q_{(\widetilde{A}_m)_+}$, $1\le m\le q-1$. By the recursive assumption, relations (7) and (8) with $(v(m),w(m))$, $1\le m\le q-2$, in place of $(v,w)$ depend only on $\tau$ and do not depend on the choice of $(y,A)$.

It remains to consider the case where $m=q-1$. The definitions imply that

$$Q_{(\widetilde{A}_{q-1})_+}(y)=\sum_{(\gamma,i_1,\dots,i_v,j_1,\dots,j_w)\in(\widetilde{A}_{q-1})_+\setminus\widetilde{A}_{q-1}}y_{\gamma,i_1,\dots,i_v,j_1,\dots,j_w}X^\gamma g_1^{i_1}\cdot\ldots\cdot g_v^{i_v}\xi_1^{j_1}\cdot\ldots\cdot\xi_w^{j_w}.$$

We have $\operatorname{ord}(P_q^{p^{u_q}}(y)-Q_{(\widetilde{A}_{q-1})_+}(y))>\operatorname{ord}(P_q^{p^{u_q}}(y))$ and

$$\operatorname{ord}(P_q^{p^{u_q}}(y))=\gamma+i_1\operatorname{ord}(g_1)+\dots+i_v\operatorname{ord}(g_v)$$

for every $(\gamma,i_1,\dots,i_v,j_1,\dots,j_w)\in(\widetilde{A}_{q-1})_+\setminus\widetilde{A}_{q-1}$.

We put $(\delta, n_1, \dots, n_v) = (\alpha_v, i_{v,1}, \dots, i_{v,v-1}, 0)$ whenever $(\mathrm{xii})_{q-1}$ or $(\mathrm{xiii})_{q-1}$ is true and $(\delta, n_1, \dots, n_v) = (\beta_w, i_{w,1}, \dots, i_{w,v})$ if $(\mathrm{xiv})_{q-1}$ is true. Then

$$P_q^{p^{u_q}}(y)/(X^\delta g_1^{n_1} \cdot \ldots \cdot g_v^{n_v})^{p^{r_{w(q)} - r_{w(q-1)}}} \tag{44}$$

is equal to $\xi_v^{p^{r_{w(q)} - r_{w(q-1)}}}$ if $(\mathrm{xii})_{q-1}$ or $(\mathrm{xiii})_{q-1}$ occur or is equal to $\eta_w^{p^{r_{w(q)} - r_{w(q-1)}}}$ if $(\mathrm{xiii})_{q-1}$ or $(\mathrm{xiv})_{q-1}$ is true.

Let $a = \mathrm{ord}(P_q^{p^{u_q}}(y))$ and assume (11).

Suppose that $(\mathrm{xii})_{q-1}$ is true. Then $(v(q-1), w(q-1)) = (v-1, w)$, $a \in (1/p^{s_{v-1}})\mathbb{Q}'$, $r_{w(q)} = r_{w(q-1)}$, and $(\alpha, \iota_1, \dots, \iota_v) = (\delta, n_1, \dots, n_v)$. By Lemma 6 (b), the basis $\bar{B}_{a,v,w}$ contains $\bar{B}_{a,v-1,w}$, whence $\bar{B}_{a,v,w} = \bar{B}_{a,v-1,w}$. Consider relations (7), (8) for $(v(q'), w(q'))$, $1 \le q' \le q-2$, in place of $(v, w)$. By the recursive assumption, these relations depend only on $\tau$ and do not depend on the choice of $(y, A)$. The elements of the basis $\bar{B}_{a,v-1,w}$ can be written as linear combinations of the elements of the standard basis (9) with $m = w$. By Remark 2, this representation depends only on $\tau$ and does not depend on the choice of $(y, A)$.

On the other hand, by Lemma 5 (b), the family of coefficients of the residue of the element (44) in the basis $\bar{B}_{a,v-1,w}$ is precisely

$$y_{\gamma, i_1, \dots, i_v, j_1, \dots, j_w}, \quad (\gamma, i_1, \dots, i_v, j_1, \dots, j_w) \in (\widetilde{A}_{q-1})_+ \setminus \widetilde{A}_{q-1}.$$

Thus, the coefficients of the representation of the residue of $\xi_v^{p^{r_{w(q)} - r_{w(q-1)}}}$ as a linear combination of elements of the basis $\bar{B}_{a,v-1,w}$ depend only on $\tau$ and do not depend on the choice of $(y, A)$. Hence, the same is true for the standard basis (9) with $m = w$ (in place of $\bar{B}_{a,v-1,w}$). Consequently, relation (7) with $(v(q-1), w(q-1))$ in place of $(v, w)$ depends only on $\tau$ and does not depend on the choice of $(y, A)$ whenever $(\mathrm{xii})_{q-1}$ is true.

Assume that $(\mathrm{xiii})_{q-1}$ is true. Then $(v(q-1), w(q-1)) = (v-1, w-1)$ and $a \in (1/p^{s_{v-1}})\mathbb{Q}'$. By Lemma 6 (b), the basis $\bar{B}_{a,v,w}$ contains $\bar{B}_{a,v-1,w-1}$. As in the case where $(\mathrm{xii})_{q-1}$ is true, we can prove that the coefficients of the representation of the residue of $P_q^{p^{u_q}}(y)/(X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})$ as a linear combination of elements of the basis $\bar{B}_{a,v-1,w-1}$ depend only on $\tau$ and do not depend on the choice of $(y, A)$. Hence, the same is true for the standard basis (9) with $m = w-1$ (in place of $\bar{B}_{a,v-1,w-1}$).

