**MATERIAŁY XVI KONFERENCJI SZKOLENIOWEJ
Z ANALIZY I GEOMETRII ZESPOLONEJ**

1995 **Łódź** **str. 49**

DOWÓD TWIERDZENIA ABHYANKARA I MOHA WEDŁUG RICHMANA

A. Nowicki (Toruń)

W niniejszym artykule zajmujemy się dowodem następującego twierdzenia.

Twierdzenie 0.1. *Niech $k[t]$ będzie pierścieniem wielomianów zmiennej t nad ciałem k charakterystyki zero i niech $f, g \in k[t] \setminus k$. Jeżeli $k[f, g] = k[t]$, to* $\deg f \mid \deg g$ *lub* $\deg g \mid \deg f$.

Twierdzenie to pojawiło się w latach pięćdziesiątych, z błędnym dowodem, w pracy Segrego [13] poświęconej hipotezie jakobianowej i po raz pierwszy zostało udowodnione w 1975 roku przez Abhyankara i Moha [3] (patrz też [1]). Historia tego twierdzenia i jego zastosowania są opisane w pracach [3] i [4]. W latach 1977 – 1982 pojawiły się inne dowody. Podali je Miyanishi [7] (patrz też [8]), Ganong [5] i Rudolph [12].

Abhyankar i Moh udowodnili to twierdzenie przy pomocy rowiniętej przez nich teorii pierwiastków aproksymatywnych wielomianów. Czytelnikowi zainteresowanemu wprowadzeniem w problematykę teorii pierwiastków aproksymatywnych polecamy piękne artykuły Arkadiusza Płoskiego [9] i [10], w których znajdziemy, między innymi, dowód omawianego twierdzenia oraz dodatkowe o nim informacje.

W 1986 roku Richman [11] podał nowy interesujący dowód, nie odwołujący się do pierwiastków aproksymatywnych. W dowodzie tym istnieje jednak pewna luka. Konstruując, istotny w całym dowodzie, ciąg $(H_1, \ldots, H_{N-1})$ spełniający równość (13) (patrz dowód Proposition 7 w [11]), Richman wykorzystuje kilkakrotnie udowodnione wcześniej Proposition 6 i twierdzi, że w ten sposób otrzyma się równość postaci $y_1 = 0$. Nie ma gwarancji, że taką równość otrzymamy. Przy pomocy Proposition 6 otrzymujemy tylko ciąg pewnych funkcji wymiernych $y_1, y_1', y_1'', \ldots$ o coraz to mniejszych stopniach. Z faktu, że stopnie są coraz mniejsze nie wynika, że któraś z tych funkcji jest równa 0. Stopnie mogą być liczbami ujemnymi.

Autor niniejszego artykułu znalazł tę usterkę, poinformował o niej Richmana i w liście do Richmana z 1987 roku udowodnił pewien dodatkowy fakt (patrz Stwierdzenie 9.4 w tym artykule) pozwalający uratować omawiany dowód. Richman (w liście z 1987 roku) przyznaje autorowi rację. Sprawa ta nie została jednak nigdzie opublikowana. Później, w 1991 roku, wspomnianą usterkę zauważył również i naprawił Kang [6].

Celem tego artykułu jest przedstawienie pełnego dowodu Twierdzenia 0.1 według idei Richmana.

Założyliśmy w Twierdzeniu 0.1, że k jest ciałem charakterystyki zero. Przy pewnym dodatkowym założeniu, mianowicie "$\mathrm{char}(k) \nmid \mathrm{NWD}(\deg f, \deg g)$", twierdzenie to zachodzi także dla ciał o dodatnich charakterystykach (patrz np. [3]). W takiej wersji dowodzi to Richman w [11]. Tym przypadkiem nie będziemy się tu jednak zajmować.

Zaznaczmy jeszcze, że Twierdzenie 0.1 można łatwo udowodnić, gdy stopień jednego z wielomianów f i g jest liczbą pierwszą (patrz Wniosek 1.7).

1 Wiadomości wstępne

Przez cały czas w tym artykule zakładamy, że k jest ciałem charakterystyki zero, $k[t]$ jest pierścieniem wielomianów jednej zmiennej t nad k oraz $k(t)$ jest ciałem funkcji wymiernych zmiennej t nad k. Jeżeli $K \subseteq L$ jest skończonym rozszerzeniem ciał, to stopień tego rozszerzenia oznaczmy przez $(L : K)$. Rozpocznijmy od następującego stwierdzenia.

Stwierdzenie 1.1. *Jeżeli R jest pierścieniem przemiennym takim, że $k \subsetneq R \subseteq k[t]$, to pierścień $k[t]$ jest całkowity nad R.*

Dowód. Niech $f = a_n t^n + \cdots + a_1 t + a_0$, gdzie $a_n \ldots, a_0 \in k, a_n \neq 0$, będzie wielomianem należącym do $R \setminus k$. Mamy wtedy równość

$$t^n + a_n^{-1} a_{n-1} t^{n-1} + \cdots + a_n^{-1}(a_0 - f) = 0,$$

z której wynika, że zmienna t jest elementem całkowitym nad R (nawet nad $k[f]$). $\boxtimes$

W podobny prosty sposób można wykazać następne stwierdzenie.

Stwierdzenie 1.2. *Jeżeli $g \in k[t] \setminus k$, to $k(t)$ jest skończonym rozszerzeniem ciała $k(g)$ oraz $(k(t) : k(g)) = \deg g$.* $\boxtimes$

Załóżmy teraz, że f i g są wielomianami należącymi do $k[t] \setminus k$. Mamy wówczas pierścienie $k \subsetneq k[g] \subseteq k[f,g] \subseteq k[t]$ oraz ciała $k \subsetneq k(g) \subseteq k(f,g) \subseteq k(t)$. Ze Stwierdzenia 1.1 wynika, że pierścień $k[f,g]$ jest całkowity nad $k[g]$. W szczególności wielomian f jest całkowitym elementem nad $k[g]$. Istnieje zatem moniczny wielomian $W \in k[g][X]$ taki, że $W(f) = 0$.

Stwierdzenie 1.3. *Niech $f, g \in k[t] \setminus k$ i niech $W \in k[g][X]$ będzie monicznym wielomianem minimalnego stopnia takim, że $W(f) = 0$. Wtedy* $\deg W = (k(f,g) : k(g))$.

Dowód. Niech $N = (k(f,g) : k(g)) = (k(g)(f) : k(g))$ i niech $B \in k(g)[X]$ będzie wielomianem minimalnym dla f nad $k(g)$. Ponieważ $W(f) = 0$ i $W \in k[g][X] \subset k(g)[X]$ więc $W = AB$, gdzie A jest pewnym wielomianem należącym do $k(g)[X]$. Istnieją wówczas elementy $a, b \in k[g]$ takie, że $aA, bB \in k[g][X]$. W pierścieniu $k[g][X]$ zachodzi więc równość: $abW = aA \cdot bB$.

Pierścień $k[g]$ jest dziedziną z jednoznacznością rozkładu (ponieważ $k[g]$ jest pierścieniem izomorficznym z $k[t]$). Istnieją zatem elementy $a_1, b_1 \in k[g]$ oraz prymitywne wielomiany $A_1, B_1 \in k[g][X]$ takie, że $aA = a_1A_1$ i $bB = b_1B_1$. Mamy zatem równość: $abW = a_1b_1(A_1B_1)$. Wielomian W jest prymitywny (bo jest moniczny) i wielomian A_1B_1 też jest prymitywny (na mocy Lematu Gaussa). Stąd wynika, że $W = c(A_1B_1)$, gdzie c jest pewnym odwracalnym elementem pierścienia $k[g]$. Istnieje więc odwracalny element $d \in k[g]$ taki, że dB_1 jest monicznym wielomianem należącym do $k[g][X]$. Niech $H = dB_1$. Wtedy $H \in k[g][X]$ jest moniczny, $H(f) = 0$ i $\deg H = \deg B = N$. Z minimalności wielomianu W wynika więc, że $\deg W = N = (k(f,g) : k(g))$. $\boxtimes$

Wniosek 1.4. *Niech $f, g \in k[t] \setminus k$. Wtedy*

$$k[f,g] = k[g]f^{N-1} + k[g]f^{N-2} + \cdots + k[g]f + k[g],$$

gdzie $N = (k(f,g) : k(g))$.

