Extension of the Newton–Puiseux algorithm to the case of a nonzero characteristic ground field

Alexander L. Chistov

Abstract. We suggest a generalization of the Newton–Puiseux algorithm for constructing roots of polynomials in the field of fractional power series to the case of nonzero characteristic of the ground field.

Let k be a ground field and $k((X))$ be the field of power series in X with coefficients in k. Let $f \in k((X))[Y]$ be a separable polynomial of the degree $\deg_Y f = d \geqslant 1$. We shall assume without loss of generality that $f \in k[[X]][Y]$ and the leading coefficient $\mathrm{lc}_Y f = 1$ (i.e., the coefficient from $k[[X]]$ of Y^d in the polynomial f). Denote by $\Delta = \mathrm{Res}\,(\, f, f'_Y\,)$ the discriminant of the polynomial f.

If the characteristic $\mathrm{char}(k) = 0$ the algebraic closure

$$\Omega = \overline{k((X))} = \bigcup_{\nu \geqslant 1} \overline{k}((X^{1/\nu})). \tag{1}$$

The classical Newton–Puiseux algorithm constructs the roots of the polynomial f in the field Ω using the method of Newton broken lines. Namely let $y_j = \sum_{i \geqslant 0} y_{j,i} X^{\alpha_{j,i}}$ be a root of f where all $y_{j,i} \in \overline{k}$, $\alpha_{j,0} < \alpha_{j,1} < \alpha_{j,2} < \dots$, all $\alpha_{j,i} \in \frac{1}{e_j}\mathbb{Z}$ for some $1 \leqslant e_j \leqslant d$ (to fix e_j we assume that it is minimal possible). Then for every $r \geqslant 0$ the pair $(y_{j,r}, \alpha_{j,r})$ can be found considering the Newton broken line of the polynomial

$$f\left(Y - \sum_{0 \leqslant i < r} y_{j,i} X^{\alpha_{j,i}}\right).$$

This is an essence of the Newton–Puiseux algorithm.

Now the field $K_j = k((X))[y_j] = k_j((\pi_j))$ where k_j the field of residues of the field K_j and $\pi_j = X^{1/e_j}$ is a uniformizing element of the field K_j. The field k_j is a finite extension of the field k and generated over k by all the elements $y_{j,i}$ (actually by a finite number of them). The degree $[k_j : k] = f_j \leqslant d$. The degree of the minimal polynomial of the element y_j over $k((X))$ is equal to $f_j e_j$.

In what follows we suppose that $\mathrm{char}(k) = p > 0$. Then there are difficulties in comparison with the case $\mathrm{char}(k) = 0$. First of all one can not describe the field $\Omega = \overline{k((X))}$ in a simple way. Namely, (1) does not hold. More than that, let $y_j \in \Omega$ be a root of the polynomial f. Then in general one can not choose an element $\pi \in \Omega$ such that the root $y_j \in \overline{k}((\pi))$ (for this fixed j).

Still the field $K_j = k((X))[y_j]$ has a discrete valuation

$$\mathrm{ord} : K_j \to \frac{1}{e_j}\mathbb{Z} \cup \{+\infty\}$$

such that $\mathrm{ord}(X) = 1$ and $\mathrm{ord}(\pi_j) = 1/e_j$ for a uniformizing element π_j of the field K_j. The residue field k_j of the field K_j with respect to this valuation is a finite (not necessarily separable!) extension of the field k of degree f_j. Similarly to the case of zero–characteristic the degree of the minimal polynomial of the element y_j over $k((X))$ is equal to $f_j e_j$. There is a system of representatives Σ_j of the field k_j in K_j. We shall assume without loss of generality that $\Sigma_j \supset k$ and Σ_j is a linear space over k (in general one can not choose Σ_j to be an algebra over k). Denote by k_s the separable closure of the field k. Then the field $k_s \cap k_j \subset K_j$. So one can assume that $k_s \cap k_j \subset \Sigma_j$. Now the root y_j can be represented as a sum of the infinite series

$$y_j = \sum_{i_0 \leqslant i \in \mathbb{Z}} y_{j,i} \pi_j^i, \tag{2}$$

where all $y_{j,i} \in \Sigma_j$, $y_{j,i_0} \neq 0$. The field k_j is generated over k by all the residues of the elements $y_{j,i}$, $i \geqslant i_0$.

So the final aim of a generalization of the Newton–Puiseux algorithm for nonzero characteristic is to construct for every root y_j of the polynomial f a uniformizing element π_j, a system of representatives Σ_j and the expansion (2). More precisely, to obtain (2) it is sufficient to construct all the elements $y_{j,i} \in \Sigma_j$ for $i_0 \leqslant i \leqslant 1 + \mathrm{ord}(\Delta)$ (we assume that $\mathrm{ord}(\Delta)$ is known). After that subsequent elements $y_{j,i}$ can be found in a simple way using a variant of the Hensel lemma.