We have $\mathrm{ord}((X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})/(X^\delta g_1^{n_1} \cdot \ldots \cdot g_v^{n_v})^{p^{r_{w(q)} - r_{w(q-1)}}}) = 0$ (and now $\iota_v = n_v = 0$). Applying the recursive assumption, Lemma 2, and Remark 2, we can represent the residue of the element $(X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})/(X^\delta g_1^{n_1} \cdot \ldots \cdot g_v^{n_v})^{p^{r_{w(q)} - r_{w(q-1)}}}$ as a linear combination of elements of the standard basis (9) with $m = w-1$ and prove that the coefficients from $k_s$ in this representation depend only on $\tau$ and do not depend on the choice of $(y, A)$. Thus, relations (7) and (8) with $(v(q-1), w(q-1))$ in place of $(v, w)$ depend only on the choice of $\tau$ and do not depend on $(y, A)$ whenever $(\mathrm{xiii})_{q-1}$ is true.

Assume that $(\mathrm{xiv})_{q-1}$ is true. Then $(v(q-1), w(q-1)) = (v, w-1)$ and $a \in (1/p^{s_v})\mathbb{Q}'$. By Lemma 6 (b), the basis $\bar{B}_{a,v,w}$ contains $\bar{B}_{a,v,w-1}$. As in the case where $(\mathrm{xiii})_{q-1}$ is true, we can prove that the coefficients of the representation of the residue of $P_q^{p^{u_q}}(y)/(X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})$ as a linear combination of elements of the basis $\bar{B}_{a,v,w-1}$ depend only on $\tau$ and do not depend on the choice of $(y, A)$. Hence, the same is true for the standard basis (9) with $m = w-1$ (in place of $\bar{B}_{a,v,w-1}$).

Like in the case where $(\mathrm{xiii})_{q-1}$ is true, we can represent the residue of the element $(X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})/(X^\delta g_1^{n_1} \cdot \ldots \cdot g_v^{n_v})^{p^{r_{w(q)} - r_{w(q-1)}}}$ as a linear combination of elements of the standard basis (9) with $m = w$ and prove that the coefficients from $k_s$ in this representation depend only on $\tau$ and do not depend on the choice of $(y, A)$. Thus,

relation (8) with $(v(q-1), w(q-1))$ in place of $(v, w)$ depends only on $\tau$ and does not depend on the choice of $(y, A)$ if $(\mathrm{xiii})_{q-1}$ occurs. This proves assertion (a).

Assertion (b) is proved similarly. The lemma is proved. □

*Remark* 3. Under the conditions of Lemma 14, if $q < q^*$, then some sons of $\tau$ in the tree $T$ may belong to $T_q$ and other sons to $T_{q+1} \setminus T_q$. Hence, in general, the property $A = \widetilde{A}_q$ depends on the choice of the root $y$ of the polynomial $f$.

## §5. Generalization of the Newton broken lines method

Now we assume that $f \in k[X, Y]$ is a polynomial with leading coefficient $\mathrm{lc}_Y(f) = 1$ and that $f$ is separable as an element of $k(X)[Y]$.

In this section our aim is to make the construction described in §1 fully algorithmic. Now we are going to construct the expansions introduced in §1 for all roots of the polynomial $f$. Therefore, we modify the description of this construction making some supplements to it. Our algorithm is recursive on the tree $\mathcal{T}$. We shall say that the step of recursion corresponds to the tree $\mathcal{T}$ if and only if the tree $\mathcal{T}$ is given at the beginning (or the input) of that step. Here $\mathcal{T}$ is a subtree of the tree $T$, see §4. The base of recursion is the tree consisting of one vertex: the root $\tau_0$ of the tree $T$. Recall that this root is equal to the singleton $\{(\varnothing, 0, 0)\}$. We shall suppose that the set of leaves $L(\mathcal{T})$ is linearly ordered. Let $1 \le q \le q^*$ be the smallest integer such that $L(\mathcal{T}) \cap T_q \setminus L(T) \ne \varnothing$ (here we identify the tree $T_q$ with the set of its vertices). Then we have an induced linear order on the set $L(\mathcal{T}) \cap T_q \setminus L(T)$. We find the least element $\tau \in L(\mathcal{T}) \cap T_q \setminus L(T)$, and construct all its sons $\tau_j$, $j \in J_\tau$, in the tree $T$ by using a generalization of the method of the Newton broken lines, see below. Thus, we obtain the new tree $\mathcal{T}_+ = \mathcal{T} \cup \{\tau_j : j \in J_\tau\}$. Then we introduce a linear order on the set $\{\tau_j : j \in J_\tau\}$ and assume that

- $\tau_j < \tau'$ for every $\tau' \in L(\mathcal{T}) \setminus \{\tau\}$;
- for all $j_1, j_2 \in J_\tau$, if $\tau_{j_1} \in T_q$ and $\tau_{j_2} \in T_{q+1} \setminus T_q$, then $\tau_{j_1} < \tau_{j_2}$.

This gives a linear order on the set

$$L(\mathcal{T}) \cup \{\tau_j : j \in J_\tau\} \setminus \{\tau\} = L(\mathcal{T}_+).$$

After that, if $\mathcal{T}_+ \ne T$ we replace $\mathcal{T}$ by $\mathcal{T}_+$ and proceed to the next step of recursion.

At the step of recursion corresponding to the tree $\mathcal{T}$, the following objects are known (i.e., were computed at the preceding steps):

(xix) the tree $\mathcal{T}$ itself with the linear order on the set its leaves $L(\mathcal{T})$;
(xx) for every leaf $\tau \in L(\mathcal{T})$, all the objects occurring in Lemma 14 that depend only on $\tau$ and do not depend on the choice of $(y, A)$.

