**MATERIAŁY XXIV KONFERENCJI SZKOLENIOWEJ
Z GEOMETRII ANALITYCZNEJ I ALGEBRAICZNEJ
ZESPOLONEJ**

2003 **Łódź** **str. 21**

ALGORYTM NEWTONA I SZEREGI PUISEUX

Andrzej Lenarcik (Kielce)

Naucz nas liczyć dni nasze ... (Ps 90,12)

Wstęp

W atrykule zaprezentowany jest konstruktywny dowód klasycznego twierdzenia Newtona-Puiseux o istnieniu rozwiązania równania $f(X,Y) = 0$, gdzie f jest szeregiem formalnym nad ciałem algebraicznie domkniętym charakterystyki zero. Podajemy przyklad, ze twierdzenie NP nie jest prawdziwe dla ciał o skończonej charakterystyce (Przykład 3.3). Informację na ten temat dla ciał o skończonej charakterystyce można np. znaleźć w [C] lub [R].

Głównym narzędziem w prezentowanym dowodzie jest zmodyfikowany algorym Newtona opracowany na podstawie [W]. Ta wersja algorytmu stosowana jest także w innych pracach np. [Can], [KP]. W literaturze można znaleźć wiele dowodów twierdzenia Newtona-Puiseux. Wymieńmy klasyczne pozycje [A], [BK] [Ch], (...). Obszerny wykład o rozwinięciach Puiseux i diagramach Newtona znajdziemy w [P].

1 Twierdzenie Newtona-Puiseux

Rozważmy szereg formalny $f \in k[[X,Y]]$ ($k = \bar{k}$, $\operatorname{char} k = 0$) bez stałego wyrazu oraz równanie

$$f(X,Y) = 0 \,. \tag{1}$$

Naszym celem jest wyznaczenie szeregu formalnego

$$y(X) = a_1 X^{\theta_1} + a_2 X^{\theta_2} + \dots, \; a_i \neq 0$$

spełniającego (1), gdzie $0 < \theta_1 < \theta_2 < \dots$ są liczbami wymiernym o wspólnym mianowniku. Mamy $y(X) \in k[[X]]^* = \bigcup_{n\geq 1} k[[X^{1/n}]]$ (*zbiór szeregów Puiseux*). Jak zwykle $\operatorname{ord} y(X) = \theta_1$, $\operatorname{in} y(X) = a_1 X^{\theta_1}$ ($\operatorname{ord} 0 = +\infty$, $\operatorname{in} 0 = 0$) oraz $\operatorname{ord}(y_1 y_2) = \operatorname{ord} y_1 + \operatorname{ord} y_2$, $\operatorname{ord}(y_1 + y_2) \geq \min\{\operatorname{ord} y_1, \operatorname{ord} y_2\}$. Każdy szereg Puiseux $y(X) = a_1 X^{\nu_1/n} + a_2 X^{\nu_2/n} + \dots$ spełniający (1) dostarcza parametryzacji $x(T) = T^n$, $y(T) = a_1 T^{\nu_1} + a_2 T^{\nu_2} + \dots$ takiej, że $f(x(T), y(T)) = 0$, $x(T), y(T) \in k[[T]]$.

Dla szeregu $f(X,Y) = \sum f_{\alpha\beta} X^\alpha Y^\beta \in k[[X,Y]]$, $f_{\alpha\beta} \in k$ definiuje się *nośnik* $\operatorname{supp} f = \{(\alpha,\beta) \in \mathbf{R}^2 : \; f_{\alpha\beta} \neq 0\}$. *Diagram Newtona* $\Delta_f = \Delta(f)$ jest najmniejszym zbiorem wypukłym zawierającym $(\operatorname{supp} f) + \mathbf{R}^2_+$ ($\mathbf{R}_+ = \{x : \; x \geq 0\}$). *Łamana Newtona* $\mathcal{N}_f = \mathcal{N}(f)$ jest zbiorem zwartych odcinków brzegu diagramu, parami nierównoległych. Dla odcinka $S \in \mathcal{N}_f$ przez $|S|_1$ i $|S|_2$ oznaczamy długości rzutów S odpowiednio na oś poziomą i pionową. Wielomian $\operatorname{in}(f,S) = \sum_{(\alpha,\beta)\in S} f_{\alpha\beta} X^\alpha Y^\beta$ nazywamy formą początkową szeregu f względem odcinka S.

Teraz możemy wypowiedzieć

Twierdzenie 1.1 (Newton-Puiseux). *Niech $f \in k[[X,Y]] \setminus \{0\}$, $S \in \mathcal{N}_f$ i $a \in k \setminus \{0\}$. Wówczas $aX^{|S|_1/|S|_2}$ jest pierwiastkiem $\operatorname{in}(f,S)$ w $k[[X]]^*$ wtedy i tylko wtedy, gdy istnieje rozwiązanie $y(X) \in k[[X]]^*$ równania $f(X,Y) = 0$ takie, że $\operatorname{in} y(X) = aX^{|S|_1/|S|_2}$.*

Dowód łatwiejszej implikacji ($\Leftarrow$) podany jest w Rozdziale 2 (Wniosek 2.5). Dowód implikacji ($\Rightarrow$) (twierdzenie o istnieniu rozwiązania) znajduje się w Rozdziale 4.

Dla $S \in \mathcal{N}_f$, iloraz $|S|_1/|S|_2$ będziemy nazywać *inklinacją* S; liczby $\alpha(S), \beta(S)$ są takie, że $\alpha/\alpha(S) + \beta/\beta(S) = 1$ jest równaniem prostej zawierającej S.