Unfortunately one can not obtain at once Σ_j and π_j. So we construct a finite number of elements $z_1, z_2, \dots, \eta_1, \eta_2, \dots$ (they depend on y_j; in what follows j is arbitrary but fixed) satisfying the following properties. For every m the orders $\mathrm{ord}(z_m) = a_m/(b_m p^{s_m})$, where $\mathrm{GCD}(a_m, p) = 1$, $\mathrm{GCD}(b_m, p) = 1$ and $s_m > s_{m-1}$ (we put $s_0 = 0$). Further, for every m denote by $\overline{\eta}_m$ the residue of the element η_m. The the field $k_s[\overline{\eta}_1, \dots, \overline{\eta}_m]$ is purely inseparable over the field k_s and has the degree p^{r_m} over k_s where $1 \leqslant r_m \in \mathbb{Z}$ and $r_m > r_{m-1}$ (we put $r_0 = 0$).

Set $w(0) = v(0) = w(1) = v(1) = 0$, $\widetilde{y}_1 = y_j$. At the beginning of the q-th step of the algorithm the elements $z_1, z_2, \dots, z_v$, $\eta_1, \eta_2, \dots, \eta_w$ and $\widetilde{y}_q$ are known. Here the integer $q \geqslant 1$ and we shall write $w = w(q)$, $v = v(q)$. We have

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

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

Then using Newton broken lines we construct the expansion

$$\widetilde{y}_q^{p^u} = \sum_{(\alpha,i_1,\dots,i_v,j_1,\dots,j_w)\in A} y_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w} X^{\alpha} z_1^{i_1} \cdot \ldots \cdot z_v^{i_v} \eta_1^{j_1} \cdot \ldots \cdot \eta_w^{j_w} + \widetilde{y}_{q+1}, \quad (3)$$

where

(i) A is a finite (or empty) subset of $\mathbb{Q} \times \mathbb{Z}^{v+w}$ (depending on q),
(ii) $0 \leqslant j_m < p^{r_m - r_{m-1}}$ for all $1 \leqslant m \leqslant w$,
(iii) there is an integer a_m such that $a_m \leqslant i_m < a_m + p^{s_m - s_{m-1}}$ for all $1 \leqslant m \leqslant v$ (these integers a_m depend on q and y_j; in this extended abstract we don't explain the sense of introducing a_m),
(iv) $\alpha = \beta/\gamma \in \mathbb{Q}$, $\beta, \gamma \in \mathbb{Z}$, and $\mathrm{G\,C\,D}\,(\gamma, p) = 1$,
(v) for every $(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A$ the element $0 \neq y_{\alpha,i_1,\dots,i_v,j_1,\dots,j_w} \in k_s$.
(vi) for any pairwise distinct $(\alpha, i_1, \dots, i_v, j_1, \dots, j_w), (\alpha', i'_1, \dots, i'_v, j'_1, \dots, j'_w) \in A$ either $(j_1, \dots, j_w) \neq (j'_1, \dots, j'_w)$ or $\alpha + \sum_{1 \leqslant m \leqslant v} i_m a_m/(b_m p^{s_m}) \neq \alpha' + \sum_{1 \leqslant m \leqslant v} i'_m a_m/(b_m p^{s_m})$.
(vii) For every $(\alpha, i_1, \dots, i_v, j_1, \dots, j_w) \in A$

$$\alpha + \sum_{1 \leqslant m \leqslant v} i_m a_m/(b_m p^{s_m}) < \min\{\mathrm{ord}(\widetilde{y}_{q+1}), \mathrm{ord}(\Delta) + 1\},$$

(viii) the number of elements $\#A$ is maximal possible, i.e., there is not a similar expansion with A' in place of A satisfying (i)–(vii) and such that $\#A' > \#A$.

If $\mathrm{ord}(\widetilde{y}_{q+1}) < \mathrm{ord}(\Delta) + 1$ then using the element $\widetilde{y}_{q+1}$ one can construct z_{v+1} or η_{w+1} (may be both of them), define $v(q+1)$, $w(q+1)$ and proceed to the next $(q+1)$-th step.

If $\mathrm{ord}(\widetilde{y}_{q+1}) \geqslant \mathrm{ord}(\Delta) + 1$ then the considered q-th step is final and after that one can construct Σ_j, π_j and expansion (2)

Actually this algorithm is *canonical*. More than that, it is natural to consider the family of expansions (3) for all q as a generalization for nonzero characteristic of one expansion (1) for zero characteristic. Of course we omit details here.

Assume that $f \in k[X, Y]$ and the field k is finitely generated over a primitive subfield. Then the interesting problem is to estimate the complexity of this algorithm and obtain the results in nonzero characteristic similar to [1], [2].

References

[1] **Chistov A. L.:** *"Polynomial complexity of the Newton–Puiseux algorithm"*, in: Lecture Notes in Computer Science, Vol. 233, Springer, 1986, p. 247–255.

[2] **Chistov A. L.:** *"Effective construction of an algebraic variety nonsingular in codimension one over a ground field of zero characteristic"*, Journal of Mathematical Sciences v.179 (2011), Issue 6, p. 729-740.

Alexander L. Chistov
St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia,
e-mail: alch@pdmi.ras.ru