Before describing the recursion step that corresponds to the tree $\mathcal{T}$, we give some definitions. Let $\tau = V_{y,A}$ for some root $y$ of the polynomial $f$, and let $A \in S_{y,q} \setminus S_{y,q-1}$ for some $0 \le q \le q_y^*$. Let $v = v(q)$, $w = w(q)$. The objects defined below will depend on $\tau$.

Let $\psi = \sum_{1 \le i \le d} \psi_i Y^i \in \Omega_0[Y]$ be an arbitrary polynomial such that

$$\psi = \sum_{1 \le i \le \deg \psi} \psi_i Y^i, \quad \psi_i \in \Omega_0,$$

and $\deg_Y \psi = d$. Recall that $\mathrm{ord}(\psi) = \min\{\mathrm{ord}(\psi_i),\ 0 \le i \le d\}$.

Let $\nu \geq 1$ be the smallest integer such that all the polynomials $\psi$, $P_A$, $G_1, \ldots, G_v, H_1, \ldots, H_w$ belong to $k_s((X^{1/\nu}))[Y]$. Then Lemma 13 allows us to represent

$$\psi = \sum_{\substack{(i_1,\ldots,i_v)\in I_v,\\ (j_1,\ldots,j_w)\in J_w,\\ 0\leq a\leq dp^{-s_v-r_w},\, a\in\mathbb{Z},\\ \operatorname{ord}(\psi)\leq\alpha\in(1/\nu)\mathbb{Z}}} \psi_{\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a} X^\alpha G_1^{i_1}\cdot\ldots\cdot G_v^{i_v} H_1^{j_1}\cdot\ldots\cdot H_w^{j_w} P_A^a, \tag{45}$$

where all $\psi_{\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a}$ belong to $k_s$. Denote by $\mathcal{I}_\tau(\psi)$ the set of all collections $(\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w, a)$ such that $(i_1, \ldots, i_v) \in I_v$, $(j_1, \ldots, j_w) \in J_w$, $0 \leq a \leq dp^{-s_v-r_w}$, $a \in \mathbb{Z}$, $\operatorname{ord}(\psi) \leq \alpha \in (1/\nu)\mathbb{Z}$, and $\psi_{\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a} \neq 0$. Then we can replace the summation conditions in (45) by $\sum_{(\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a)\in\mathcal{I}_\tau(\psi)}$.

In what follows we shall assume that $\operatorname{ord}(\psi) = 0$ and $\operatorname{lc}_Y \psi = \psi_d = 1$.

For every $0 \leq a \leq d$ we introduce the set

$$\mathcal{P}_{\tau,a}(\psi) = \big\{ \operatorname{ord}(X^\alpha g_1^{i_1}\cdot\ldots\cdot g_v^{i_v} h_1^{j_1}\cdot\ldots\cdot h_w^{j_w}) \,:\, (\alpha, i_1, \ldots, i_v, j_1, \ldots, j_w, a) \in \mathcal{I}_\tau(\psi)\big\}.$$

Notice that $\mathcal{P}_{\tau,a}(\psi) \subset (1/p^{s_v})\mathbb{Q}'$.

For every $b \in \mathcal{P}_{\tau,a}(\psi)$ we introduce the element

$$\psi_{b,a} = \sum_{\substack{(\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a)\in\mathcal{I}_\tau(\psi),\\ \operatorname{ord}(X^\alpha g_1^{i_1}\cdot\ldots\cdot g_v^{i_v} h_1^{j_1}\cdot\ldots\cdot h_w^{j_w})=b}} \psi_{\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a} X^\alpha g_1^{i_1}\cdot\ldots\cdot g_v^{i_v} h_1^{j_1}\cdot\ldots\cdot h_w^{j_w}. \tag{46}$$

We have $\operatorname{ord}(\psi_{b,a}) = b$ (this can easily be deduced from Lemma 5). Set $\mathcal{P}_\tau(\psi) = \{(b, a) : 0 \leq a \leq d \;\&\; b \in \mathcal{P}_{\tau,a}(\psi)\}$. Put

$$\psi_\tau = \sum_{(b,a)\in\mathcal{P}_\tau(\psi)} \psi_{b,a} Z^a.$$

Let $\gamma, \delta$ be integers, $\gamma > 0$, $\delta \geq 0$. Put

$$\mathcal{P}_\tau(\psi,\gamma,\delta) = \big\{(b,a) \in \mathcal{P}_\tau(\psi) \,:\, \forall (b_1,a_1) \in \mathcal{P}_\tau(\psi)(\gamma b_1 + \delta a_1 \geq \gamma b + \delta a)\big\},$$

$$\psi_\tau(\gamma,\delta) = \sum_{(b,a)\in\mathcal{P}_\tau(\psi,\gamma,\delta)} \psi_{b,a} Z^a.$$

Set $d(\gamma,\delta) = \max\{a : \exists (b,a) \in \mathcal{P}_\tau(\psi,\gamma,\delta)\}$. Then $\deg_Z \psi_\tau(\gamma,\delta) = d(\gamma,\delta)$.

