RUGOWNIK SYLVESTERA I JAKOBIAN

Arkadiusz Płoski (Kielce)

Pojęcie rugownika należy do algebry klasycznej. W ostatnich latach w związku ze wzrostem znaczenia metod efektywnych algebry ukazało się wiele podręczników i artykułów poświęconych temu pojęciu. Jednak nie wszystkie użyteczne własności rugownika są dostatecznie znane: do nich należy formuła dla rugownika jako jakobianu pewnego ciągu wielomianów. Celem tego artykułu jest przypomnienie tej formuły należącej do Nasha (por. [8], str 412) i zastosowanie jej do dowodu lematu Hensela (por. [6], Rozdział I i [9]). Klasyczny wykład własności rugownika Czytelnik znajdzie w podręczniku A. Mostowskiego i M. Starka [7]. Wiele interesujących twierdzeń o rugowniku można znaleźć w podręcznikach [2] oraz [3] gdzie mimo encyklopedycznego charakteru tych książek związek z jakobianem nie jest wspomniany. Z nowszych artykułów o rugowniku cytujemy [4], autorzy podają tam jawny opis jednomianów występujących w rugowniku. Szereg zastosowań tytułowego pojęcia Czytelnik znajdzie w artykułach [10, 11, 12].

1 Rugownik

Niech $m > 0$ i $n > 0$ będą liczbami całkowitymi. Ustalmy dwa ciągi zmiennych $\vec{A} = (A_0, \dots, A_n)$, $\vec{B} = (B_0, \dots, B_m)$ i rozważmy wielomiany jednej zmiennej X o ogólnych współczynnikach $F(\vec{A}, X) = A_0X^n + A_1X^{n-1} + \cdots + A_n$ oraz $G(\vec{B}, X) = B_0X^m + B_1X^{m-1} + \cdots + B_m$. Są to elementy pierścienia $\mathbb{Z}[\vec{A}, \vec{B}][X]$. W pierścieniu tym rozważamy ciąg wielomianów $P_0(X) = X^{m-1}F(X)$, $P_1(X) = X^{m-2}F(X)$, ... , $P_{m-1}(X) = F(X)$, $P_m(X) = X^{n-1}G(X)$, $P_{m+1}(X) = X^{n-2}G(X), \dots, P_{m+n-1}(X) = G(X)$. Napiszmy $P_i(X) = c_{i0}(\vec{A}, \vec{B})X^{m+n-1} + c_{i1}(\vec{A}, \vec{B})X^{m+n-2} + \cdots + c_{i,m+n-1}(\vec{A}, \vec{B})X^{m+n-1}$ dla $i = 0, 1, \dots, m + n - 1$ i rozważmy macierz

$$SYL(\vec{A}, \vec{B}) = [c_{ij}(\vec{A}, \vec{B})]_{\substack{i=0,1,\dots,m+n-1 \\ j=0,1,\dots,m+n-1}} .$$

Macierz wyżej zdefiniowaną nazywamy macierzą Sylvestera. Pierwsze m wierszy macierzy Sylvestera zawiera ciąg $A_0, \dots, A_n$ oraz zera, ostatnie n wierszy tej macierzy zawiera ciąg $B_0, \dots, B_m$ oraz zera.

Rugownikiem Sylvestera (dalej krótko: rugownikiem) nazywamy wyznacznik $R(\vec{A}, \vec{B}) = \det SYL(\vec{A}, \vec{B}) \in \mathbb{Z}[\vec{A}, \vec{B}]$.

PRZYKŁAD. Niech $n = 3$ i $m = 2$. Wówczas $F(\vec{A}, X) = A_0X^3 + A_1X^2 + A_2X + A_3$, $G(\vec{B}, X) = B_0X^2 + B_1X + B_2$. Mamy

$$
\begin{aligned}
XF(\vec{A},X) &= A_0X^4 + A_1X^3 + A_2X^2 + A_3X + \ 0 \\
F(\vec{A},X) &= \ 0 \ X^4 + A_0X^3 + A_1X^2 + A_2X + A_3 \\
X^2G(\vec{B},X) &= B_0X^4 + B_1X^3 + B_2X^2 + \ 0 \ X + \ 0 \\
XG(\vec{B},X) &= \ 0 \ X^4 + B_0X^3 + B_1X^2 + B_2X + \ 0 \\
G(\vec{B},X) &= \ 0 \ X^4 + \ 0 \ X^3 + B_0X^2 + B_1X + B_2
\end{aligned}
$$