Dowód. Niech $E = k[g]f^{N-1} + \cdots + k[g]f + k[g]$. Ze Stwierdzenia 1.3 wynika, że $f^N \in E$ i stąd otrzymujemy (stosując prostą indukcję), że $f^n \in E$ dla wszystkich $n \geqslant N$. $\boxtimes$

Wniosek 1.5. *Niech $f, g \in k[t]$. Jeżeli $k(f,g) = k(g)$, to $k[f,g] = k[g]$.*

Dowód. Wynika to z Wniosku 1.4 dla $N = 1$. $\boxtimes$

Wniosek 1.6. *Jeżeli $g \in k[t]$, to $k(g) \cap k[t] = k[g]$.*

Dowód. Niech $f \in k(g) \cap k[t]$. Wtedy $k(f,g) = k(g)$ a zatem, $k[f,g] = k[g]$ (Wniosek 1.5), czyli $f \in k[g]$. $\boxtimes$

Następny wniosek jest szczególnym przypadkiem Twierdzenia 0.1.

Wniosek 1.7. *Niech $f, g \in k[t] \setminus k$. Załóżmy, że stopień jednego z wielomianów f i g jest liczbą pierwszą. Jeżeli $k[f,g] = k[t]$, to* $\deg f \mid \deg g$ *lub* $\deg g \mid \deg f$.

Dowód. Niech $\deg g = p$, gdzie p jest liczbą pierwszą. Wtedy (na mocy założenia oraz Stwierdzenia 1.2)

$$\begin{aligned}(k(f,g) : k(g)) &= 1 \cdot (k(f,g) : k(g)) = (k(t) : k(f,g))(k(f,g) : k(g)) \\ &= (k(t) : k(g)) = \deg g = p,\end{aligned}$$

a zatem z Wniosku 1.4 wynika, że $k[f,g] = k[g]f^{p-1} + \cdots + k[g]f + k[g]$.

Wiemy, że $t \in k[f,g]$. Istnieją więc niezerowe elementy $a_1, \ldots, a_s \in k[g]$ takie, że

$$t = a_1 f^{i_1} + \cdots + a_s f^{i_s},$$

gdzie $s \geqslant 1$ oraz $p > i_1 > \cdots i_s \geqslant 0$.

Przypuśćmy, że $\deg g \nmid \deg f$. Wtedy stopnie wielomianów $a_1 f^{i_1}, \ldots, a_s f^{i_s}$ są parami nieprzystające modulo p (ponieważ stopnie wielomianów $a_1, \ldots, a_s$ są podzielne przez p i $p \nmid \deg f$), a zatem istnieje $r \in \{1, \ldots, s\}$ takie, że $i_r > 0$ i $1 = \deg t = \deg(a_r f^{i_r})$. Stąd wynika, że $\deg f = 1$, czyli $\deg f \mid \deg g$. $\boxtimes$

2 Ustalenie oznaczeń i definicje

W dalszym ciągu niniejszego artykułu zakładamy, że f i g są wielomianami należącymi do $k[t] \setminus k$. Przez N oznaczamy liczbę $(k(f,g) : k(g))$. Jeżeli $N = 1$, to (patrz Wniosek 1.5) $f \in k[g]$ i wtedy $\deg g \mid \deg f$. Zakładać więc będziemy, że $N > 1$. Z równości

$$\deg g = (k(t) : k(g)) = (k(t) : k(f,g))(k(f,g) : k(g))$$

wynika, że $N \leqslant \deg g$.

Jeżeli n jest dodatnią liczbą całkowitą, to oznaczmy:

$$\begin{aligned}A_n &= f^n + k[g]f^{n-1} + \cdots + k[g]f + k[g], \\ \overline{A}_n &= f^n + k(g)f^{n-1} + \cdots + k(g)f + k(g), \\ L_n &= k[g]f^n + k[g]f^{n-1} + \cdots + k[g]f + k[g], \\ \overline{L}_n &= k(g)f^n + k(g)f^{n-1} + \cdots + k(g)f + k(g).\end{aligned}$$

Dodatkowo przyjmujemy, że $L_0 = k[g]$ oraz $\overline{L}_0 = k(g)$. Wtedy $A_n = f^n + L_{n-1}$, $\overline{A}_n = f^n + \overline{L}_{n-1}$. Ponadto $A_n = k[f,g]$ i $\overline{A}_n = k(f,g)$ dla wszytkich $n \geqslant N$ oraz $L_n = k[f,g]$ i $\overline{L}_n = k(f,g)$ dla $n \geqslant N-1$ (patrz Wniosek 1.4).

Stwierdzenie 2.1. *Jeżeli n jest liczbą naturalną, to $\overline{A}_n \cap k[f,g] = A_n$ i $\overline{L}_n \cap k[f,g] = L_n$.*

Dowód. Pokażemy, że $\overline{A}_n \cap k[f,g] = A_n$. Jeżeli $n \geqslant N$, to równość ta jest oczywista, gdyż wtedy $\overline{A}_n = k(f,g)$. Załóżmy, że $n < N$ i niech $u \in \overline{A}_n \cap k[f,g]$. Wtedy $u = f^n + a_{n-1}f^{n-1} + \cdots + a_1 f + a_0$, dla pewnych $a_{n-1}, \ldots, a_0 \in k(g)$. Z drugiej strony $u = b_{N-1}f^{N-1} + \cdots + b_1 f + b_0$, gdzie $b_{N-1}, \ldots, b_0 \in k[g]$, ponieważ $u \in k[f,g] = k[g]f^{N-1} + \cdots + k[g]f + k[g]$. Wielomiany $f^{N-1}, \ldots, f^1, f^0$ tworzą bazę przestrzeni $k(g)(f)$ nad $k(g)$. Przedstawienie elementu u jest więc jednoznaczne. To implikuje, że elementy $a_{n-1}, \ldots, a_0$ należą do $k[g]$, czyli $u \in A_n$. Mamy zatem inkluzję $\overline{A}_n \cap k[f,g] \subseteq A_n$. Inkluzja w przeciwnym kierunku jest oczywista. Podobnie wykazujemy, że $\overline{L}_n \cap k[f,g] = L_n$. $\boxtimes$

Definicja 2.2. *α-Systemem nazywamy każdy ciąg $(h_1, \ldots, h_{N-1})$ elementów z ciała $k(f,g)$ taki, że:*
(*a*) $h_n \in \overline{A}_n$ *dla wszystkich* $n = 1, \ldots, N-1$,
(*b*) *liczby* $0, \deg h_1, \ldots, \deg h_{N-1}$ *są parami nieprzystające modulo* $\deg g$.

Definicja 2.3. *β-Systemem nazywamy każdy ciąg $(h_1, \ldots, h_{N-1})$ elementów pierścienia*
$k[f,g]$ taki, że:
(*a*) $h_n \in A_n$ *dla wszystkich* $n = 1, \ldots, N-1$,
(*b*) *liczby* $0, \deg h_1, \ldots, \deg h_{N-1}$ *są parami nieprzystające modulo* $\deg g$.

3 Własności α i β-systemów

Ze Stwierdzenia 2.1 wynika, że każdy α-system $(h_1, \ldots, h_{N-1})$ taki, że $h_1, \ldots, h_{N-1} \in k[f,g]$, jest β-systemem. Bez trudu wykazujemy następujące dwa stwierdzenia.

Stwierdzenie 3.1. *Niech $(h_1, \ldots, h_{N-1})$ będzie α-systemem i niech $n \in \{1, \ldots, N-1\}$. Wtedy*
(1) $\overline{A}_n = h_n + \overline{L}_{n-1}$,
(2) $\overline{L}_n = k(g)h_n + \cdots + k(g)h_1 + k(g)$. $\boxtimes$

Stwierdzenie 3.2. *Niech $(h_1, \ldots, h_{N-1})$ będzie β-systemem. Wtedy $L_n = k[g]h_n + \cdots + k[g]h_1 + k[g]$ dla wszystkich $n \in \{1, \ldots, N-1\}$.* $\boxtimes$

Udowodnimy teraz następne stwierdzenie.

Stwierdzenie 3.3. *Niech $(h_1, \ldots, h_{N-1})$ będzie β-systemem. Niech $h_0 = 1$, $n < N$ i niech $w \in L_n$. Istnieją wtedy jednoznacznie wyznaczone liczby całkowite s i r takie, że $\deg w = \deg g^s h_r$, $s \geqslant 0$ i $r \in \{0, 1, \ldots, n\}$.*

Dowód. Wiemy z poprzedniego stwierdzenia, że $L_n = k[g]h_n + \cdots + k[g]h_1 + k[g]h_0$. Istnieją więc wielomiany $u_n, \ldots, u_0 \in k[g]$ takie, że $w = u_n h_n + \cdots + u_0 h_0$. Z definicji β-systemu wynika, że stopnie wielomianów $u_n h_n, \ldots, u_0 h_0$ są parami różne. Zatem $\deg w = \deg u_r h_r$, dla pewnego $r \in \{0, 1, \ldots, n\}$. Liczba $\deg u_r$ jest podzielna przez $\deg g$ (ponieważ $u_r \in k[g]$). Istnieje więc nieujemna liczba całkowita s spełniająca równość $\deg u_r = s \deg g$. Mamy zatem $\deg w = \deg u_r h_r = \deg g^s h_r$.