Assume additionally that $\delta/\gamma \in (1/p^s)\mathbb{Q}'$, where the integer $s \geq s_v$ is the smallest possible and $v = v(q)$. We shall write $s = s(\gamma,\delta)$. Now we are going to define the polynomials

$$\psi_\tau^\star(\gamma,\delta),\ \psi_\tau^*(\gamma,\delta) \in k_s[\overline{\eta}_1, \ldots, \overline{\eta}_w][Z],$$

where $w = w(q)$. Let $a_0 \in \mathbb{Z}$ be such that $Z^{a_0}$ divides the polynomial $\psi_\tau(\gamma,\delta)$ but $Z^{a_0+1}$ does not divide $\psi_\tau(\gamma,\delta)$. Notice that the constant $c = b + (\delta/\gamma)(a - a_0) \in (1/p^s)\mathbb{Q}'$ is the same for all $(b,a) \in \mathcal{P}_\tau(\psi,\gamma,\delta)$. In particular, taking $a - a_0 = 0$, we see that $c \in (1/p^{s_v})\mathbb{Q}'$. Therefore, $p^{s-s_v}$ divides $a - a_0$ for every $a$ such that there exists $b$ with $(b,a) \in \mathcal{P}_\tau(\psi,\gamma,\delta)$.

There are unique $\varepsilon \in \mathbb{Q}'$ and $(d_1, \ldots, d_v) \in I_v$ such that

$$\operatorname{ord}(X^\varepsilon g_1^{d_1}\cdot\ldots\cdot g_v^{d_v}) = p^{s-s_v}\delta/\gamma. \tag{47}$$

Next, there are unique $\varepsilon' \in \mathbb{Q}'$ and $(d_1', \ldots, d_v') \in I_v$ such that

$$\operatorname{ord}(X^{\varepsilon'} g_1^{d_1'}\cdot\ldots\cdot g_v^{d_v'}) = c.$$

For every integer $a$ such that $(b, ap^{s-s_v} + a_0) \in \mathcal{P}_\tau(\psi,\gamma,\delta)$ for some $b$, put

$$\varphi_a = \psi_{b,ap^{s-s_v}+a_0} \cdot \big(X^\varepsilon g_1^{d_1}\cdot\ldots\cdot g_v^{d_v}\big)^a / \big(X^{\varepsilon'} g_1^{d_1'}\cdot\ldots\cdot g_v^{d_v'}\big).$$

Now, $\operatorname{ord}(\varphi_a) = 0$ for such $a$. Hence, the residue $\overline{\varphi}_a$ of the element $\varphi_a$ is well defined.

**Lemma 15.** *The residue $\overline{\varphi}_a$ depends only on $\psi$, $a$, $\gamma$, $\delta$, and $\tau$, but does not depend on the choice of $(y, A)$*

*Proof.* Set

$$b_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w,a} = \psi_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w,ap^{s-s_v}+a_0} X^\alpha g_1^{i_1} \cdot \ldots \cdot g_v^{i_v} h_1^{j_1} \cdot \ldots \cdot h_w^{j_w}$$

for every summand on the right-hand side of identity (46) with $ap^{s-s_v} + a_0$ in place of $a$. It suffices to show that for every such summand $b_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w,a}$ the residue of the element

$$b_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w,a} \cdot \bigl(X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v}\bigr)^{ap^{s-s_v}+a_0} / \bigl(X^{\varepsilon'} g_1^{d'_1} \cdot \ldots \cdot g_v^{d'_v}\bigr) \tag{48}$$

depends only on $\psi$, $\alpha, i_1, \dots, i_v, j_1, \dots, j_w, a$, $\gamma$, $\delta$, and $\tau$ and does not depend on the choice of $(y, A)$. By Corollary 1, the element (48) can be represented in the form

$$\psi_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w,ap^{s-s_v}+a_0} \xi_1^{a_1} \cdot \ldots \cdot \xi_v^{a_v} \eta_1^{j_1} \cdot \ldots \cdot \eta_w^{j_w}$$

with some integers $a_1, \dots, a_v$. These integers depend only on $i_1, \dots, i_v, j_1, \dots, j_w$, $a$, $\gamma$, $\delta$, and $\tau$ by Corollary 1 and Lemma 14. Hence, $\bar{\xi}_1^{a_1}, \dots, \bar{\xi}_v^{a_v}$, $\bar{\eta}_1^{j_1}, \dots, \bar{\eta}_w^{j_w}$ depend only on $i_1, \dots, i_v, j_1, \dots, j_w, a$, $\gamma$, $\delta$, and $\tau$ and do not depend on the choice of $(y, A)$ by Lemma 14. The lemma is proved. □

By definition, we put

$$\psi^\star_\tau(\gamma, \delta) = \sum_{\{a\,:\,\exists b\ (b, ap^{s-s_v}+a_0) \in \mathcal{P}_\tau(\psi,\gamma,\delta)\}} \overline{\varphi}_a Z^a,$$

$$\psi^*_\tau(\gamma, \delta) = Z^{a_0} \psi^\star_\tau(\gamma, \delta)(Z^{p^{s-s_v}}).$$

Then $\psi^*_\tau(\gamma, \delta)/Z^{a_0}$ is a polynomial in $Z^{p^{s-s_v}}$. We have $\deg_Z \psi^*_\tau(\gamma, \delta) = d(\gamma, \delta)$. By Lemma 15, the polynomials $\psi^\star_\tau(\gamma, \delta)$ and $\psi^*_\tau(\gamma, \delta)$ depend only on $\psi$, $\delta$, $\gamma$, and $\tau$ and do not depend on the choice of $(y, A)$

The set of vertices $V_\tau(\psi)$ of the generalized Newton broken line of the polynomial $\psi$ is defined by the formula

$$V_\tau(\psi) = \bigl\{(b, a) \in \mathcal{P}_\tau(\psi)\ :\ \exists(\gamma, \delta) \in \mathbb{Z}^2(\gamma > 0\ \&\ \delta \geq 0\ \&\ \mathcal{P}_\tau(\psi, \gamma, \delta) = \{(b, a)\})\bigr\}.$$

In other words, $(b, a)$ is a vertex of the generalized Newton broken line of $\psi$ if and only if it is the element of the singleton $\mathcal{P}_\tau(\psi, \gamma, \delta)$ for some integers $\gamma > 0$ and $\delta \geq 0$.