2 Rodziny sumowalne [C]

W tym rozdziale zastanawiamy się nad sensem algebraicznym wyrażenia $f(X, y(X))$, gdzie $f \in k[[X,Y]]$ i $y(X) \in k[[X]]^*$. Niech $f(X,Y) = \sum_{i=0}^{\infty} Y^i$ i $y(X) = 1 + X$. Wówczas $f(X, y(X)) = \sum_{i=1}^{\infty} (1+X)^i$. Tu niemożliwe jest dodanie do siebie poszczególnych składników w sposób algebraiczny, gdyż nieskończenie wiele jednomianów ma takie same wykładniki.

Definicja 2.1 *Rodzinę $\{\varphi_i\}$, $\varphi_i \in k[[X]]^*$ nazywamy sumowalną, gdy dla każdej dodatniej stałej M zbiór $\{i : \; \operatorname{ord} \varphi_i < M\}$ jest skończony.*

Uwaga 2.2 *Niech $\{\varphi_i\}$, $\varphi_i \in k[[X]]^*$ będzie rodziną sumowalną. Wówczas*

(i) $\sum \varphi_i$ *jest dobrze zdefiniowana,*

(ii) $\min(\operatorname{ord} \varphi_i)$ *jest dobrze zdefiniowane,*

(iii) $\operatorname{ord}(\sum \varphi_i) \geq \min(\operatorname{ord} \varphi_i) = \min.$

(iv) *Nierówność* (iii) *jest ostra wtedy i tylko wtedy, gdy*

$$\sum_{\operatorname{ord}\varphi_i=\min} \operatorname{in}\varphi_i = 0 \ ,$$

i wówczas $\#\{i : \operatorname{ord}\varphi_i = min\} \geq 2$.

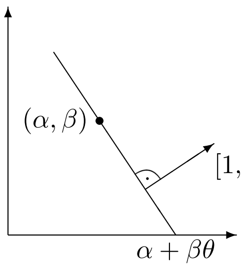
Dowód. Ustalmy wykładnik α. Ponieważ tylko skończona liczba szeregów ma rząd mniejszy od α, więc x^α może wystąpić tylko w tych szeregach. Zatem współczynnik przy x^α jest dobrze zdefiniowany dla dowolnego α i tym samym cała suma.

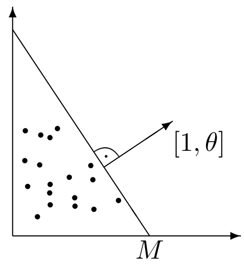
Minimum rzędów jest dobrze określone, gdyż ustalając dowolnie wykładnik α większy od któregokolwiek z rzędów, możemy ograniczyć się do rzędów mniejszych od α, a tych jest skończona liczba.

Nierówność (iii) wynika z inkluzji $\operatorname{supp}(\sum \varphi_i) \subset \bigcup \operatorname{supp}\varphi_i$. Jest ona silna wtedy i tylko wtedy, gdy wyrazy minimalnego rzędu redukują się między sobą. Zatem w tym przypadku wyrazy te muszą pochodzić od co najmniej dwóch szeregów.

Własność 2.3 *Niech* $f = \sum f_{\alpha\beta}X^\alpha Y^\beta \in k[[X,Y]] \setminus \{0\}$ *oraz* $y(X) \in k[[X]]^*$, $\operatorname{ord} y(X) > 0$. *Połóżmy* $\varphi_{\alpha\beta}(X) = f_{\alpha\beta}X^\alpha y(X)^\beta$ *dla* $(\alpha,\beta) \in \operatorname{supp} f$. *Wówczas rodzina* $\{\varphi_{\alpha\beta}\}$ *jest sumowalna.*

Dowód. Jeżeli $y(X) = 0$ w $k[[X]]^*$, to stwierdzenie jest oczywiste, gdyż rodzina $\{f_{\alpha,0}X^\alpha\}$ jest sumowalna. Jeżeli $y(X) \neq 0$, to oznaczmy $\theta = \operatorname{ord} y(X)$, $0 < \theta < +\infty$. Mamy $\operatorname{ord}\varphi_{\alpha\beta} = \alpha + \beta\theta$. Ta liczba ma interpretację geometryczną. Prosta, która przechodzi przez (α,β), prostopadła do wektora $[1,\theta]$, przecina oś poziomą w punkcie o odciętej $\alpha+\beta\theta$. Ustalmy $M > 0$.





Prosta $\alpha + \beta\theta = M$ jest prostopadłą do $[1,\theta]$ i przechodzi przez $(M,0)$. Aby zakończyć dowód wystarczy zauważyć, że

$$\operatorname{ord}\varphi_{\alpha\beta} < M \Leftrightarrow (\alpha,\beta) \text{ leży poniżej prostej .}$$

Łącząc Uwagę 2.2 z Własnością 2.3 otrzymujemy

Wniosek 2.4 (przy wcześniejszych założeniach i oznaczeniach)

(i) $f(X,y(X)) = \sum \varphi_{\alpha\beta}$ *jest dobrze zdefiniowana,*

(ii) $\operatorname{ord} f(X,y(X))$ *jest dobrze zdefiniowany,*

(iii) $\operatorname{ord} f(X, y(X)) \geq \min\{\alpha + \beta\theta : (\alpha, \beta) \in \operatorname{supp} f\} = \min$.