Przypuśćmy teraz, że dla pewnych liczb całkowitych r_1, s_1, r_2, s_2 takich, że $s_1, s_2 \geqslant 0$ i $r_1, r_2 \in \{0, \ldots, n\}$, zachodzi równość $\deg g^{s_1} h_{r_1} = \deg g^{s_2} h_{r_2}$. Wtedy $\deg h_{r_1} - \deg h_{r_2} = (s_1 - s_2) \deg g$, czyli $\deg h_{r_1} \equiv \deg h_{r_2} \pmod{\deg g}$. Stąd wynika, że $r_1 = r_2$ i stąd dalej otrzymujemy równość $s_1 = s_2$. ⊠

Istotną rolę w dowodzie Twierdzenia 0.1 odgrywać będzie następujące twierdzenie.

Twierdzenie 3.4. *Istnieje co najmniej jeden β-system.*

Twierdzenie to udowodnimy w Rozdziale 10.

4 Dowód Twierdzenia 0.1

Dowód. Oznaczmy: $d_f = \deg f$, $d_g = \deg g$, $d = \mathrm{NWD}(d_f, d_g)$. Niech $d_f = ad$, $d_g = bd$, gdzie a i b są względnie pierwszymi liczbami naturalnymi. Istnieją liczby całkowite m i n takie, że $1 = ma + nb$ oraz $0 \leqslant m < b$. Mamy wtedy $d = md_f + nd_g$, a zatem

$$d \equiv \deg f^m \pmod{d_g}. \tag{4.1}$$

Przypomnijmy, że przez N oznaczmy liczbę $(k(f, g) : k(g))$. W naszym przypadku liczba ta jest oczywiście równa liczbie d_g (gdyż $d_g = (k(t) : k(g)) = (k(t) : k(f, g))N = 1 \cdot N = N$).

Niech $(h_0 = 1, h_1, \ldots, h_{N-1})$ będzie β-systemem. Ponieważ wielomian t^d należy do $k[f, g] = L_{N-1}$ (patrz Wniosek 1.4) więc, na mocy Stwierdzenia 3.3, istnieją liczby całkowite r i s takie że

$$d = \deg t^d = \deg g^s h_r, \ \ s \geqslant 0 \ \text{ i } \ r \in \{0, 1, \ldots, N-1\}. \tag{4.2}$$

Wielomian f^m należy do L_m. Stosując jeszcze raz Stwierdzenie 3.3 (tym razem dla wielomianu f^m) stwierdzamy, że $\deg f^m = \deg g^{s_1} h_{r_1}$, gdzie $0 \leqslant r_1 \leqslant m$ i $s_1 \geqslant 0$.

Z (4.1) i (4.2) wynika, że $\deg h_{r_1} \equiv \deg h_r \pmod{d_g}$, czyli $r_1 = r$. Mamy zatem nierówność $r < b$, z której wynika, że $h_r \in L_{b-1} = k[g]f^{b-1} + \cdots + k[g]f^0$.

Zauważmy teraz, że wielomiany $f^0, f^1, \ldots, f^{b-1}$ mają parami nieprzystające stopnie modulo d_g. Istotnie, przypuśćmy, że $\deg f^i \equiv \deg f^j \pmod{d_g}$ dla pewnych $i, j \in \{0, 1, \ldots, b-1\}$. Wtedy $(i - j)d_f = ud_g$, gdzie $u \in \mathbb{Z}$. Stąd

mamy równość $(i-j)a = ub$, z której wynika, że $b \mid i-j$ (gdyż liczby a i b są względnie pierwsze). To implikuje, że $i = j$.

Powtarzając dowód Stwierdzenia 3.3 widzimy, że $\deg h_r = \deg g^p f^i$, gdzie p, i są pewnymi nieujemnymi liczbami całkowitymi. Mamy zatem

$$d = \deg g^s h_r = sd_g + \deg h_r = sd_g + \deg g^p f^i = (s+p)d_g + id_f,$$

gdzie $s + p \geqslant 0$, $i \geqslant 0$ oraz $s + p + i > 0$. Stąd mamy dalej

$$d = (s+p)d_g + id_f \geqslant \min(d_f, d_g) \geqslant \mathrm{NWD}(d_f, d_g) = d,$$

czyli $\mathrm{NWD}(d_f, d_g) = \min(d_f, d_g)$, a zatem $d_f \mid d_g$ lub $d_g \mid d_f$. ⊠

W powyższym dowodzie założenie "$k[t] = k[f, g]$" potrzebne było tylko po to by stwierdzić, że istnieje niezerowy wielomian w należący do $k[f, g]$ i posiadający stopień d, gdzie $d = \mathrm{NWD}(\deg f, \deg g)$. Rolę wielomianu w odgrywał tu wielomian t^d. Udowodniliśmy zatem

Twierdzenie 4.1 ([11]). *Niech $f, g \in k[t] \setminus k$ i niech $d = \mathrm{NWD}(\deg f, \deg g)$. Jeżeli pierścień $k[f, g]$ zawiera niezerowy wielomian stopnia d, to* $\deg f \mid \deg g$ *lub* $\deg g \mid \deg f$. ⊠

W dowodzie wykorzystaliśmy Twierdzenie 3.4 mówiące o tym, że istnieje co najmniej jeden β-system. Faktu tego jeszcze jednak nie udowodniliśmy. Cała pozostała część artykułu zmierza do przedstawienia dowodu tego faktu.

5 Istnienie α-systemu

W tym rozdziale udowodnimy, że istnieje co najmniej jeden α-system.

Niech S będzie podzbiorem zbioru $k[t] \setminus \{0\}$. Załóżmy że każde dwa różne wielomiany należące do S mają różne stopnie i oznaczmy przez $\deg S$ zbiór $\{\deg s;\ s \in S\}$. Przypomnijmy, że stopień wielomianu zerowego jest równy $-\infty$.

Jeżeli $h \in k[t]$, to przez $R(h, S)$ oznaczać będziemy wielomian należący do $k[t]$, który definiujemy w następujący indukcyjny sposób.

Definicja 5.1.

(1) $R(0, S) = 0$.

(2) *Niech $h \neq 0$, $\deg h = m \geqslant 0$ i załóżmy, że $R(h', S)$ jest już określone dla wszystkich wielomianów $h' \in k[t]$ takich, że $\deg h' < \deg h$. Wtedy:*

(a) *Jeżeli $\deg h \notin \deg S$, to przyjmujemy $R(h, S) = h$.*

(b) *Jeżeli $\deg h \in \deg S$, to istnieje (dokładnie jedno) $s \in S$ takie, że $\deg h = \deg s$ i istnieje ponadto (dokładnie jeden) niezerowy element $a \in k$ taki, że $\deg(h - as) < \deg h$. Przyjmujemy wówczas, że $R(h, S) = R(h - as, S)$.*

Przykład 5.2. Niech $S = \{x^2+1, 2x+1\}$. Wtedy $\deg S = \{2,1\}$ i mamy:
(1) $R(x^3, S) = x^3$, $R(x^5+3x, S) = x^5+3x$ (gdyż stopnie wielomianów x^3 i x^5+3x nie należą do zbioru $\deg S$),
(2) $R(x^2+x, S) = R((x^2+x)-(x^2+1), S) = R(x-1, S) = R((x-1) - 1/2(2x+1), S) = R(-3/2, S) = -3/2$. $\boxtimes$

Mamy zatem funkcję $R(\_, S) : k[t] \longrightarrow k[t]$. Łatwo sprawdzić następujące stwierdzenie.

Stwierdzenie 5.3. *Niech $h \in k[t]$. Wtedy:*
(1) $\deg R(h,S) \notin \deg S$*;*
(2) *jeżeli* $\deg h \notin \deg S$*, to* $R(h,S) = h$*;*
(3) $R(h,S) = 0 \iff h = a_1 s_1 + \cdots + a_p s_p$*, gdzie* $a_1, \ldots, a_p \in k$ *i* $s_1, \ldots, s_p \in S$. $\boxtimes$

Udowodnimy teraz

Stwierdzenie 5.4 ([11]). *Istnieją wielomiany $h_1, \ldots, h_{N-1} \in k[t]$ takie, że:*
(1) $h_n \in L_n \setminus L_{n-1}$*, dla* $n = 1, \ldots, N-1$*;*
(2) *liczby* $0, \deg h_1, \ldots, \deg h_{N-1}$ *są parami nieprzystające modulo* $\deg g$.