a więc

$$
R(\vec{A},\vec{B}) = \begin{vmatrix} A_0 & A_1 & A_2 & A_3 & 0 \\ 0 & A_0 & A_1 & A_2 & A_3 \\ B_0 & B_1 & B_2 & 0 & 0 \\ 0 & B_0 & B_1 & B_2 & 0 \\ 0 & 0 & B_0 & B_1 & B_2 \end{vmatrix}.
$$

Przypomnijmy podstawową własność rugownika.

Własność 1 *Niech $\mathbb{K}$ będzie ciałem i niech $\vec{a} = (a_0, \ldots, a_n) \in \mathbb{K}^{n+1}$ i $\vec{b} = (b_0, \ldots, b_m) \in \mathbb{K}^{m+1}$ będą takimi ciągami, że $a_0 \neq 0$ lub $b_0 \neq 0$. Wtedy wielomiany $F(\vec{a},X), G(\vec{b},X) \in \mathbb{K}[X]$ mają wspólny dzielnik dodatniego stopnia wtedy i tylko wtedy, gdy $R(\vec{a},\vec{b}) = 0$.*

Dowód. Wprost z definicji rugownika wynika, że warunek $R(\vec{a},\vec{b}) = 0$ zachodzi dokładnie wtedy, gdy ciąg wielomianów $X^{m-1}F(\vec{a},X), \ldots, F(\vec{a},X)$, $X^{n-1}G(\vec{b},X), \ldots, G(\vec{b},X)$ jest liniowo zależny nad ciałem $\mathbb{K}$. Oznacza to, że istnieją $\Phi(X), \Psi(X) \in \mathbb{K}[X]$ nie równe jednocześnie zero takie, że $\Phi(X)F(\vec{a},X) = \Psi(X)G(\vec{b},X)$ przy czym obie strony równości są stopnia $\leqslant m+n-1$. Jest to równoważne z istnieniem wspólnego podzielnika dodatniego stopnia wielomianów $F(\vec{a},X), G(\vec{b},X)$ (por. [7], Lemat na stronie 103). $\square$

2 Rugownik i jakobian

Zatrzymujemy oznaczenia wprowadzone wyżej. Rozważmy tożsamość

$$
\begin{aligned}
&F(\vec{A},X)G(\vec{B},X) = \\
(1) \qquad &\quad = Q_0(\vec{A},\vec{B})X^{m+n} + Q_1(\vec{A},\vec{B})X^{m+n-1} + \cdots + Q_{m+n}(\vec{A},\vec{B})
\end{aligned}
$$

w pierścieniu $\mathbb{Z}[\vec{A},\vec{B}][X]$. Jest więc $Q_0(\vec{A},\vec{B}) = A_0B_0, Q_1(\vec{A},\vec{B}) = A_0B_1 + A_1B_0, \ldots, Q_{m+n}(\vec{A},\vec{B}) = A_nB_m$.

Mamy

Własność 2

$$
\begin{aligned}
(2.1) \qquad SYL(\vec{A},\vec{B}) &= \tfrac{J(Q_1, \quad \ldots, \quad Q_{m+n})}{J(B_1,\ldots,B_m,A_1,\ldots,A_n)}, \quad \textit{(macierz Jacobiego wielomianów } Q_1, \ldots, Q_{m+n}\textit{)}, \\
(2.2) \qquad R(\vec{A},\vec{B}) &= (-1)^{mn} \det \tfrac{J(Q_1, \quad \ldots, \quad Q_{m+n})}{J(A_1,\ldots,A_n,B_1,\ldots,B_m)}.
\end{aligned}
$$