(iv) *Nierówność w* (iii) *jest ostra wtedy i tylko wtedy, gdy* $\sum_{\alpha+\beta\theta=\min} \operatorname{in} \varphi_{\alpha\beta} = 0$ *i wówczas zbiór* $\{(\alpha, \beta) \in \operatorname{supp} f : \alpha + \beta\theta = \min\}$ *jest co najmniej dwuelementowy.*

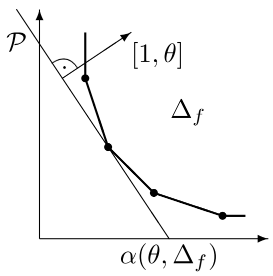
Liczba $\alpha(\theta, \Delta_f) = \min\{\alpha + \beta\theta : (\alpha, \beta) \in \operatorname{supp} f\}$, występująca w (iii), może być zinterpretowana geometrycznie. Prosta $\mathcal{P}$ podpierająca diagram Δ_f, prostopadła do $[1, \theta]$, przecina oś poziomą w punkcie o odciętej $\alpha(\theta, \Delta_f)$.

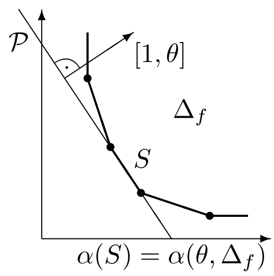
Zdefiniujmy *formę początkową względem kierunku* $[1, \theta]$ [1]

$$\operatorname{in}(f, \theta) = \sum_{\alpha+\beta\theta=\alpha(\theta,\Delta_f)} f_{\alpha\beta} X^\alpha Y^\beta .$$

Ponieważ $\operatorname{in} \varphi_{\alpha\beta} = \operatorname{in}[f_{\alpha\beta} X^\alpha y(X)^\beta] = f_{\alpha\beta} X^\alpha [\operatorname{in} y(X)]^\beta$ zatem

$$\sum_{\alpha+\beta\theta=\alpha(\theta,\Delta_f)} \operatorname{in} \varphi_{\alpha\beta} = \operatorname{in}(f, \theta)(X, \operatorname{in} y(X)) .$$





Jeżeli zbiór punktów $(\alpha, \beta) \in \operatorname{supp} f$ takich, że $\alpha + \beta\theta = \alpha(\theta, \Delta_f)$ ma przynajmniej dwa elementy, wówczas istnieje $S \in \mathcal{N}_f$ zawarty w prostej $\mathcal{P}$. W tym przypadku $\theta = |S|_1/|S|_2$ oraz $\operatorname{in}(f, \theta) = \operatorname{in}(f, S)$. Wówczas będziemy oznaczać $\alpha(\theta, \Delta_f) =: \alpha(S)$. Uwzględniając nowe oznaczenia można powtórnie zredagować Własności 2.4 (iii) oraz (iv).

(iii)′ Jeżeli rząd $\theta = \operatorname{ord} y(X)$ jest dodatni, to $\operatorname{ord} f(X, y(X)) \geq \alpha(\theta, \Delta_f)$.

(iv)′ Nierówność w (iii)′ jest ostra wtedy i tylko wtedy, gdy istnieje $S \in \mathcal{N}_f$ taki, że $\theta = |S|_1/|S|_2$ oraz

$$\operatorname{in}(f, S)(X, \operatorname{in} y(X)) = 0 . \tag{2}$$

Od razu mamy

Wniosek 2.5 *Jeżeli* $y(X) \in k[[X]]^*$, $0 < \operatorname{ord} y(X) < +\infty$ *jest rozwiązaniem równania* $f(X, Y) = 0$, *to istnieje* $S \in \mathcal{N}_f$ *taki, że zachodzi (2).*

[1] Notacja może być nieco myląca, gdyż używamy liczby θ lub odcinka S na miejscu kropki w $\operatorname{in}(f, \cdot)$.

Dowód. Jeżeli $f(X, y(X)) = 0$, to oczywiście $+\infty = \operatorname{ord} f(X, y(X)) > \alpha(\theta, \Delta_f)$ i korzystamy z (iv)$'$.

W ten sposób udowodniliśmy implikację ($\Leftarrow$) w Twierdzeniu 1.1.

3 Algorytm Newtona

Wniosek 2.5 podpowiada, że aby wyznaczyć pierwszy wyraz rozwiązania o dodatnim rzędzie, wystarczy wziąć pod uwagę pierwiastki formy początkowej $\operatorname{in}(f, S)$ w $k[[X]]^*$ dla $S \in \mathcal{N}_f$. Zauważmy, że $y = 0$ jest rozwiązaniem $f(X, Y) = 0$ wtedy i tylko wtedy, gdy

$$y \mid f \Leftrightarrow f(X, 0) = 0 \Leftrightarrow \Delta_f \text{ nie dotyka osi poziomej.}$$

Idea algorytmu Newtona jest następująca. Niech $a_1 X^{\theta_1}$ będzie formą początkową rozwiązania

$$y(X) = a_1 X^{\theta_1} + a_2 X^{\theta_2} + a_3 X^{\theta_3} + \dots \ .$$

Aby znaleźć drugi wyraz oznaczmy

$$\tilde{y}(X) = a_2 X^{\theta_2} + a_3 X^{\theta_3} + \dots \ .$$

Mamy

$$\begin{aligned} 0 &= f(X, y(X)) = f(X, a_1 X^{\theta_1} + a_2 X^{\theta_2} + a_3 X^{\theta_3} + \dots) \\ &= f(X, a_1 X^{\theta_1} + \tilde{y}(X)) \\ &= \tilde{f}(X, \tilde{y}(X)) \ , \end{aligned}$$

gdzie

$$\tilde{f}(X, Y) = f(X, a_1 X^{\theta_1} + Y) \ .$$

Zatem w celu wyznaczenia $a_2 X^{\theta_2}$ wystarczy wybrać $\tilde{S} \in \mathcal{N}(\tilde{f})$ taki, że $|\tilde{S}|_1 / |\tilde{S}|_2 > \theta_1$ a następnie dowolny pierwiastek formy $\operatorname{in}(\tilde{f}, \tilde{S})$. Ta procedura może być kontynuowana.