The set of edges $E_\tau(\psi)$ of the generalized Newton broken line of the polynomial $\psi$ (or simply the generalized Newton broken line of the polynomial $\psi$) is defined by the formula

$$E_\tau(\psi) = \bigl\{((b_1, a_1), (b_2, a_2)) \in V_\tau(\psi)^2\ :\ \exists(\gamma, \delta) \in \mathbb{Z}^2(\gamma > 0\ \&\ \delta \geq 0\ \&\ \mathcal{P}_\tau(\psi, \gamma, \delta) \supset \{(b_1, a_1), (b_2, a_2)\}\ \&\ a_1 > a_2)\bigr\}.$$

It should be emphasized that here $E_\tau(\psi)$ is a generalized Newton broken line corresponding to $\tau$. Sometimes we shall omit the word "generalized" if this does not lead to ambiguity.

If $e = ((b_1, a_1), (b_2, a_2)) \in E_\tau(\psi)$, then, by definition, $\psi^*_{\tau,e} = \psi^*_\tau(\gamma, \delta)$ and $\psi^\star_{\tau,e} = \psi^\star_\tau(\gamma, \delta)$, where $\{(b_1, a_1), (b_2, a_2)\} \subset \mathcal{P}_\tau(\psi, \gamma, \delta)$. In this case the slope $\lambda(e)$ of the edge $e$ is defined by the formula $\lambda(e) = \delta/\gamma = (b_1 - b_2)/(a_1 - a_2)$. For every $e \in E_\tau(\psi)$ we define integers $\gamma(e) > 0$ and $\delta(e) \geq 0$ such that $\delta(e)/\gamma(e) = \lambda(e)$ and $\mathrm{GCD}(\gamma(e), \delta(e)) = 1$. Put $s(e) = s(\gamma(e), \delta(e))$.

If $e \in V_\tau(\psi)$, then by definition $\psi^*_{\tau,e} = \psi^*_\tau(\gamma, \delta)$ and $\psi^\star_{\tau,e} = \psi^\star_\tau(\gamma, \delta)$, where $\{e\} = \mathcal{P}_\tau(\psi, \gamma, \delta)$.

Now we proceed to the description of the recursion step corresponding to the tree $\mathcal{T}$. Let us find the minimal element $\tau \in L(\mathcal{T}) \cap T_q \setminus L(T)$. Here $1 \le q \le q^*$ is the smallest integer such that $L(\mathcal{T}) \cap T_q \setminus L(T) \ne \varnothing$, see the beginning of the section.

Let $\tau = V_{y,A}$ for a root $y$ of the polynomial $f$ and a set $A$ belonging to $S_{y,q} \setminus S_{y,q-1}$, $0 \le q \le q^*_y$. In what follows we consider objects occurring in Lemma 14 (they depend only on $\tau$).

Let $\nu \ge 1$ be the smallest integer and $k''$ the least separable extension of the field $k$ such that all the polynomials $P_A, G_1, \ldots, G_v, H_1, \ldots, H_w$ lie in $k''((X^{1/\nu}))[Y]$.

Notice that the set $\mathcal{I}_\tau(f)$ is finite by Lemma 12 and Lemma 13 because $f \in k[X,Y]$. Applying Lemma 13 and solving a linear system over the field $k''(X^{1/\nu})$, we construct the set $\mathcal{I}_\tau(f)$ and the family of coefficients

$$\{f_{\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a}\}_{(\alpha,i_1,\ldots,i_v,j_1,\ldots,j_w,a)\in\mathcal{I}_\tau(f)}. \tag{49}$$

In accordance with the definitions given, to find $E_\tau(f)$ it suffices to know $\operatorname{ord}(g_m)$ and $\operatorname{ord}(h_n)$ for all $1 \le m \le v$, $1 \le n \le w$, and these numbers are known by the recursive assumption. Let us construct the Newton broken line $E_\tau(f)$ of the polynomial $f$. Obviously $\lambda(e) \ge 0$ for every $e \in E_\tau(f)$. Denote by $E'_\tau(f)$ the subset of all $e \in E_\tau(f)$ such that $\lambda(e) > \operatorname{ord}(Q_A(y))$ if $A \ne \varnothing$ and $\lambda(e) \ge 0$ if $A = \varnothing$ (recall that $A = \varnothing$ only if $q = 0$ and $\tau = \tau_0$). For every $e \in E'_\tau(f)$ we compute the polynomial $f^\star_{\tau,e} \in k_{s,w}[Z]$ using Lemma 2 and identities (5) (here we leave the details to the reader). Next, we use the algorithm (known in advance) for factoring polynomials over finite extensions of $k_s$ to factor each polynomial $f^\star_{\tau,e}$ over the field $k_{s,w}$, obtaining a decomposition into irreducible factors

$$f^\star_{\tau,e} = \varphi_{\tau,e,0} \prod_{j\in J_{\tau,e}} (Z^{p^{\nu_j}} - \varphi_j)^{\mu_j},$$

where $J_{\tau,e}$ is a finite set of indices, $0 \ne \varphi_{\tau,e,0} \in k_{s,w}$ (it is the leading coefficient of the polynomial $f^\star_{\tau,e}$), $0 \ne \varphi_j \in k_{s,w}$, $1 \le \mu_j \in \mathbb{Z}$, $0 \le \nu_j \in \mathbb{Z}$, and each polynomial $Z^{p^{\nu_j}} - \varphi_j$ is irreducible over the field $k_{s,w}$ for every $j \in J_{\tau,e}$. We shall assume without loss of generality that $J_{\tau,e_1} \cap J_{\tau,e_2} = \varnothing$ for all pairwise distinct $e_1, e_2 \in E'_\tau(f)$.