Dowód. Wielomiany $h_1, \ldots, h_{N-1}$ skonstruujemy indukcyjnie.
Niech $S = \{g^n; n = 0, 1, \ldots\}$. Przyjmijmy $h_1 = R(f, S)$. Wtedy $h_1 \in L_1 \setminus L_0$ i liczby 0 oraz $\deg h_1$ nie przystają do siebie modulo $\deg g$.
Załóżmy, że wielomiany $h_1, \ldots, h_n$ są już skonstruowane. Jeżeli $n+1 = N$, to konstrukcja jest już zakończona. Załóżmy więc, że $n+1 < N$ i niech $h_0 = 1$. Rozważmy zbiór

$$T = \{h_r g^i;\ r = 0, \ldots, n,\ i \geqslant 0\}.$$

Jest oczywiste, że $T \subset k[t] \setminus \{0\}$ oraz, że elementy zbioru T mają parami różne stopnie. Niech

$$y_0 = R(f^{n+1}, T).$$

Wtedy $y_0 \in f^{n+1} + L_n$ (w szczególności $y_0 \neq 0$) i elementy zbioru $T \cup \{y_0\}$ (patrz Stwierdzenie 5.3) mają parami różne stopnie. Możemy więc rozpatrzyć wielomian

$$y_1 = R(gf^{n+1}, T \cup \{y_0\}).$$

Wielomian ten należy do zbioru $(g+a_0)f^{n+1} + L_n$, dla pewnego $a_0 \in k$. W szczególności $y_1 \neq 0$. Ponadto elementy zbioru $T \cup \{y_0, y_1\}$ mają parami różne stopnie.
Kontynuując to postępowanie możemy skonstruować nieskończony ciąg y_0, $y_1, \ldots$, niezerowych wielomianów z $k[t]$ takich, że

$$y_i = R(g^i f^{n+1}, T \cup \{y_0, \ldots, y_{i-1}\})$$

dla $i = 0, 1, \ldots$.

Z łatwością sprawdzamy, że stopnie wielomianów zbioru $T \cup \{y_0, \ldots, y_i\}$ są parami różne. Stąd w szczególności wynika, że stopień każdego z wielomianów $y_0, y_1, \ldots$ nie jest podzielny przez $\deg g$. Z łatwością też sprawdzmy, że $y_i \in (g^i + a_{i-1}g^{i-1} + \cdots + a_0)f^{n+1} + L_n$, dla pewnych $a_0, \ldots, a_{i-1} \in k$. To implikuje, że wszystkie wielomiany $y_0, y_1, \ldots$ należą do zbioru $L_{n+1} \setminus L_n$.

Wykażemy teraz że wśród wielomianów y_0, $y_1, \ldots$ istnieje taki, którego stopień nie przystaje do żadnej z liczb $\deg h_0, \deg h_1, \ldots, \deg h_n$ modulo $\deg g$.

Przypuśćmy, że tak nie jest. Wówczas dla każdej nieujemnej liczby całkowitej j istnieje liczba $m_j \in \{0, \ldots, n\}$ taka, że

$$\deg y_j \equiv \deg h_{m_j} \pmod{\deg g}.$$

Ponieważ elementów zbioru $\{0, \ldots, n\}$ jest tylko skończona ilość, więc istnieje nieskończony podzbiór U, nieujemnych liczb całkowitych, oraz istnieje liczba $s \in \{0, \ldots, n\}$ taka, że $\deg y_u \equiv \deg h_s \pmod{\deg g}$ dla wszystkich $u \in U$. Wtedy

$$\deg y_u + p_u \deg g = \deg h_s, \quad \text{gdzie} \quad p_u \in \mathbb{Z}. \tag{5.1}$$

Zauważmy, że $p_u > 0$. Istotnie, przypuśćmy, że $p_u \leqslant 0$. Wtedy $\deg y_u = \deg(g^{-p_u} h_s)$, $g^{-p_u} h_s \in T$ i mamy sprzeczność ponieważ stopnie elementów zbioru $T \cup \{y_0, \ldots, y_u\}$ są parami różne. Każda więc liczba całkowita postaci p_u jest dodatnia. Zatem z (5.1) wynika, że $\deg y_u < \deg h_s$ dla każdego $u \in U$ wbrew temu, że zbiór U jest nieskończony i stopnie wielomianów $y_0, y_1, \ldots$ są parami różne.

Otrzymana sprzeczność dowodzi, że istnieje nieujemna liczba całkowita j taka, że liczby $\deg y_j, 0, \deg h_1, \ldots, \deg h_n$ są parami nieprzystające modulo $\deg g$. Definiujemy teraz wielomian h_{n+1} przyjmując $h_{n+1} = y_j$. $\boxtimes$

Niech $h_1, \ldots, h_{N-1}$ będą wielomianami takimi jak w powyższym stwierdzeniu. Z tego, że $h_n \in L_n \setminus L_{n-1}$ (dla $n = 1, \ldots, N-1$) wynika, że h_n ma przy f^n niezerowy współczynnik należący do $k[g]$. Dzieląc h_n przez ten niezerowy współczynnik otrzymujemy wymierną funkcję h'_n należącą do zbioru $\overline{A}_n$. Liczby $0, \deg h'_1, \ldots, \deg h'_{N-1}$ są oczywiście parami nieprzystające modulo $\deg g$. Wykazaliśmy zatem następujące stwierdzenie.

Stwierdzenie 5.5. *Istnieje co najmniej jeden α-system.* $\boxtimes$

6 Definicje ciągu c(1), ..., c(p)

Przypomnijmy (patrz Rozdział 2), że jeżeli $n = 0, 1, \ldots, N-1$, to przez $\overline{L}_n$ oznaczamy zbiór $k(g)f^n + \cdots + k(g)f^1 + k(g)f^0$. Wprowadźmy jeszcze dwa następne oznaczenia:

$$\begin{aligned} U_n &= \{\deg \varphi;\ \varphi \in \overline{L}_n\}, \\ G_n &= \text{ ideał w } \mathbb{Z} \text{ generowany przez zbiór } U_n. \end{aligned}$$

Mamy więc ciąg ideałów $G_0 \subseteq G_1 \subseteq \ldots \subseteq G_{N-1}$. Zauważmy, że G_0 jest ideałem głównym generowanym przez $\deg g$. Mamy ponadto

Stwierdzenie 6.1. *$G_0 \neq G_1$.*

Dowód. Wiemy ze Stwierdzenia 5.4, że istnieje $h_1 \in L_1 \setminus L_0$ takie, że $\deg h_1$ nie przystaje do 0 modulo $\deg g$. Oznacza to, że $\deg h_1 \in G_1 \setminus G_0$. ⊠

Zdefiniujemy teraz ciąg $c(1), c(2), \ldots, c(p)$ pewnych liczb naturalnych.

Definicja 6.2.
(1) $c(1) = 1$.
(2) *Załóżmy, że liczby $c(1), \ldots, c(m)$ są już określone i niech S będzie zbiorem wszystkich liczb naturalnych $n \in \{c(m)+1, c(m)+2, \ldots, N-1\}$ takich, że $G_{c(m)} \subsetneq G_n$. Jeżeli $S = \emptyset$, to definiowanie kończymy i liczbę m oznaczamy przez p. Jeżeli $S \neq \emptyset$, to $c(m+1)$ jest najmniejszym elementem zbioru S.*

Przyjmujemy dodatkowo, że $c(p+1) = N$.
Zdefiniowany powyżej ciąg $c(1), \ldots, c(p)$ posiada następujące własności:

(i) $\quad c(1) = 1,$

(ii) $\quad c(1) < c(2) < \ldots < c(p) \leqslant N-1,$

(iii) $\quad G_0 \subsetneq G_{c(1)} \subsetneq \ldots \subsetneq G_{c(p)},$

(iv) $\quad G_{c(n)} = G_{c(n)+1} = \ldots = G_{c(n+1)-1}, \quad \text{dla } n = 1, \ldots, p.$

Pokażemy teraz, że ciąg $c(1), \ldots, c(p)$ można zdefiniować także w inny sposób; przy pomocy α-systemu. W tym celu udowodnimy najpierw następujące stwierdzenie.

Stwierdzenie 6.3. *Niech $(h_1, \ldots, h_{N-1})$ będzie α-systemem. Oznaczmy $h_0 = g$ i niech n będzie liczbą naturalną należącą do zbioru $\{1, \ldots, N-1\}$. Wtedy:*

(1) $U_n = \bigcup_{j=0}^{n} \{\deg h_j + \mathbb{Z} \deg g\}$,
(2) $G_n = (\deg h_0, \deg h_1, \ldots, \deg h_n)$.