Teraz posłużymy się wyżej zaprezentowaną ideą w trzech konkretnych przykładach.

Przykład 3.1 Rozważmy równanie $Y^3 + Y - X = 0$. Support ma trzy punkty $(0, 3)$, $(0, 1)$ i $(1, 0)$. Łamana Newtona $\mathcal{N}_f$ ma jeden odcinek S, który łączy $(0, 1)$ i $(1, 0)$. Mamy $\operatorname{in}(f, S) = Y - X$ z jedynym pierwiastkiem $y(X) = X$. Zatem

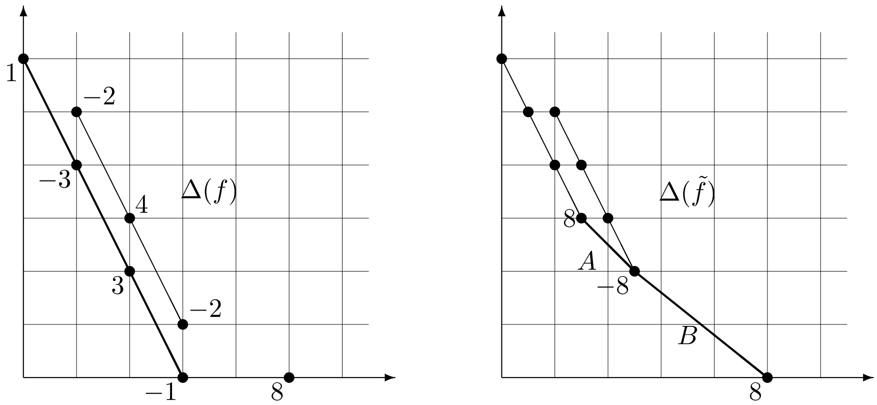
$$\tilde{f}(X, Y) = f(X, X + Y) = (X + Y)^3 + Y \ .$$

Łamana $\mathcal{N}(\tilde{f})$ ma jeden odcinek łączący $(0, 1)$ z $(3, 0)$ oraz $\operatorname{in}(\tilde{f}, \tilde{S}) = Y + X^3$ z jedynym pierwiastkiem $y(X) = -X^3$. Możemy kontynuować: $\tilde{\tilde{f}}(X, Y) = \tilde{f}(X, -X^3 + Y) = 3X^2(-X^3 + Y) + 3X(-X^3 + Y)^2 + Y^3 + Y$. Mamy jeden odcinek $\tilde{\tilde{S}} \in \mathcal{N}(\tilde{\tilde{f}})$

i $\mathrm{in}(\tilde{\tilde{f}}, \tilde{\tilde{S}}) = Y - 3X^5$ z pierwiastkiem $y(X) = 3X^5$. Otrzymaliśmy trzy wyrazy rozwiązania

$$y(X) = X - X^3 + 3X^5 - \dots \,.$$

W tym przypadku można także stosować twierdzenie o funkcji uwikłanej, gdyż szereg f jest nieosobliwy w zerze.



Przykład 3.2 Teraz rozważmy krzywą osobliwą $f = Y^6 - 3XY^4 + 3X^2Y^2 - X^3 - 2XY^5 + 4X^2Y^3 - 2X^3Y + 8X^5$. Możemy zapisać prościej $f = (Y^2 - X)^3 - 2XY(Y^2 - X)^2 + 8X^5$. Mamy dokładnie jeden odcinek $S \in \mathcal{N}_f$, który łączy $(0, 6)$ z $(3, 0)$. Forma $\mathrm{in}(f, S) = (Y^2 - X)^3 = (Y - X^{1/2})^3 (Y + X^{1/2})^3$ ma dwa pierwiastki $X^{1/2}$ oraz $-X^{1/2}$ w $k[[X]]^*$ (nie uwzględniamy krotności), dlatego mamy dwie możliwości kontynuowania algorytmu. Wybierzmy najpierw $y(X) = X^{1/2}$ i połóżmy

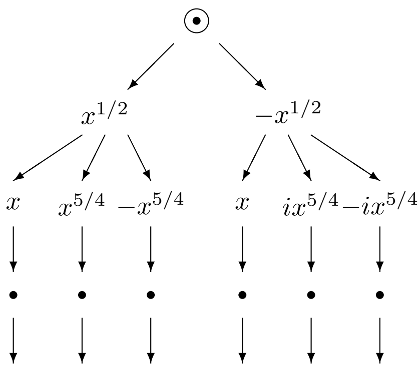
$$\begin{aligned} \tilde{f}(X, Y) &= f(X, X^{1/2} + Y) = \\ &= Y^3(Y + 2X^{1/2})^3 - 2X(Y + X^{1/2})Y^2(Y + 2X^{1/2})^2 + 8X^5 \,. \end{aligned}$$