Dowód. Różniczkując tożsamość (1) względem zmiennych $B_1, \ldots, B_m$, $A_1, \ldots, A_n$ otrzymujemy

$$
(2) \qquad \begin{cases}
X^{m-1} F(\vec{A}, X) = \frac{\partial Q_1}{\partial B_1} X^{m+n-1} + \frac{\partial Q_2}{\partial B_1} X^{m+n-2} + \cdots + \frac{\partial Q_{m+n}}{\partial B_1} \\
\vdots \\
F(\vec{A}, X) \quad = \frac{\partial Q_1}{\partial B_m} X^{m+n-1} + \frac{\partial Q_2}{\partial B_m} X^{m+n-2} + \cdots + \frac{\partial Q_{m+n}}{\partial B_m} \\
X^{n-1} G(\vec{B}, X) = \frac{\partial Q_1}{\partial A_1} X^{m+n-1} + \frac{\partial Q_2}{\partial A_1} X^{m+n-2} + \cdots + \frac{\partial Q_{m+n}}{\partial A_1} \\
\vdots \\
G(\vec{B}, X) \quad = \frac{\partial Q_1}{\partial A_n} X^{m+n-1} + \frac{\partial Q_2}{\partial A_n} X^{m+n-2} + \cdots + \frac{\partial Q_{m+n}}{\partial A_n}
\end{cases}
$$

Własność (2.1) wynika bezpośrednio z formuł (2) i definicji macierzy Sylvestera. Własność (2.2) otrzymujemy z własności (2.1). □

3 Lemat Hensela

Niech $\underline{k}[[\vec{X}]]$ będzie pierścieniem szeregów formalnych p zmiennych $\vec{X} = (X_1, \ldots, X_p)$ o współczynnikach w ciele $\underline{k}$. Rozważmy ciąg $\vec{P} = (P_1, \ldots, P_q) \in (\underline{k}[[\vec{X}]][Y])^q$ wielomianów zmiennych $\vec{Y} = (Y_1, \ldots, Y_q)$ i niech $\vec{c} = (c_1, \ldots, c_q) \in \underline{k}^q$. Mamy następujące

Twierdzenie o funkcjach uwikłanych
Załóżmy, że $\vec{P}(0, \vec{c}) = 0$ *oraz* $\det \frac{J(P_1, \ldots, P_q)}{J(Y_1, \ldots, Y_q)}(0, \vec{c}) \neq 0$. *Wtedy istnieje jedyny ciąg szeregów potęgowych* $\vec{C}(\vec{X}) = (C_1(\vec{X}), \ldots, C_q(\vec{X}))$ *taki, że* $\vec{C}(\vec{0}) = \vec{c}$ *oraz* $\vec{P}(\vec{X}, \vec{C}(\vec{X})) = 0$.

Twierdzenie powyższe jest natychmiastowym wnioskiem z twierdzenia o szeregach uwikłanych (por. [5], Twierdzenie 7.1, gdzie autorzy rozważają szeregi o współczynnikach rzeczywistych. Podany tam dowód przenosi się bez zmian na przypadek dowolnego ciała).

Stosując formułę Nasha (2.2) i podane wyżej twierdzenie udowodnimy słynny

Lemat Hensela *Niech* $F(\vec{X}, Y) = c_0(\vec{X}) Y^N + c_1(\vec{X}) Y^{N-1} + \cdots + c_N(\vec{X}) \in \underline{k}[[\vec{X}]][Y]$ *będzie wielomianem stopnia* $N > 1$. *Zakładamy, że istnieją ciągi* $(a_1, \ldots, a_n) \in \underline{k}^n$ *i* $(b_1, \ldots, b_m) \in \underline{k}^m$ $n, m > 0$, $m + n = N$ *takie, że*

(α) $F(\vec{0}, Y) = \big(c_0(0) Y^n + a_1 Y^{n-1} + \cdots + a_n\big)\big(Y^m + b_1 Y^{m-1} + \cdots + b_m\big)$ *jest rozkładem wielomianu* $F(\vec{0}, Y)$ *na czynniki względnie pierwsze.*