Dowód. (1) Niech $0 \leqslant j \leqslant n$, $s \in \mathbb{Z}$. Wtedy $\deg h_j + s \deg g = \deg(g^s h_j) \in U_n$, więc $\cup_{j=0}^{n} \{\deg h_j + \mathbb{Z} \deg g\} \subseteq U_n$. Inkluzja odwrotna wynika z faktu, że wszystkie liczby $\deg g, \deg h_1, \ldots, \deg h_{N-1}$ są parami nieprzystające modulo $\deg g$.
(2) Wynika z (1) oraz ze Stwierdzenia 3.1. ⊠

Niech $(h_1, \ldots, h_{N-1})$ będzie α-systemem. Przyjmijmy dodatkowo, że $h_0 = g$ i oznaczmy:

$$\begin{aligned} d_0 &= \deg h_0 = \deg g \\ d_1 &= \deg h_1 \\ &\vdots \\ d_{N-1} &= \deg h_{N-1}. \end{aligned}$$

Liczby $d_0, d_1, \ldots, d_{N-1}$ są całkowite (mogą być ujemne) i żadne dwie spośród nich nie przystają do siebie modulo $d_0 = \deg g$. Teraz ciąg $c(1), \ldots, c(p)$ można zdefiniować w następujący sposób:

Definicja 6.4.
(1) $c(1) = 1$.
(2) *Załóżmy, że liczby* $c(1), \ldots, c(m)$ *są już zdefiniowane. Jeżeli liczby* d_0, $d_1, \ldots, d_{N-1}$ *należą do ideału* $(d_0, d_1, \ldots, d_{c(m)})$, *to* $c(m)$ *jest ostatnim wyrazem ciągu i w tym przypadku liczbę* m *oznaczamy przez* p. *W przeciwnym przypadku przyjmujemy* $c(m+1) = i$, *gdzie* i *jest najmniejszą z liczb* $c(m)+1, c(m)+2, \ldots, N-1$ *taką, że* $d_i \notin (d_0, d_1, \ldots, d_{c(m)})$.

Widzimy (na mocy Stwierdzenia 6.3), że powyższe dwie definicje określają ten sam ciąg $c(1), \ldots, c(p)$. Z Definicji 6.2 wynika, że ciąg ten nie zależy od wyboru α-systemu.

Zanotujmy jeszcze następujące oczywiste stwierdzenie.

Stwierdzenie 6.5. *Niech* $n \in \{1, \ldots, N-1\}$. *Następujące warunki są równoważne:*
(1) n *występuje w ciągu* $c(1), \ldots, c(p)$;
(2) *istnieje* $\varphi \in \overline{A}_n$ *takie, że* $\deg \varphi \notin G_n$;
(3) $G_{n-1} \neq G_n$. $\boxtimes$

7 Liczby e_1,...,e_p i własności ciągu c(1),...,c(p)

Niech $(h_1, \ldots, h_{N-1})$ będzie ustalonym α-systemem. Niech $h_0 = g$ i niech $d_i = \deg h_i$ dla $i = 0, 1, \ldots, N-1$. W poprzednim rozdziale zdefiniowaliśmy ciąg $c(1), \ldots, c(p)$. Przyjmujemy dodatkowo, że $c(p+1) = N$.

Oznaczmy przez $D_0, D_1, \ldots, D_p$ ideały pierścienia $\mathbb{Z}$ zdefiniowane następująco:

Definicja 7.1.

$$D_j = \begin{cases} (d_0), & dla \quad j = 0, \\ (d_0, d_1, \ldots, d_{c(j)}), & dla \quad j \in \{1, \ldots, p\}. \end{cases}$$

Niech $s \in \{1, \ldots, p\}$. Wiemy (patrz Definicja 6.4), że $d_{c(s)} \notin D_{s-1}$. Każdy ideał w $\mathbb{Z}$ jest ideałem głównym. W szczególności D_{s-1} jest ideałem głównym. Istnieje zatem liczba naturalna n taka, że $nd_{c(s)} \in D_{s-1}$.

Definicja 7.2. *Najmniejszą liczbę naturalną* n *taką, że* $nd_{c(s)} \in D_{s-1}$ *oznaczać będziemy przez* e_s.

W ten sposób pojawiają nam się liczby naturalne $e_1, \ldots, e_p$. Są to liczby większe od 1. W niniejszym rozdziale udowodnimy następujące stwierdzenie.

Stwierdzenie 7.3 ([11]). *Jeżeli $s \in \{1, \ldots, p\}$, to $e_s c(s) = c(s+1)$.*

Przed dowodem tego stwierdzenia wprowadzimy pewien nowy zbiór B_s i udowodnimy kilka lematów.

Niech s będzie ustalonym elementem zbioru $\{1, \ldots, p\}$. Oznaczmy:

$$B_s = \{h_n h_{c(s)}^j \ ; \ 0 \leqslant n < c(s), \ 0 \leqslant j < e_s\}.$$

W szczególności mamy:

$$B_1 = \{g = gh_1^0, \ gh_1^1, \ \ldots, \ gh_1^{e_1-1}\}.$$

Lemat 7.4.

(1) *Stopnie elementów zbioru B_s są parami nieprzystające modulo $d_0 = \deg g$.*

(2) *$|B_s| = e_s c(s)$ (gdzie $|B_s|$ oznacza moc zbioru B_s).*

(3) *Zbiór B_s jest liniowo niezależny nad $k(g)$.*

(4) *$e_s c(s) \leqslant N$.*

(5) *Zbiór B_s jest bazą przestrzeni liniowej $\overline{L}_{e_s c(s)-1}$ nad $k(g)$.*

Dowód. (1). Przypuśćmy, że

$$\deg(h_n h_{c(s)}^a) \equiv \deg(h_m h_{c(s)}^b) \pmod{d_0},$$

gdzie $n, m \in \{0, 1, \ldots, c(s)-1\}$ oraz $0 \leqslant a, b < e_s$. Jeżeli $a = b$, to $\deg h_n \equiv \deg h_m \pmod{d_0}$ i z definicji α-systemu wynika, że $n = m$. Możemy więc założyć, że $a \neq b$.

Niech $a > b$. Wtedy $(a-b)d_{c(s)} \in D_{s-1}$ i mamy sprzeczność z własnością minimalności liczby e_s. Podobnie postępujemy w przypadku gdy $b > a$.

(2). Z (1) wynika, że elementy postaci $h_n h_{c(s)}^j$ (gdzie $0 \leqslant n < c(s)$ i $0 \leqslant j < e_s$) są parami różne. Jest ich oczywiście $c(s)e_s$.

(3). Niech $\alpha_1 a_1 + \cdots + \alpha_n a_n = 0$, gdzie $\alpha_1, \ldots, \alpha_n \in k(g)$ oraz $a_1, \ldots, a_n$ są parami różnymi elementami zbioru B_s.

Przypuśćmy, że $\alpha_1 \neq 0$. Wtedy $a_1 = -\alpha_1^{-1}\alpha_2 a_2 - \cdots - \alpha_1^{-1}\alpha_n a_n$. Ponieważ stopnie elementów postaci $\alpha_1^{-1}\alpha_i$ są podzielne przez d_0, więc z (1) wynika, że liczba $\deg a_1$ jest równa jednej z liczb $\deg(\alpha_1^{-1}\alpha_2 a_2), \ldots, \deg(\alpha_1^{-1}\alpha_n a_n)$. Jest to jednak sprzeczne z (1).

(4). Wynika to z (2) i (3) oraz z tego, że $B_s \subseteq k(f,g)$ i $N = (k(f,g) : k(g))$.

(5). Jeżeli $0 \leqslant n < N$, to wielomiany $f^0, f^1, \ldots, f^n$ są liniowo niezależne nad $k(g)$. Każda więc przestrzeń nad $k(g)$, postaci $\overline{L}_n$, ma wymiar równy $n+1$. Ponieważ $e_s c(s) - 1 < N$ (patrz (4)), więc w szczególności $\dim_{k(g)} \overline{L}_{e_s c(s)-1} = e_s c(s)$. Wiemy z (2) i (3), że podprzestrzeń generowana przez zbiór B_s ma też wymiar równy $e_s c(s)$. Wystarczy zatem pokazać, że $B_s \subseteq \overline{L}_{e_s c(s)-1}$.

Niech $u = h_n h_{c(s)}^j$, gdzie $0 \leqslant n < c(s)$ i $0 \leqslant j < e_s$. Mamy wtedy:

$$u \in \overline{A}_n (\overline{A}_{c(s)})^j \subseteq \overline{A}_{n+jc(s)} \subseteq \overline{L}_{n+jc(s)} \subseteq \overline{L}_{e_s c(s)-1}$$

i stąd wynika, że $B_s \subseteq \overline{L}_{e_s c(s)-1}$. $\boxtimes$

Lemat 7.5. $e_s c(s) \leqslant c(s+1)$.