Łamana $\mathcal{N}(\tilde{f})$ ma teraz dwa odcinki o inklinacji większej od $1/2$: odcinek A, który łączy wierzchołki $(3/2, 3)$ i $(5/2, 2)$ oraz odcinek B łączący $(5/2, 2)$ i $(5, 0)$. Mamy

$$\begin{aligned} \mathrm{in}(\tilde{f}, A) &= 8X^{3/2}Y^3 - 8X^{5/2}Y^2 = 8X^{3/2}Y^2(Y - X) \,, \\ \mathrm{in}(\tilde{f}, B) &= -8X^{5/2}(Y - X^{5/4})(Y + X^{5/4}) \,, \end{aligned}$$

zatem istnieją trzy możliwości kontynuowania algorytmu. Analogicznie otrzymamy trzy ścieżki startując od pierwiastka $y(X) = -X^{1/2}$. W dalszych krokach nie będzie już więcej rozgałęzień. Otrzymaliśmy sześć rozwiązań

$$\begin{aligned} y_1(X) &= X^{1/2} + X + \dots \,, & y_4(X) &= -X^{1/2} + X + \dots \,, \\ y_2(X) &= X^{1/2} + X^{5/4} + \dots \,, & y_5(X) &= -X^{1/2} + iX^{5/4} + \dots \,, \\ y_3(X) &= X^{1/2} - X^{5/4} + \dots \,, & y_6(X) &= -X^{1/2} - iX^{5/4} + \dots \,. \end{aligned}$$



Przykład 3.3 Stosując algorytm Newtona do $f = Y^2+X+XY$ w charakterystyce 2 otrzymamy szereg

$$y(X) = X^{1/2} + X^{3/4} + X^{7/8} + X^{15/16} + X^{31/32} + \ldots \ .$$

Łatwo sprawdzić, że $y(X)$ jest rzeczywiście rozwiązaniem, gdyż $(c_1 + c_2 + \ldots)^2 = c_1^2 + c_2^2 + \ldots$. Zatem

$$y(X)^2 + X + X\,y(X) = 2(X^{1/2} + X^{3/4} + X^{7/8} + X^{15/16} + X^{31/32} + \ldots) = 0\ .$$

Przykład ten pokazuje, że w charakterystyce skończonej algorytm Newtona może prowadzić do rozwiązań, które nie są szeregami Puiseux.

Rozdział ten zakończymy następującym komentarzem.

Komentarz 3.4 Aby stosować kolejne kroki algorytmu Newtona musimy rozważać szeregi $f(X,Y) = \sum f_{\alpha\beta} X^\alpha Y^\beta \in k[[X^{1/Q}, Y]]$ dla dodatnich całkowitych Q. Oczywiście możemy tutaj zdefiniować Δ_f oraz $\mathcal{N}_f$. Również na te szeregi w sposób naturalny uogólniamy pojęcie rodziny sumowalnej. Wówczas dla $y(X) \in k[[X]]^*$, $\operatorname{ord} y(X) > 0$, możemy poprawnie zdefiniować $f(X, y(X)+Y)$ jako sumę rodziny $\{\varphi_{\alpha\beta}\}$, gdzie $\varphi_{\alpha\beta} = f_{\alpha\beta} X^\alpha (y(X)+Y)^\beta$. Ponadto dla $y(X)$ istnieje minimalne q takie, że $y(X) \in k[[X^{1/q}]]$. Wówczas $f(X, y(X)+Y) \in k[[X^{1/Qq}, Y]]$.

4 Dowód istnienia rozwiązania

W tym rozdziale dowodzimy implikacji ($\Rightarrow$) w Twierdzeniu 1.1. Trzeba udowodnić, że:

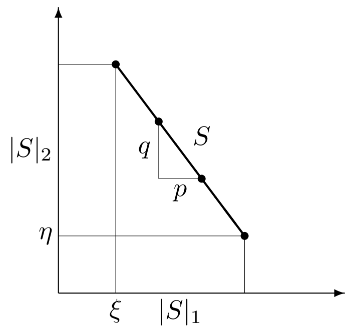
- kontynuacja algorytmu jest zawsze możliwa,
- istnieje wspólny mianownik dla wszystkich wykładników,
- zbudowany szereg spełnia równanie.

Zaczniemy od następujących faktów. Przez *formę quasi-jednorodną* rozumiemy wielomian, którego nośnik zawarty jest w prostej.

Fakt 4.1 *Niech* $g(X,Y) \in k[X,Y]$ *będzie formą quasi-jednorodną, której nośnik ma przynajmniej dwa punkty. Połóżmy* $S = \operatorname{conv}(\operatorname{supp} g)$. *Wówczas*

(a) *istnieje* h *forma jednorodna stopnia* $d = \mathrm{NWP}(|S|_1, |S|_2)$ *taka, że* $g(X,Y) = X^\xi Y^\eta h(X^p, Y^q)$ *gdzie* $p = |S|_1/d$, $q = |S|_2/d$.

(b) *Jeżeli* $g(X,Y)$ *ma tylko jeden pierwiastem w* $k[[X]]^*$ *(bez krotności), to musi być* $q = 1$, $\eta = 0$ *oraz* h *musi być czystą potęgą.*



Dowód. (a) Można zapisać g w postaci $g = X^\xi Y^\eta g_1$, gdzie $g_1 = aX^{|S|_1} + \ldots + bY^{|S|_2} \in k[X,Y]$, $ab \neq 0$. Jeżeli $(\alpha, \beta) \in \operatorname{supp} g_1$ wówczas $\alpha/|S|_1 + \beta/|S|_2 = 1$. Teraz sprawdzamy, że dla każdego takiego (α,β) istnieją i,j takie, że $(X^p)^i (Y^q)^j = X^\alpha Y^\beta$, $i + j = d$, skąd $g_1(X,Y) = h(X^p, Y^q)$ i h jest formą jednorodną stopnia d.