Wówczas istnieje jedyny rozkład postaci

(β) $F(\vec{X}, Y) = \Big(c_0(\vec{X}) Y^n + a_1(\vec{X}) Y^{n-1} + \cdots + a_n(\vec{X})\Big) \cdot$
$\cdot \Big(Y^m + b_1(\vec{X}) Y^{m-1} + \cdots + b_m(\vec{X})\Big)$ *w* $\underline{k}[[\vec{X}]][Y]$
taki, że $a_i(0) = a_i$ *dla* $i = 1, \ldots, n$ *oraz* $b_j(0) = b_j$ *dla* $j = 1, \ldots, m$

Dowód. Nawiązując do oznaczeń wprowadzonych w §1 tego artykułu oznaczmy $\vec{A}' = (A_1, \ldots, A_n)$, $\vec{B}' = (B_1, \ldots, B_m)$ oraz $\vec{a}' = (a_1, \ldots, a_n)$ i $\vec{b}' = (b_1, \ldots, b_m)$.

Rozważmy wielomiany

$$q_i(\vec{X}, \vec{A}', \vec{B}') = Q_i(c_0(\vec{X}), \vec{A}', 1, \vec{B}') \in \underline{k}[[\vec{X}]][\vec{A}', \vec{B}'] \tag{3}$$

dla $i = 1, 2, \ldots, m+n$.

Z (1) otrzymujemy

$$\begin{aligned} &\Big(c_0(\vec{X})Y^n + A_1Y^{n-1} + \cdots + A_n\Big) \left(Y^m + B_1Y^{m-1} + \cdots + B_m\right) = \\ &= c_0(\vec{X})Y^{m+n} + q_1(\vec{X}, \vec{A}', \vec{B}')Y^{m+n-1} + \cdots + q_{m+n}(\vec{X}, \vec{A}', \vec{B}') \end{aligned} \tag{4}$$

a z własności Nasha (2.2)

$$\det \frac{J(q_1, \quad \ldots, \quad q_{m+n})}{J(A_1, \ldots, A_n, B_1, \ldots, B_m)}(\vec{X}, \vec{A}', \vec{B}') = (-1)^{mn} R(c_0(\vec{X}), \vec{A}', 1, \vec{B}'). \tag{5}$$

Podstawienie elementów $\vec{0} \in \underline{k}^p$, $\vec{a}' \in \underline{k}^n$ i $\vec{b}' \in \underline{k}^m$ na miejsce zmiennych $\vec{X}$, $\vec{A}'$, $\vec{B}'$ w formule (4) i założenie (α) implikują

$$q_i(\vec{0}, \vec{a}', \vec{b}') = c_i(\vec{0}) \qquad \text{dla} \quad i = 1, \ldots, m+n. \tag{6}$$

To samo podstawienie i formuła (5) pokazuje, że

$$\det \frac{J(q_1, \quad \ldots, \quad q_{m+n})}{J(A_1, \ldots, A_n, B_1, \ldots, B_m)}(\vec{0}, \vec{a}', \vec{b}') = (-1)^{mn} R(c_0(\vec{0}), \vec{a}', 1, \vec{b}'). \tag{7}$$

Oznaczmy teraz $p_i(\vec{X}, \vec{A}', \vec{B}') = q_i(\vec{X}, \vec{A}', \vec{B}') - c_i(\vec{X})$ dla $i = 1, \ldots, m+n$. Jest więc na mocy (6) i (7):

$$\begin{gathered} p_i(\vec{0}, \vec{a}', \vec{b}') = 0 \qquad \text{dla} \quad i = 1, \ldots, m+n \\ \text{oraz } \det \frac{J(p_1, \quad \ldots, \quad p_{m+n})}{J(A_1, \ldots, A_n, B_1, \ldots, B_m)}(\vec{0}, \vec{a}', \vec{b}') \neq 0 \end{gathered} \tag{8}$$

gdyż $R(c_0(\vec{0}), \vec{a}', \vec{b}')$ jako rugownik względnie pierwszych wielomianów $c_0(\vec{0})Y^n + a_1Y^{n-1} + \cdots + a_n$ i $Y^m + b_1Y^{m-1} + \cdots + b_m$ jest $\neq 0$.