Dowód. Jeżeli $s = p$, to nierówność wynika z Lematu 7.4(4) (gdyż $c(p+1) = N$). Załóżmy więc, że $s < p$ i niech m będzie liczbą naturalną mniejszą od $e_s c(s)$. Wtedy $h_m \in \overline{L}_{e_s c(s)-1}$, a zatem, na mocy Lematu 7.4(5), $h_m = \alpha_1 a_1 + \cdots + \alpha_n a_n$, gdzie $\alpha_1, \ldots, \alpha_n \in k(g)$ i $a_1, \ldots, a_n$ są parami różnymi elementami zbioru B_s. Z Lematu 7.4(1) wiemy, że elementy $a_1, \ldots, a_s$ mają parami nieprzystające stopnie modulo d_0. Stąd wynika, że $d_m = \deg h_m = \deg(\alpha_j a_j)$, dla pewnego $j \in \{1, \ldots, n\}$. Ponadto jest oczywiste, że $\deg(\alpha_j a_j) \in D_s$, czyli $d_m \in D_s$. Jeżeli więc $m < e_s c(s)$, to $d_m \in D_s$. Z definicji ciągu $c(1), \ldots, c(p)$ wiemy, że $d_{c(s+1)} \notin D_s$. Zatem $c(s+1) \geqslant e_s c(s)$. $\boxtimes$

Lemat 7.6. *Dla każdego $w \in D_s$ istnieje $b \in B_s$ takie, że $w \equiv \deg b \pmod{d_0}$.*

Dowód. Indukcja ze względu na s. Niech $s = 1$. Przypomnijmy, że $c(1) = 1$, $B_1 = \{gh_1^0 = g, gh_1^1, \ldots, gh_1^{e_1-1}\}$ oraz $D_1 = (d_0, d_1)$. Niech $w \in D_1$. Istnieją wtedy liczby całkowite a i m takie, że $w = ad_0 + md_1$. Ponieważ $e_1 d_1 \in (d_0)$, więc możemy założyć, że $0 \leqslant m < e_1$. Wtedy $w = a \deg g + \deg h_1^m = (a-1)\deg g + \deg(gh_1^m)$, czyli $w \equiv b \pmod{d_0}$, gdzie $b = gh_1^m \in B_1$.

Załóżmy teraz, że lemat jest prawdziwy dla pewnego $s \in \{1, \ldots, p-1\}$ i niech $w \in D_{s+1}$. Ponieważ $D_{s+1} = D_s + (d_{c(s+1)})$, więc $w = w' + md_{c(s+1)}$, gdzie $w' \in D_s$ oraz $m \in \mathbb{Z}$. Wiemy, że $e_{s+1} d_{c(s+1)} \in D_s$. Możemy zatem założyć, że $0 \leqslant m < e_{s+1}$. Ponadto, na mocy indukcji, $w' \equiv \deg b' \pmod{d_0}$ dla pewnego $b' \in B_s$. Z Lematów 7.4 i 7.5 oraz ze Stwierdzenia 3.1 wynika, że

$$b' \in B_s \subseteq \overline{L}_{e_s c(s)-1} \subseteq \overline{L}_{c(s+1)-1} = k(g)h_{c(s+1)-1} + \cdots + k(g)h_0.$$

Zatem $\deg b' \equiv \deg h_r \pmod{d_0}$, dla pewnego $r < c(s+1)$ (gdyż $h_0, \ldots, h_{c(s+1)-1}$ mają parami nieprzystające stopnie). Mamy teraz:

$$w = w' + md_{c(s+1)} \equiv \deg b' + \deg h_{c(s+1)}^m \equiv \deg h_r + \deg h_{c(s+1)}^m = \deg b,$$

gdzie $b = h_r h_{c(s+1)}^m \in B_{s+1}$. $\boxtimes$

Teraz możemy już udowodnić zapowiedziane stwierdzenie.

Dowód Stwierdzenia 7.3. Niech $n = e_s c(s)$. Wtedy (Lemat 7.4) $n \leqslant N$. Załóżmy, że $n = N$ i przypuśćmy, że $s < p$. Wówczas (na mocy Lematu 7.5) otrzymujemy następującą sprzeczność: $N = e_s c(s) \leqslant c(s+1) \leqslant c(p) \leqslant N - 1$. Jeżeli więc $n = N$, to $s = p$ i mamy $e_p c(p) = N = c(p+1)$.

Załóżmy teraz, że $n < N$. Pokażemy, że $d_n \notin D_s$. Przypuśćmy, że tak nie jest. Niech $d_n \in D_s$. Wtedy istnieje element $b \in B_s$ (patrz Lemat 7.6) taki, że $d_n \equiv \deg b \pmod{d_0}$. Ale, na mocy Lematu 7.4 i Stwierdzenia 3.1, $B_s \subset \overline{L}_{e_s c(s)-1} = \overline{L}_{n-1} = k(g)h_{n-1} + \cdots + k(g)h_0$, więc $\deg b \equiv \deg h_j$ dla

pewnego $j < n$. Stąd wynika, że $\deg h_n = d_n \equiv \deg h_j$ wbrew temu, że elementy $h_0, \ldots, h_n$ mają parami nieprzystające stopnie.

Wykazaliśmy więc, że $d_n \notin D_s$. Zatem $n \geqslant c(s+1)$ (patrz Definicja 6.4), czyli $e_s c(s) \geqslant c(s+1)$ i z Lematu 7.5 wynika, że $e_s c(s) = c(s+1)$. ⊠

Wniosek 7.7. *Jeżeli* $s \in \{1, \ldots, p\}$, *to* $e_1 e_2 \ldots e_s = c(s+1)$.

Dowód. $e_1 = e_1 c(1) = c(2)$, $e_1 e_2 = c(2) e_2 = c(3)$, itd. ⊠

8 Funkcje wymierne postaci w(H, s)

Począwszy od Rozdziału 5 zmierzamy do wykazania, że istnieje β-system. Fakt ten jest istotny w dowodzie Twierdzenia Abhyankara i Moha przedstawionym w Rozdziale 4. Wiemy już, że istnieje α-system. Wykazaliśmy to w Rozdziale 5.

W niniejszym rozdziale z każdym α-systemem $\mathbb{H}$ stowarzyszymy pewne, jednoznacznie wyznaczone, funkcje wymierne $w(\mathbb{H}, 1), \ldots, w(\mathbb{H}, p)$, należące odpowiednio do przestrzeni $\overline{L}_{c(1)-1}, \ldots, \overline{L}_{c(p)-1}$. Wykażemy, że stopnie tych funkcji są mniejsze odpowiednio od liczb $d_{c(1)}, \ldots, d_{c(s)}$. To pozwoli nam udowodnić (w następnym rozdziale), że istnieje α-system, dla którego wszystkie powyższe funkcje są zerowe. Fakt ten będzie bardzo użyteczny w dowodzie twierdzenia o istnieniu β-systemu.

Niech $\mathbb{H} = (h_1, \ldots, h_{N-1})$ będzie α-systemem i niech s będzie ustaloną liczbą naturalną należącą do zbioru $\{1, \ldots, p\}$. Zakładać będziemy dodatkowo, że $h_0 = g$ oraz $h_N = 0$. Przed wprowadzeniem zapowiedzianej funkcji wymiernej postaci $w(\mathbb{H}, s)$ udowodnimy następujące dwa stwierdzenia.

Stwierdzenie 8.1. *Dla każdego* $w \in \overline{L}_{c(s+1)-1}$ *istnieją jednoznacznie wyznaczone elementy* $w_1, w_2, \ldots, w_e$ *należące do* $\overline{L}_{c(s)-1}$ *takie, że*

$$w = w_1 h^{e-1} + w_2 h^{e-2} + \cdots + w_{e-1} h^1 + w_e h^0, \tag{8.1}$$

gdzie $h = h_{c(s)}$ *oraz* $e = e_s$.