(b) Niech teraz $h(X,Y) = b(Y - c_1 X)^{r_1} \ldots (Y - c_s X)^{r_s}$ gdzie $c_1, \ldots, c_s \in k \setminus \{0\}$ są parami różne. Wówczas

$$g(X,Y) = bX^\xi Y^\eta (Y^q - c_1 X^p)^{r_1} \ldots (Y^q - c_s X^p)^{r_s}$$

jest rozkładem g na czynniki w $k[X,Y]$ (również w $k[[X,Y]]$). Ponieważ $\operatorname{char} k = 0$, c_i ma dokładnie q różnych pierwiastków $c_{i,1}, \ldots, c_{i,q}$ stopnia q. ([B], Tw. 3, Rozdz. IV, Par. 1). Dla dowolnego $i = 1, \ldots, s$ mamy zatem rozkład

$$Y^q - c_i X^p = (Y - c_{i,1} X^{p/q}) \ldots (Y - c_{i,q} X^{p/q}) \,.$$

Otrzymujemy w ten sposób rozkład formy $g(X,Y)$ na czynniki w $k[[X^{1/q}, Y]]$, przy czym wszystkie $c_{1,1}, \ldots, c_{1,q}, \ldots, c_{s,1}, \ldots, c_{s,q} \in k \setminus \{0\}$ są różne!

Jeżeli teraz g ma tylko jeden pierwiastek w $k[[X]]^*$, to $s = q = 1$ oraz $\eta = 0$. W tym przypadku

$$g(X,Y) = bX^\xi (Y - cX^p)^r \,.$$

Będziemy potrzebować poniższego ogólniejszego sformułowania Faktu 4.1. Formą quasi-jednorodną nazywamy wielomian, którego nośnik zawarty jest w pewnej prostej.

Fakt 4.2 *Niech* $g(X,Y) \in k[X^{1/Q}, Y]$ *będzie formą quasi-jednorodną taką, że* $\#\operatorname{supp} g \geq 2$. *Połóżmy* $S = \operatorname{conv}(\operatorname{supp} g)$. *Wówczas*

(a) *istnieje forma jednorodna h stopnia* $d = \mathrm{NWP}(|S|_1 Q, |S|_2)$ *taka, że* $g(X,Y) = X^\xi Y^\eta h(X^{p/Q}, Y^q)$ *gdzie* $p = |S|_1 Q/d$, $q = |S|_2/d$.

(b) *Jeżeli* $g(X,Y)$ *ma dokładnie jeden pierwiastek w* $k[[X]]^*$ *(bez krotności), to* $q = 1$, $\eta = 0$ *oraz h jest czystą potęgą.*

Dowód. Bierzemy $\bar{g}(X,Y) = g(X^Q, Y)$ i stosujemy Fakt 4.1.

Poniższy lemat opisuje jeden krok algorytmu Newtona.

Lemat 4.3 *Niech* $f \in k[[X^{1/Q}, Y]]$, $S \in \mathcal{N}_f$, $Y = aX^\theta$ *pierwiastek* $\mathrm{in}(f,S)$. *Niech* p, q *będą względnie pierwsze takie, że* $\theta = |S|_1/|S|_2 = p/(Qq)$. *Połóżmy* $\tilde{f}(X,Y) = f(X, aX^\theta + Y) \in k[[X^{1/(Qq)}, Y]]$. *Wówczas co najmniej jeden z poniższych warunków jest spełniony:*

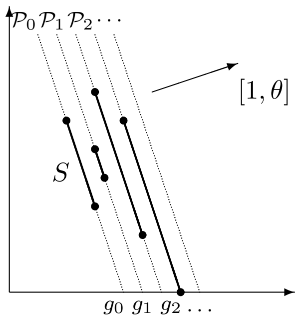
(I) $y(X) = 0$ *jest rozwiązaniem równania* $\tilde{f}(X,Y) = 0$,

(II) *istnieje odcinek* $\tilde{S} \in \mathcal{N}(\tilde{f})$ *taki, że*

(a) $|\tilde{S}|_1/|\tilde{S}|_2 > |S|_1/|S|_2$,

(b) $\alpha(\tilde{S}) \geq \alpha(S) + 1/(Qq)$,

(c) $\deg_Y \mathrm{in}(f,S) \geq \deg_Y \mathrm{in}(\tilde{f}, \tilde{S})$ *i jeżeli zachodzi równość, to* $q = 1$.