Stosując twierdzenie o funkcjach uwikłanych do ciągu $\vec{p} = (p_1, \ldots, p_{m+n})$ i punktu $(\vec{0}, \vec{a}', \vec{b}')$ stwierdzamy, że istnieje jedyny ciąg $(a_1(\vec{X}), \ldots, a_n(\vec{X}), b_1(\vec{X}), \ldots, b_m(\vec{X})) \in \underline{k}[[\vec{X}]]^{m+n}$ taki, że $(a_1(\vec{0}), \ldots, a_n(\vec{0}), b_1(\vec{0}), \ldots, b_m(\vec{0})) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$ oraz $\vec{p}(\vec{X}, a_1(\vec{X}), \ldots, a_n(\vec{X}), b_1(\vec{X}), \ldots, b_m(\vec{X})) = \vec{0}$ w $\underline{k}[[\vec{X}]]^{m+n}$. Warunki te są równoważne warunkom (β) co dowodzi lematu Hensela. $\square$

Uwagi

1) W podanym przez nas dowodzie lematu Hensela pierścień szeregów formalnych $\underline{k}[[\vec{X}]]$ można zastąpić przez dowolny pierścień lokalny $\mathbb{A}$, w którym prawdziwe jest twierdzenie o funkcjach uwikłanych w cytowanej przez nas formie. W szczególności lemat Hensela prawdziwy jest dla pierścienia $\underline{k}\{\vec{X}\}$ zbieżnych szeregów o współczynnikach w ciele z waluacją zupełną $\underline{k}$.

2) Wyprowadzenie lematu Hensela z użyciem formuły Nasha dla rugownika pojawia się w pracach [6, 9]. Najbardziej popularny dowód lematu Hensela w geometrii analitycznej opiera się na twierdzeniu przygotowawczym Weierstrassa (por. [1] i [5]). Dowód ten jest krótki w przypadku gdy ciało $\underline{k}$ jest algebraicznie domknięte, przypadek dowolnego ciała $\underline{k}$ wymaga dodatkowych rozważań.

3) M. Nagata wprowadził na początku lat 50-tych minionego wieku pojęcie pierścienia Hensela jako pierścienia lokalnego, w którym prawdziwy jest lemat Hensela. Pojęcie to studiowane było przez wielu autorów i dzisiaj umieszczane jest w kursach algebry przemiennej. Dobre wprowadzenie do przedmiotu Czytelnik znajdzie w monografii [6].

4) Często lemat Hensela jest formułowany w słabszej formie: dla wielomianów unormowanych. Jednak przedstawiona w tym artykule mocniejsza postać pozwala na porównanie lematu Hensela z twierdzeniem przygotowawczym Weierstrassa (por. wniosek z lematu Hensela podany niżej).

Przypomnijmy, że wielomianem wyróżnionym stopnia $m > 0$ nazywamy wielomian postaci $Y^m + b_1(\vec{X})Y^{m-1} + \cdots + b_m(\vec{X}) \in \underline{k}[[\vec{X}]]$ taki, że $b_1(\vec{0}) = \ldots = b_m(\vec{0}) = 0$.

Wniosek (Twierdzenie przygotowawcze dla wielomianów)
Niech $F(\vec{X}, Y) = c_0(\vec{X})Y^N + c_1(\vec{X})Y^{N-1} + \cdots + c_N(\vec{X}) \in \underline{k}[[\vec{X}]][Y]$ *będzie wielomianem stopnia* N *takim, że rząd* $m = \operatorname{ord} F(\vec{0}, Y)$ *jest dodatni i skończony. Wtedy* $F(\vec{X}, Y) = U(\vec{X}, Y)W(\vec{X}, Y)$ *w* $\underline{k}[[\vec{X}]][Y]$ *gdzie* $U(\vec{0}, 0) \neq 0$ *zaś* $W(\vec{X}, Y)$ *jest wielomianem wyróżnionym (koniecznie stopnia* m*). Para* U, W *jest jedyna.*

Dowód. Gdy $m = N$ wniosek jest trywialny, załóżmy więc, że $m < N$. Mamy zatem $F(\vec{0}, Y) = c_0(\vec{0})Y^N + c_1(\vec{0})Y^{N-1} + \cdots + c_{N-m}(\vec{0})Y^m = (c_0(\vec{0})Y^{N-m} + c_1(\vec{0})Y^{N-m-1} + \cdots + c_{N-m}(\vec{0}))Y^m$ i istnienie rozkładu wynika z lematu Hensela bo $c_{N-m}(\vec{0}) \neq 0$ na mocy definicji liczby m.