If $Z$ does not divide the polynomial $f_\tau$, then we put $J_\tau = \bigcup_{e\in E'_\tau(f)} J_{\tau,e}$.

If $Z$ divides the polynomial $f_\tau$, then we shall suppose without loss of generality that $j_{\tau,0} \notin \bigcup_{e\in E'_\tau(f)} J_{\tau,e}$. In this case we put $J_\tau = \{j_{\tau,0}\} \cup \bigcup_{e\in E'_\tau(f)} J_{\tau,e}$.

In both cases the set of all sons of the vertex $\tau$ in the tree $T$ (and therefore also in the tree $\mathcal{T}_+$) is in one-to-one correspondence with the set $J_\tau$. Let $\{\tau_j\}_{j\in J_\tau}$ denote the family of all sons of the vertex $\tau$.

Recall that $\tau_j \setminus \tau$ is a singleton, see §4. We have $\tau_j = V_{y_j,A_j}$ for some root $y_j$ of $f$ and $A_j \in S_{y_j}$. Now we need to define these $y_j$, $A_j$ and construct $\tau_j$ and all the objects from the statement of Lemma 14 related to $\tau_j$ for every $j \in J_\tau$.

Suppose that $j \in J_\tau$, $j \ne j_{\tau,0}$. Then there exists a root $y_j$ of $f$ such that $\tau = V_{y_j,A}$, $\operatorname{ord}(P_A(y_j)) = \lambda(e)$, $s = s(e)$, and

$$\operatorname{ord}\left(\left(P_A(y_j)^{p^{s-s_v}}/(X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v})\right)^{p^{\nu_j}} - \varphi_j\right) > 0$$

(here $\varepsilon, d_1, \ldots, d_v$ depend on $e$ and $\lambda(e) = \delta/\gamma$, see (47) above). We choose and fix such a root $y_j$.

If $j \in J_\tau$, $j = j_{\tau,0}$, then there is a unique root $y_{j_{\tau,0}}$ of the polynomial $f$ such that $P_A(y_{j_{\tau,0}}) = 0$.

Put $A_j = A_+$, where $A, A_+ \in S_{y_j}$, see §2, and $\tau_j = V_{y_j,A_j}$. Thus, $\tau_j$ is defined for every $j \in J_\tau$. The tree $\mathcal{T}_+$ is constructed. We introduce the linear order on the set of leaves $L(\mathcal{T}_+)$ as described at the beginning of the section.

The explicit algorithm for finding $V_{y_j,A_j}$ and all the objects related to $\tau_j$ is obtained straightforwardly from the construction described in the preceding sections. Still we give some details here. Namely, one of the following conditions is fulfilled.

(xii)′ $j \in J_{\tau,e}$, $e \in E'_\tau(f)$, $\lambda(e) \in (1/p^s)\mathbb{Q}'$, $\lambda(e) \notin (1/p^{s-1})\mathbb{Q}'$, where $s > s_v$ and $\nu_j = 0$;

(xiii)′ $j \in J_{\tau,e}$, $e \in E'_\tau(f)$, $\lambda(e) \in (1/p^s)\mathbb{Q}'$, $\lambda(e) \notin (1/p^{s-1})\mathbb{Q}'$, where $s > s_v$ and $\nu_j > 0$;

(xiv)′ $j \in J_{\tau,e}$, $e \in E'_\tau(f)$, $\lambda(e) \in (1/p^{s_v})\mathbb{Q}'$, and $\nu_j > 0$;

(xv)′ $j = j_{\tau,0}$, or $j \in J_{\tau,e}$, $e \in E'_\tau(f)$, and $\lambda(e) \geq N+1$;

(xvi)′ & (xvii)′ $j \in J_{\tau,e}$, $e \in E'_\tau(f)$, $\lambda(e) \in (1/p^{s_v})\mathbb{Q}'$, $\lambda(e) < N+1$, and $\nu_j = 0$

(here (xii)′, (xiii)′, (xiv)′, and (xv)′ correspond to (xii), (xiii), (xiv), and (xv) from §1, and the item (xvi) & (xvii) corresponds to the two items (xvi) and (xvii) from §2 and the subcase (a) where $\operatorname{ord}(\widetilde{y}_A) < N+1$).

In what follows till the end of the section all the objects correspond to the root $y_j$ (in place of $y$), say, the polynomial $P_{q+1}$, the integer-valued functions $v$, $w$ and so on.

Now we have $Q_{A_j} = Q_{A_+}$, $P_{A_j} = P_{A_+}$. Next, $A_j \in S_{y_j,q+1} \setminus S_{y_j,q}$ if (xii)′, (xiii)′, or (xiv)′ are true, and $A_j \in S_{y_j,q} \setminus S_{y_j,q-1}$ if (xv)′ or (xvi)′ & (xvii)′ are true. Therefore, $s_{A_j} = s_{v(q+1)}$ and $r_{A_j} = r_{w(q+1)}$ if (xii)′, (xiii)′, or (xiv)′ are true, and $s_{A_j} = s_v$, $r_{A_j} = r_w$ if (xv)′ or (xvi)′ & (xvii)′ are true.

In the cases where (xii)′, (xiii)′, or (xiv)′ are fulfilled, we have $\lambda(e) < N+1$, $q < q^*_y$, and $\tau_j \in T_{q+1} \setminus T_q$. If (xv)′ is fulfilled, then $\tau_j \in L(T) \cap T_q$.