Dowód. Istnieje rozkład (skończony lub nieskończony)

$$f = g_0 + g_1 + g_2 + \dots\ , \tag{3}$$

gdzie $g_0, g_1, g_2, \ldots$ jest ciągiem niezerowych form quasi-jednorodnych, $g_0 = \mathrm{in}(f,S)$, $g_j \in k[X^{1/Q}, Y]$ oraz istnieje ciąg prostych $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \ldots$ równoległych do odcinka S takich, że $\mathrm{supp}\, g_j \subset \mathcal{P}_j$. Można sprawdzić, że odcięta punktu przecięcia każdej prostej z osią poziomą ma postać

$$(\text{liczba całkowita})/(Qq)\ . \tag{4}$$

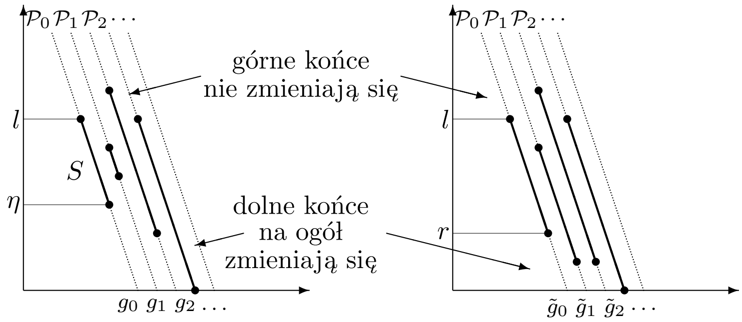
Ponieważ $\theta = |S|_1/|S|_2$, zatem po podstawieniu $aX^\theta + Y$ w miejsce Y dla każdego j, support formy quasi-jednorodnej $\tilde{g}_j(X,Y) = g_j(X, aX^\theta + Y)$ pozostaje wewnątrz prostej $\mathcal{P}_j$. To znaczy, że suma

$$\tilde{f} = \tilde{g}_0 + \tilde{g}_1 + \tilde{g}_2 + \dots \tag{5}$$

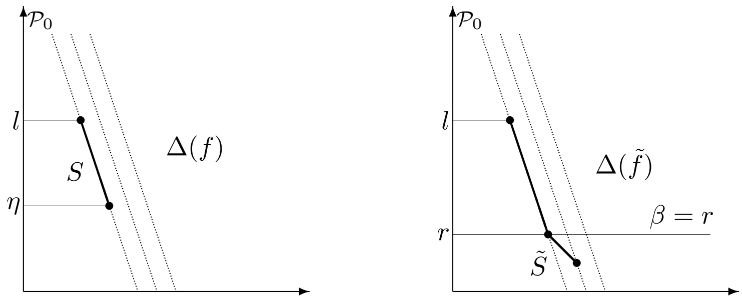
jest rozwinięciem postaci (3) dla $\tilde{f}$ i mamy ważną równość

$$\mathrm{in}(\tilde{f},\theta)(X,Y) = \tilde{g}_0(X,Y) = g_0(X, aX^\theta + Y) = \mathrm{in}(f,S)(X, aX^\theta + Y)\ .$$

Teraz porównajmy rozwinięcia (3) i (5). Górne końce $\operatorname{supp} g_j$ oraz $\operatorname{supp} \tilde{g}_j$ są identyczne ze względu na $\deg_Y g_j = \deg_Y \tilde{g}_j$, ale dolne końce ogólnie rzecz biorąc zmieniają się. Łatwo pokazać, że rzędne dolnych końców dla $\operatorname{supp} \tilde{g}_j$ są takie same jak krotności aX^θ jako pierwiastka g_j. Oznaczmy $l = \deg_Y g_0 = \deg_Y \mathrm{in}(f,S)$ i niech r będzie krotnością aX^θ jako pierwiastka $\mathrm{in}(f,S)$. Mamy $l \geq r \geq 1$. Jeżeli zbiór $\{(\alpha,\beta) :\ \beta < r\} \cap \operatorname{supp} \tilde{f}$ jest pusty wówczas $\tilde{f}$ dzieli się przez Y i warunek (I) lematu jest spełniony.



Załóżmy, że $\{(\alpha,\beta) :\ \beta < r\} \cap \operatorname{supp} \tilde{f}$ jest niepusty. Wówczas istnieje odcinek $\tilde{S} \in \mathcal{N}(\tilde{f})$ poniżej prostej $\beta = r$.



Nierówność (a) jest jasna. Nierówność (b) jest konsekwencją (4). Dla sprawdzenia nierówności w (c) wystarczy zauważyć

$$\deg_Y \mathrm{in}(f,S) = l \geq r \geq \deg_Y \mathrm{in}(\tilde{f},\tilde{S})\ .$$

Jeżeli teraz $\deg_Y \mathrm{in}(f,S) = \deg_Y \mathrm{in}(\tilde{f},\tilde{S})$ wówczas $l = r$ i aX^θ jest jedynym pierwiastkiem $\mathrm{in}(f,S)$ w $k[[X]]^*$. Z Faktu 4.2(b) mamy $q = 1$, co kończy dowód lematu.

Dowód twierdzenia 1.1 ($\Rightarrow$). Korzystając z Lematu 4.3 można skonstruować skończoną lub nieskończoną liczbę kolejnych wyrazów rozwiązania. W każdej iteracji stosujemy punkt (I) lub (II) lematu. Należy podkreślić, że wybór ścieżki algorytmu na ogół nie jest jednoznaczny. Jeżeli (I) zostało wybrane w jakimkolwiek kroku, to procedura jest przerywana i zbudowane rozwiązanie posiada skończoną liczbę składników.