Aby sprawdzić jednoznaczność załóżmy, że $F = UW$ w $\underline{k}[[\vec{X}]][Y]$ gdzie $U(\vec{0}, 0) \neq 0$ oraz W jest wielomianem wyróżnionym. Jest zatem $U(\vec{0}, Y) = c_0(\vec{0})Y^{N-m} + c_1(\vec{0})Y^{N-m-1} + \cdots + c_{N-m}(\vec{0})$ i $W(\vec{0}, Y) = Y^m$ a więc jedyność pary U, W wynika z jednoznaczności w lemacie Hensela. □

Oczywiście powyższy wniosek prawdziwy jest także dla szeregów zbieżnych i ogólnie dla wielomianów zmiennej Y o współczynnikach w pierścieniu lokalnym, w którym prawdziwe jest twierdzenie o funkcjach uwikłanych.

Literatura

[1] **S. S. Abhyankar**, *Local Analytic Geometry,* Academic Press 1964,

[2] ———, *Lectures on Algebra,* vol I, World Scientific 2006,

[3] **F. Apèry, J. P. Jouanolou**, *Élimination. Le cas d'une variable,* Hermann 2007,

[4] **I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky**, *Newton Polytopes of the Classical Resultant and Discriminant,* Advances in Math. 84 (1990), 237-254,

[5] **St. Łojasiewicz, J. Stasica**, *Analiza formalna i funkcje analityczne,* Wydawnictwo Uniwersytetu Jagiellońskiego 2005,

[6] **J. S. Milne**, *Étale Cohomology,* Princeton 1980,

[7] **A. Mostowski i M. Stark**, *Elementy algebry wyższej,* Warszawa 1965,

[8] **J. Nash**, *Real Algebraic Manifolds,* Annals of Math. vol. 56, No. 3, November 1952,

[9] **A. Płoski**, *Remarque sur le lemme de Hensel,* Bull. Acad. Polon. Sci. Sér. Sci. Math. 28 (1980), n^o 3-4, 115-116,

[10] ———, *Teoria eliminacji i niezmienniki algebraiczne,* I Konferencja Zastosowań Niezmienników Algebraicznych, Warszawa, 26-27 listopada 1994, str. 21-30,

[11] ———, *Efektywne Twierdzenie o Zerach,* Materiały XVIII Konferencji Szkoleniowej z Geometrii Analitycznej i Algebraicznej, Łódź 1997, str. 45-51,

[12] ———, *Wstęp do lokalnej teorii krzywych algebraicznych,* Materiały na XXVIII Konferencję Szkoleniową z Geometrii Analitycznej i Algebraicznej Zespolonej, Łódź 2007, str. 21-40.

SYLVESTER RESULTANT AND JACOBIAN

Summary. For any integers $n > 0$ and $m > 0$ we take interminates $\vec{A} = (A_0, \ldots, A_n)$, $\vec{B} = (B_0, \ldots, B_m)$ and X and let $R(\vec{A}, \vec{B})$ be the Sylvester resultant of the polynomials $F(X) = A_0X^n + A_1X^{n-1} + \cdots + A_n$ and $G(X) = B_0X^m + B_1X^{m-1} + \cdots + B_m$.

Let $F(X)G(X) = Q_0(\vec{A}, \vec{B})X^{m+n} + Q_1(\vec{A}, \vec{B})X^{m+n-1} + \cdots + Q_{m+n}(\vec{A}, \vec{B})$ in $\mathbb{Z}[\vec{A}, \vec{B}][X]$. In this article we recall that $R(\vec{A}, \vec{B}) = (-1)^{mn} \det \frac{J(Q_1, \quad \ldots, \quad Q_{m+n})}{J(A_1, \ldots, A_n, B_1, \ldots, B_m)}$ (see J. Nash, Annals of Math. vol 56, No. 3, November 1952, page 412). Then using the above formula and the Implicit Function Theorem we prove Hensel's lemma for polynomials with coefficients in the formal (convergent) power series rings.