Dowód. Niech, tak jak w Rozdziale 7, $B = B_s = \{h_n h^j;\ 0 \leqslant n < c(s),\ 0 \leqslant j < e\}$. Wiemy, że zbiór B jest bazą nad $k(g)$ przestrzeni $\overline{L}_{ec(s)-1} = \overline{L}_{c(s+1)-1}$ (patrz Lemat 7.4 i Stwierdzenie 7.3). Zatem $w = a_1 b_1 + \cdots + a_r b_r$, gdzie $a_1, \ldots, a_r \in k(g)$ oraz $b_1, \ldots, b_r$ są parami różnymi elementami zbioru B. Wyłączając w tym rozkładzie elementy postaci $h^0, \ldots, h^{e-1}$ i grupując odpowiednio pozostałe elementy, otrzymujemy rozkład (8.1), w którym elementy $w_1, \ldots, w_e$ należą do przestrzeni $k(g)h_0 + \cdots + k(g)h_{c(s)-1} = \overline{L}_{c(s)-1}$. Jednoznaczność wynika z tego, że zbiory B_s są liniowo niezależne nad $k(g)$. ⊠

Stwierdzenie 8.2. $h_{c(s)}^{e_s} - h_{c(s+1)} \in \overline{L}_{c(s+1)-1}$.

Dowód. Niech $H = h_{c(s)}^{e_s} - h_{c(s+1)}$. Jeżeli $s = p$, to $H = h_{c(p)}^{e_p}$ (gdyż $h_{c(p+1)} = h_N = 0$) i wtedy $H \in k(f,g) = \overline{L}_{N-1} = \overline{L}_{c(p+1)-1}$. Dla $s < p$ mamy:

$$h_{c(s)}^{e_s} \in (\overline{A}_{c(s)})^{e_s} \subseteq \overline{A}_{e_s c(s)} = \overline{A}_{c(s+1)}$$

(patrz Stwierdzenie 7.3) oraz $h_{c(s+1)} \in \overline{A}_{c(s+1)}$. Ponieważ $\overline{A}_{c(s+1)} = f^{c(s+1)} + \overline{L}_{c(s+1)-1}$, więc $H \in \overline{L}_{c(s+1)-1}$. ⊠

Z powyższych dwóch stwierdzeń wynika natychmiast następujący wniosek.

Wniosek 8.3. *Istnieją jednoznacznie wyznaczone elementy $w_1, w_2, \ldots, w_e$ należące do $\overline{L}_{c(s)-1}$ takie, że*

$$h^e - h_{c(s+1)} = w_1 h^{e-1} + w_2 h^{e-2} + \cdots + w_{e-1} h^1 + w_e h^0, \tag{8.2}$$

gdzie $h = h_{c(s)}$ oraz $e = e_s$. ⊠

Definicja 8.4. *Element $w_1 \in \overline{L}_{c(s)-1}$ z Wniosku 8.3 oznaczać będziemy przez $w(\mathbb{H}, s)$.*

Stwierdzenie 8.5. $\deg w(\mathbb{H}, s) < \deg h_{c(s)}$.

Dowód. Niech $h = h_{c(s)}$, $e = e_s$, $B = B_s = \{h_n h^j;\ 0 \leqslant n < c(s),\ 0 \leqslant j < e\}$ i niech

$$h^e - h_{c(s+1)} = a_1 b_1 + \cdots + a_r b_r, \tag{8.3}$$

gdzie $a_1, \ldots, a_r \in k(g)$ i $b_1, \ldots, b_r$ są parami różnymi elementami zbioru B. Ponieważ stopnie elementów $b_1, \ldots, b_r$ są parami nieprzystające modulo d_0 (Lemat 7.4), więc istnieje $q \in \{1, \ldots, r\}$ takie, że

$$\deg(h^e - h_{c(s+1)}) = \deg(a_q b_q) \tag{8.4}$$

oraz $\deg(h^e - h_{c(s+1)}) > \deg(a_i b_i)$ dla wszystkich $i \neq q$.

Z równości (8.4) wynika, że liczba $\deg(h^e - h_{c(s+1)})$ należy do ideału D_s. Mamy ponadto: $\deg h^e = e d_{c(s)} \in D_s$ oraz $\deg h_{c(s+1)} = d_{c(s+1)} \notin D_s$. Stąd wnioskujemy, że $\deg h_{c(s+1)} < \deg h^e$, czyli $\deg(h^e - h_{c(s+1)}) = \deg h^e = e \deg h$. Mamy zatem:

$$\deg(a_q b_q) = e \deg h \quad \text{oraz} \quad \deg(a_i b_i) < e \deg h \quad \text{dla} \quad i \neq q. \tag{8.5}$$

Zauważmy jeszcze, że jeżeli $\deg b_j \notin D_{s-1}$ (gdzie $j \in \{1, \ldots, r\}$), to $j \neq q$. Istotnie, gdyby j było równe q wówczs, na mocy (8.5), $\deg(a_j b_j) = e \deg h = e_s d_{c(s)} \in D_{s-1}$ (patrz definicja liczby e_s). Ponadto $\deg a_j \in D_0 \subseteq D_{s-1}$.

Mielibyśmy więc sprzeczność: $\deg b_j = \deg(a_j b_j) - \deg a_j \in D_{s-1}$. Zatem $j \neq q$, a zatem z (8.5) wynika, że

$$\text{jeżeli } \deg b_j \notin D_{s-1}, \text{ to } \deg(a_j b_j) < e \deg h. \tag{8.6}$$

Wróćmy teraz do równości (8.3) i spójrzmy na elementy $b_1, \ldots, b_r$ należące do zbioru B. Wybierzmy spośród tych elementów te wszystkie, które posiadają czynnik h^{e-1}. Jeżeli takich elementów nie ma, to z jednoznaczności rozkładów (8.3) i (8.2) wynika, że $w(\mathbb{H}, s) = 0$ i wtedy stwierdzenie nasze jest udowodnione, gdyż wtedy $\deg w(\mathbb{H}, s) = -\infty < \deg h$ (ponieważ $h \neq 0$).

Załóżmy więc, że $\{b_1, \ldots, b_m\}$, gdzie $m \leqslant r$, jest zbiorem tych wszystkich elementów spośród $b_1, \ldots, b_r$, które posiadają czynnik h^{e-1}. Mamy wówczas:

$$a_1 b_1 + \cdots + a_m b_m = w(\mathbb{H}, s) h^{e-1}. \tag{8.7}$$

Niech $j \in \{1, \ldots, m\}$. Wtedy $b_j = h_n h^{e-1}$, dla pewnego n takiego, że $0 \leqslant n < c(s)$. To implikuje, że $\deg b_j \notin D_{s-1}$. Istotnie, gdyby liczba $\deg b_j = \deg h_n + (e-1)d_{c(s)}$ należała do ideału D_{s-1}, to należałaby do tego ideału także liczba $(e-1)d_{c(s)}$ (gdyż $\deg h_n = d_n \in D_{s-1}$). Byłoby to sprzeczne z własnością minimalności liczby e. Teraz, na mocy (8.6) wnioskujemy, że $\deg(a_j b_j) < e \deg h$, czyli (patrz (8.7) $\deg(w(\mathbb{H}, s) + (e-1) \deg h = \deg(w(\mathbb{H}, s) h^{e-1} < e \deg h$ i stąd wynika, że $\deg w(\mathbb{H}, s) < \deg h_{c(s)}$. ⊠

9 Nowe α-systemy

Niech $\mathbb{H} = (h_1, \ldots, h_{N-1})$ będzie α-systemem. Niech $h_0 = g$, $h_N = 0$ i załóżmy, że s jest ustaloną liczbą ze zbioru $\{1, \ldots, p\}$. Oznaczmy przez $\overline{\mathbb{H}}$ ciąg $(\overline{h}_1, \ldots, \overline{h}_{N-1})$ funkcji wymiernych należących do ciała $k(f, g)$, zdefiniowanych następująco:

Definicja 9.1.

$$\overline{h}_n = \begin{cases} h_n, & dla \quad n \neq c(s), \\ h_{c(s)} - (1/e_s) w(\mathbb{H}, s), & dla \quad n = c(s). \end{cases}$$

Stwierdzenie 9.2. *$\overline{\mathbb{H}}$ jest α-systemem.*

Dowód. Ponieważ $h_{c(s)} \in \overline{A}_{c(s)} = f^{c(s)} + \overline{L}_{c(s)-1}$ i $w(\mathbb{H}, s) \in \overline{L}_{c(s)-1}$, więc $\overline{h}_{c(s)}$ należy do zbioru $\overline{A}_{c(s)}$. Zatem $\overline{h}_n \in \overline{A}_n$, dla $n \in \{1, \ldots, N-1\}$. Wiemy (patrz Stwierdzenie 8.5), że $\deg w(\mathbb{H}, s) < \deg h_{c(s)}$. To implikuje, że $\deg \overline{h}_{c(s)} = \deg h_{c(s)}$, a zatem liczby $0, \deg \overline{h}_1, \ldots, \overline{h}_{N-1}$ są parami nieprzystające modulo $\deg g$. ⊠

W dowodzie następnego stwierdzenia wykorzystamy następujący lemat.