Zacznijmy od $f(X,Y) \in k[[X,Y]]$, $S \in \mathcal{N}_f$ i aX^θ jest pierwiastkiem $\mathrm{in}(f,S)$ ($\theta = |S|_1/|S|_2$). Połóżmy $f^{(1)} = f$, $S^{(1)} = S$, $a_1X^{\theta_1} = aX^\theta$, $Q_1 = 1$. Załóżmy, że ciągi

$$f^{(1)},\ldots,f^{(i)}; \quad S^{(1)},\ldots,S^{(i)}; \quad a_1X^{\theta_1},\ldots,a_iX^{\theta_i}; \quad Q_1,\ldots,Q_i;$$

zostały już zdefiniowane. Teraz można zastosować lemat do $f^{(i)}(X,Y) \in k[[X^{1/Q_i},Y]]$, $S^{(i)} \in \mathcal{N}(f^{(i)})$ oraz $a_iX^{\theta_i}$ jako pierwiastka $\mathrm{in}(f^{(i)},S^{(i)})$. Niech $p_i,q_i > 0$ będą względnie pierwsze takie, że $|S^{(i)}|_1/|S^{(i)}|_2 = p_i/(Q_iq_i)$. Połóżmy $Q_{i+1} = Q_iq_i$ i rozważmy

$$f^{(i+1)}(X,Y) := \widetilde{f^{(i)}}(X,Y) = f^{(i)}(X, a_iX^{\theta_i} + Y) \in k[[X^{1/Q_{i+1}},Y]]\ .$$

Jeżeli zostało wybrane rozwiązanie $y=0$ równania $f^{(i+1)} = 0$, wówczas

$$y(X) = a_1X^{\theta_1} + \ldots + a_iX^{\theta_i}$$

jest rozwiązaniem dla $f=0$, gdyż

$$\begin{aligned} 0 &= f^{(i+1)}(X,0) = f^{(i)}(X,a_iX^{\theta_i}) = \ldots = f^{(1)}(X, a_1X^{\theta_1} + \ldots + a_iX^{\theta_i}) \\ &= f(X,y(X))\ . \end{aligned}$$

Drugą możliwością (Lemat 4.3 II)jest wybór odcinka $S^{(i+1)} = \widetilde{S^{(i)}} \in \mathcal{N}(f^{(i+1)})$ o inklinacji θ_{i+1} silnie większej od inklinacji odcinka $S^{(i)}$. Wystarczy rozważyć sytuację kiedy druga możliwość jest wybierana zawsze. Połóżmy

$$y(X) = a_1X^{\theta_1} + a_2X^{\theta_2} + \ldots\ .$$

Należy pokazać, że $y(X) \in k[[X]]^*$, to znaczy, istnieje wspólny mianownik dla $\theta_1,\theta_2,\ldots$. Niech $l_i = \deg_Y \mathrm{in}(f^{(i)},S^{(i)})$. Z Lematu 4.3 II(c) mamy $l_1 \geq l_2 \geq \ldots$. Ponieważ l_i są całkowite dodatnie, zatem istnieje j takie, że $l_j = l_{j+1} = \ldots$. Z tego samego punktu lematu mamy $1 = q_j = q_{j+1} = \ldots$ oraz $Q := Q_{j+1} = Q_{j+2} = \ldots$ jest wspólnym mianownikiem.

Dla zakończenia dowodu wystarczy pokazać, że $y(X)$ jest faktycznie rozwiązaniem. Sprawdzimy, że $\mathrm{ord}\, f(X,y(X)) > M$ dla dowolnego $M > 0$. Połóżmy $\psi_i(X) = a_{i+1}X^{\theta_{i+1}} + a_{i+2}X^{\theta_{i+2}} + \ldots$. Mamy $f(X,y(X)) = f^{(1)}(X,\psi_1(X)) = f^{(2)}(X,\psi_2(X)) = \ldots$. Z Wniosku 2.4 (iii)$'$

$$\mathrm{ord}\, f^{(i)}(X,\psi_i(X)) \geq \alpha(\theta_i, \Delta(f^{(i)}) = \alpha(S^{(i)})\ .$$

I z punktu II(b) Lematu 4.3

$$\lim_{i\to\infty} \alpha(S^{(i)}) = +\infty\ .$$

Bibliografia

[A] S. S. Abhyankar, *Expansion Techniques in Algebraic Geometry*, TATA Institute of Fundamental Research, Bombay 1977.

[B] J. Browkin, *Wybrane Zagadnienia Algebry*, PWN, Warszawa 1968.

[C] H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann, Paris, 1961.

[BK] E. Brieskorn, H. Knörer, *Ebene Algebraische Kurven*, Birkhäuser (1981).

[Cam] A. Campillo, *Algebroid Curves in Positive Characteristic*, Lectures Notes in Math. 813, Springer Verlag 1980.

[Can] J. Cano, *The Puiseux theorem for differential equations*, in D. T. Lê, K. Saito, B. Teissier (eds), *Singularity Theory*, Word Scientific Publ., 1995, 128–152.

[Ch] A. Chenciner, *Courbes algébriques planes*, Publ. Math. Univ. Paris VII, 1979.

[KP] T. C. Kuo, A. Parusiński, *Newton polygon relative to an arc*, preprint (1998).

[P] A. Płoski, *Szeregi Puiseux, diagramy Newtona i odwzorowania holomorficzne płaszczyzny* $\mathbf{C}^2$, Materiały X Konferencji Szkoleniowej z Teorii Zagadnień Ekstremalnych, Łódź (1989), 74–99.

[R] P. Russel, *Hamburger–Noether expansions and approximate roots of polynomials*, Manuscripta Math. 31, (1980), 25–95.

[W] R. Walker, *Algebraic curves*, Princeton Uniwersity Press 1950.

NEWTON ALGORITHM AND PUISEUX SERIES

Summary. We present a constructive proof of classical Newton-Puiseux theorem for formal power series in two variables over a field with characteristic zero. An example that the theorem is not true for finite characteristic is given.

Łódź, 6 – 10 stycznia 2003 r.