If (xii)′, (xiii)′, (xiv)′, or (xv)′ are fulfilled, then $\widetilde{A}_q = A$ and

$$P_{q+1} = P_A = P_q^{p^{u_q}} - \sum_{A' \in S_{y,A} \setminus S_{y,q-1}} Q_{A'}, \tag{50}$$

where all the elements on the right-hand side of (50) are defined recursively and depend only on $\tau$.

Assume that (xii)′ are fulfilled. Then $v(q+1) = v+1$, $w(q+1) = w$, $s_{v+1} = s$, $u_{q+1} = s_{v+1} - s_v$, $G_{v+1} = P_{q+1}$, $(\alpha_{v+1}, i_{v+1,1}, \dots, i_{v+1,v}) = (\varepsilon, d_1, \dots, d_v)$, $\xi_{v+1} = P_{q+1}(y_j)^{p^{s-s_v}}/(X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v})$, and $\bar{\xi}_{v+1} = \varphi_j$.

Assume that (xiii)′ is fulfilled. Then $v(q+1) = v+1$, $w(q+1) = w+1$, $s_{v+1} = s$, $r_{w+1} = r_w + \nu_j$, $u_{q+1} = s_{v+1} - s_v + r_{w+1} - r_w$, $G_{v+1} = P_{q+1}$, $H_{w+1} = P_{q+1}^{p^{s_{v+1}-s_v}}$,

$$(\alpha_{v+1}, i_{v+1,1}, \dots, i_{v+1,v}) = (\beta_{v+1}, \iota_{v+1,1}, \dots, \iota_{v+1,v}) = (\varepsilon, d_1, \dots, d_v),$$

$\eta_{w+1} = \xi_{v+1} = P_{q+1}(y_j)^{p^{s-s_v}}/(X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v})$, and $\bar{\eta}_{w+1}^{p^{r_{w+1}-r_w}} = \varphi_j$.

Assume that (xiv)′ is fulfilled. Then $v(q+1) = v$, $w(q+1) = w+1$, $r_{w+1} = r_w + \nu_j$, $u_{q+1} = r_{w+1} - r_w$, $H_{w+1} = P_{q+1}$, $(\beta_{v+1}, \iota_{v+1,1}, \dots, \iota_{v+1,v}) = (\varepsilon, d_1, \dots, d_v)$, $\eta_{w+1} = P_{q+1}(y_j)^{p^{s-s_v}}/(X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v})$, and $\bar{\eta}_{w+1}^{p^{r_{w+1}-r_w}} = \varphi_j$.

It remains to show how to construct the polynomials $P_{A_j}$ and $Q_{A_j}$ explicitly.

Assume that (xii)′, (xiii)′, or (xiv)′ are fulfilled. Put $a = p^{u_{q+1}}\lambda(e)$ and assume (11), see §2.

Let $a < N+1$. Now $a \in (1/p^{s_v})\mathbb{Q}'$. Hence, by Lemma 6 (b), the basis $\bar{B}_{a,v(q+1),w(q+1)}$ contains $\bar{B}_{a,v,w}$. One constructs the bases $\bar{B}_{a,v(q+1),w(q+1)}$ and $\bar{B}_{a,v,w}$ immediately.

Put

$$\Psi_j = \big((X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v})^{p^{r_{w(q+1)}-r_{w(q)}}}\big)/\big(X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v}\big).$$

Then $\operatorname{ord}(\Psi_j) = 0$. Hence, by Lemma 5, there are integers $a_1, \dots, a_v$ (one can construct them easily) such that $\Psi_j = \xi_1^{a_1} \cdot \ldots \cdot \xi_v^{a_v}$. Therefore, the residue of the element $P_{q+1}(y_j)^{p^{u_{q+1}}}/(X^\alpha g_1^{\iota_1} \cdot \ldots \cdot g_v^{\iota_v})$ is equal to $\varphi_j \bar{\xi}_1^{a_1} \cdot \ldots \cdot \bar{\xi}_v^{a_v}$. We represent this residue $\varphi_j \bar{\Psi}_j$ as a linear combination of elements of the basis $\bar{B}_{a,v(q+1),w(q+1)}$ (in fact, of the

basis $\bar{B}_{a,v,w}$). Then, by Lemma 5 (b), the family of nonzero coefficients from $k_s$ in this representation is exactly

$$y_{\gamma,i_1,\dots,i_{v(q+1)},j_1,\dots,j_{w(q+1)}}, \quad \bigl(\gamma, i_1, \dots, i_{v(q+1)}, j_1, \dots, j_{w(q+1)}\bigr) \in A_j \setminus A$$

(recall that now $A = \widetilde{A}_q$ and $A_j = (\widetilde{A}_q)_+$). Thus, using (28), (29) with $(q+1, A_j)$ in place of $(q, A)$, we can construct $P_{A_j}$ and $Q_{A_j}$ explicitly in the case where (xii)′, (xiii)′, or (xiv)′ are fulfilled and $a < N+1$.

Let (xii)′, (xiii)′, or (xiv)′ be fulfilled, and let $a \geq N+1$. Then $q^*_{y_j} = q+1$. Put $A_j = \widetilde{A}_{q+1} = A \cup (N+1, 0, \dots, 0)$, $y_{N+1,0,\dots,0} = 0$, where $(N+1, 0, \dots, 0) \in \mathbb{Q}' \times \mathbb{Z}^{v(q+1)+w(q+1)}$. Hence, $P_{A_j} = P_{q+2} = P_{q+1}^{p^{u_{q+1}}}$, $Q_{A_j} = 0$, and $\tau_j \in L(T) \cap T_{q+1}$ in this case.

Assume that (xvi)′ & (xvii)′ is fulfilled. Let $a = \lambda(e)$ and assume (11), see §2. The residue of the element $P_A(y_j)/(X^\varepsilon g_1^{d_1} \cdot \ldots \cdot g_v^{d_v})$ is equal to $\varphi_j$. We represent $\varphi_j$ as a linear combination of elements of the basis $\bar{B}_{a,v,w}$. Then, by Lemma 5 (b), the family of nonzero coefficients from $k_s$ in this representation coincides with the family

$$y_{\gamma,i_1,\dots,i_v,j_1,\dots,j_w}, \quad \bigl(\gamma, i_1, \dots, i_v, j_1, \dots, j_w\bigr) \in A_j \setminus A.$$

Thus, using (28), (29) with $A_j$ in place of $A$, we can construct $P_{A_j}$ and $Q_{A_j}$ explicitly in the case where (xvi)′ & (xvii)′ is fulfilled.

Assume that (xv)′ is fulfilled. Then we put $q^*_{y_j} = q$ and $A_j = A \cup \{(N+1, 0, \dots, 0)\}$, where $(N+1, 0, \dots, 0) \in \mathbb{Q}' \times \mathbb{Z}^{v+w}$. We have $y_{N+1,0,\dots,0} = 0$. Hence, $P_{A_j} = P_A$ and $Q_{A_j} = 0$. In this case $\tau_j \in L(T)$ is a leaf of the tree $T$.

We have finished the description of the algorithm for constructing the tree $T$ and the objects corresponding to its vertices.

*Proof of Theorem* 1. Let $N$ be as in the statement of that theorem. Put $N_1 = N + \operatorname{ord}(\Delta)/2$. We apply the algorithm described in this section to $(f, N_1)$ in place of $(f, N)$. Let $\tau \in L(T)$ and let $\tau = V_{y,A}$ for some root $y$ of the polynomial $f$ and a set $A \in S_y$. By Lemma 10, we have $\operatorname{ord}(F - P_{q^*_y+1}) \geq N+1$. Hence, by Lemma 14 (b), using the polynomials $P_{q^*_y+1}$, we can obtain the approximations $F_{\#,N}$ of all factors $F$ of the polynomial $f$ irreducible over $\Omega_0$.

All the other assertions of the theorem follow immediately from the construction described in the paper. The theorem is proved. □

## Appendix: A version of the Hensel lemma

Let $f \in k[[X]][Y]$ be a polynomial as in the Introduction, and let $y \in \overline{k((X))}$ be a root of $f$.

**Lemma 16.** *Let $\widetilde{f} \in k[[X]][Y]$ be another polynomial similar to $f$ and such that* $\operatorname{ord}(f - \widetilde{f}) \geq \operatorname{ord}(\Delta) + 1$. *Then the following assertions are true.*

(a) *The separable algebras $k((X))[Y]/(f)$ and $k((X))[Y]/(\widetilde{f})$ are isomorphic over the field $k((X))$.*

(b) *For every root $y$ of $f$ there is precisely one root $\widetilde{y}$ of $\widetilde{f}$ such that* $\operatorname{ord}(y - \widetilde{y}) \geq \operatorname{ord}(\Delta)/2$ (*we assume that all the roots of the polynomials $f$ and $\widetilde{f}$ belong to the fixed algebraic closure $\overline{k((X))}$ of the field $k((X))$*). *We have $\widetilde{y} \in k((X))[y]$.*

(c) *Denote by $\varphi$ and $\widetilde{\varphi}$ the minimal polynomials of the elements $y$ and $\widetilde{y}$ over the field $k((X))$ with the leading coefficients* $\operatorname{lc}_Y \varphi$ *and* $\operatorname{lc}_Y \widetilde{\varphi}$ *equal to* 1. *Then* $\operatorname{ord}(\varphi - \widetilde{\varphi}) \geq \operatorname{ord}(\Delta)/2$.

(d) *Let us identify $y = Y \bmod \varphi \in k((X))[Y]/(\varphi)$. Then there is an isomorphism of fields $k((X))[Y]/(\widetilde{\varphi}) \to k((X))[Y]/(\varphi)$, $Y \bmod \widetilde{\varphi} \mapsto \widetilde{y}$ over $k((X))$.*

(e) *Moreover, the element $\widetilde{y}$ and the polynomial $\widetilde{\varphi}$ can be constructed by using the Hensel lifting process, provided that the polynomial $\varphi_{\#,N}$, $N = \operatorname{ord}(\Delta) + 1$, is known.*

*Proof.* We leave the proof to the reader. Actually, it is known. □

## References

[1] A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm*, Lecture Notes in Comput. Sci., vol. 233, Springer, Berlin, 1986, pp. 247–255. MR874601

[2] ———, *Effective construction of an algebraic variety nonsingular in codimension one over a ground field of zero characteristic*, Zap. Nauchn. Sem. POMI **387** (2011), 167–188; English transl., J. Math. Sci. (N. Y.) **179** (2011), no. 6, 729–740. MR2822513

[3] ———, *An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 1124–188; English transl., J. Soviet Math. **34** (1986), no. 4, 1838–1882. MR0762101 (86g:11077a)

St. Petersburg Branch, Steklov Mathematical Institute, Russian Academy of Sciences, Fontanka 27, 191023 St. Petersburg, Russia

*E-mail address*: alch@pdmi.ras.ru

Received 19/AUG/2016

Translated by THE AUTHOR