Lemat 9.3. *Jeżeli $a_2, a_3, \ldots, a_e \in \overline{L}_{c(s)-1}$, to istnieją jednoznacznie wyznaczone elementy $b_2, b_3, \ldots, b_e \in \overline{L}_{c(s)-1}$ takie, że*

$$a_2 h^{e-2} + a_3 h^{e-3} + \cdots + a_e = b_2 \overline{h}^{e-2} + b_3 \overline{h}^{e-3} + \cdots + b_e,$$

gdzie $h = h_{c(s)}$, $\overline{h} = \overline{h}_{c(s)}$ i $e = e_s$.

Dowód. Niech $u = a_2 h^{e-2} + \cdots + a_e$. Zauważmy, że $u \in \overline{L}_{(e-1)c(s)-1}$. Istotnie,

$$\begin{aligned} u \in \overline{L}_{c(s)-1}(\overline{A}_{c(s)})^{e-2} &\subseteq \overline{L}_{c(s)-1}(\overline{L}_{c(s)})^{e-2} \\ &\subseteq \overline{L}_{c(s)-1+(e-2)c(s)} = \overline{L}_{(e-1)c(s)-1}. \end{aligned} \tag{9.1}$$

Przestrzeń $\overline{L}_{(e-1)c(s)-1}$ jest oczywiście zawarta w $\overline{L}_{ec(s)-1} = \overline{L}_{c(s+1)-1}$, a zatem $u \in \overline{L}_{c(s+1)-1}$ i, na mocy Stwierdzenia 8.1, istnieją jednoznacznie wyznaczone elementy $b_1, \ldots, b_e \in \overline{L}_{c(s)-1}$ takie, że

$$u = b_1 \overline{h}^{e-1} + b_2 \overline{h}^{e-2} + \cdots + b_e.$$

Musimy pokazać, że $b_1 = 0$. Przypuśćmy, że tak nie jest. Niech $b_1 \in \overline{L}_n \setminus \overline{L}_{n-1}$, gdzie $0 \leqslant n < c(s)$ (przy czym zakładamy, że $\overline{L}_{-1} = 0$). Wtedy $b_1 \overline{h}^{e-1} \in \overline{L}_{n+(e-1)c(s)} \setminus V$, gdzie $V = \overline{L}_{n-1+(e-1)c(s)}$ oraz

$$b_1 \overline{h}^{e-1} = u - \overline{u}, \tag{9.2}$$

gdzie $\overline{u} = b_2 \overline{h}^{e-2} + \cdots + b_e$. Tak samo jak w (9.1) pokazujemy, że $\overline{u} \in \overline{L}_{(e-1)c(s)-1}$. Ale $\overline{L}_{(e-1)c(s)-1} \subseteq V$. Zatem prawa strona równości (9.2) należy V. Natomiast lewa strona tej równości do V nie należy. Otrzymana sprzeczność świadczy o tym, że $b_1 = 0$ i to kończy dowód naszego lematu. ⊠

Stwierdzenie 9.4 (por. [6] str. 403**).** *Niech $w = w(\mathbb{H}, s)$ i $\overline{w} = w(\overline{\mathbb{H}}, s)$. Załóżmy, że $w \neq 0$.*

(1) Jeżeli $w \in \overline{L}_0 = k(g)$, to $\overline{w} = 0$.

(2) Jeżeli $w \in \overline{L}_j \setminus \overline{L}_{j-1}$, gdzie $0 < j < c(s)$, to $\overline{w} = 0$ lub $\overline{w} \in \overline{L}_i \setminus \overline{L}_{i-1}$ dla pewnego i takiego, że $0 \leqslant i < j$.

Dowód. Niech $e = e_s$, $h = h_{c(s)}$, $\overline{h} = \overline{h}_{c(s)} = h - (1/e)w$ i niech

$$R = \sum_{r=0}^{e-2} \binom{e}{r} h^r (-\frac{1}{e} w)^{e-r}$$

(przypomnijmy że $e \geqslant 2$; patrz Rozdział 7). Wtedy

$$h^e - h_{c(s+1)} = w h^{e-1} + w_2 h^{e-2} + \cdots + w_{e-1} h^1 + w_e h^0,$$

gdzie $w_2, \ldots, w_e \in \overline{L}_{c(s)-1}$, oraz

$$\begin{aligned} \overline{h}^e - \overline{h}_{c(s+1)} &= (h - \tfrac{1}{e}w)^e - h_{c(s+1)} \\ &= h^e - \tbinom{e}{1}h^{e-1}(\tfrac{1}{e})w^1 + R - h_{c(s+1)} \\ &= (h^e - h_{c(s+1)}) - wh^{e-1} + R \\ &= (w_2h^{e-2} + \cdots + w_{e-1}h^1 + w_e) + R \end{aligned}$$

Z Lematu 9.3 wynika, że istnieją elementy $b_2, \ldots, b_e \in \overline{L}_{c(s)-1}$ takie, że $w_2h^{e-2} + \cdots + w_{e-1}h^1 + w_e = b_2\overline{h}^{e-2} + \cdots + b_{e-1}\overline{h}^1 + b_e$, a zatem

$$\overline{h}^e - \overline{h}_{c(s+1)} = (b_2\overline{h}^{e-2} + \cdots + b_{e-1}\overline{h}^1 + b_e) + R. \tag{9.3}$$

Zajmiemy się teraz składnikiem R. Załóżmy, że $w \in \overline{L}_j$, gdzie $0 \leqslant j < c(s)$ i niech $m \in \{0, 1, \ldots, e-2\}$. Wtedy

$$h^m w^{e-m} \in \overline{L}^m_{c(s)}\overline{L}^{e-m}_j \subseteq \overline{L}_{mc(s)+j(e-m)}$$

i łatwo można sprawdzić, że $mc(s)+j(e-m) \leqslant (e-1)c(s)+j-1$. Stąd wynika, że

$$R \in \overline{L}_{(e-1)c(s)+j-1}. \tag{9.4}$$

Zauważmy dalej, że $(e-1)c(s) + j - 1 \leqslant ec(s) - 1 = c(s+1) - 1$. Zatem $R \in \overline{L}_{c(s+1)-1}$, a zatem na mocy Stwierdzenia 8.1, istnieją jednoznacznie wyznaczone elementy $z_1, \ldots, z_e \in \overline{L}_{c(s)-1}$ takie, że

$$R = z_1\overline{h}^{e-1} + \cdots + z_{e-1}\overline{h}^1 + z_e. \tag{9.5}$$

Teraz z (9.3) i (9.5) otrzymujemy równość

$$\overline{w} = w(\overline{\mathbb{H}}, s) = z_1.$$

Zauważmy jeszcze, że

$$z_2\overline{h}^{e-2} + \cdots + z_e \in \overline{L}_{c(s)-1}(\overline{L}_{c(s)})^{e-2} \subseteq \overline{L}_{(e-1)c(s)-1}.$$

Mamy więc, na mocy (9.4),

$$\overline{w}\overline{h}^{e-1} = z_1\overline{h}^{e-1} \in \overline{L}_{(e-1)c(s)+j-1}. \tag{9.6}$$

Stąd już łatwo można wywnioskować tezę naszego stwierdzenia. Załóżmy, że $\overline{w} \neq 0$. Wtedy $\overline{w} \in \overline{L}_i \setminus \overline{L}_{i-1}$ dla pewnego i takiego, że $0 \leqslant i < c(s)$, przy czym zakładamy, że $\overline{L}_{-1} = 0$. Ponieważ $\overline{h}^{e-1} \in \overline{A}_{(e-1)c(s)}$, więc

$$\overline{w}\overline{h}^{e-1} \in \overline{L}_{(e-1)c(s)+i} \setminus \overline{L}_{(e-1)c(s)+i-1}. \tag{9.7}$$

Jeżeli $j = 0$, to własność (9.6) jest sprzeczna z własnością (9.7). Jeżeli więc $j = 0$ (czyli, gdy $w \in k(g)$), to $\overline{w} = 0$. Udowodniliśmy zatem (1).

Niech teraz $j > 0$. Wtedy z (9.6) i (9.7) wynika, że $(e-1)c(s) + i - 1 < (e-1)c(s) + j - 1$ czyli $i < j$, a zatem wykazaliśmy (2). $\boxtimes$

Pokazaliśmy, że przy pomocy danego α-system $\mathbb{H}$ można otrzymać nowy α-system $\overline{\mathbb{H}}$. W ten sam sposób z α-systemu $\overline{\mathbb{H}}$ powstaje α-system $\overline{\overline{\mathbb{H}}}$ itd. Zróbmy taką zamianę dostateczną ilość razy (dla każdego $s = 1, \ldots, p$). Wówczas, na podstawie Stwierdzenia 9.4, otrzymujemy:

Stwierdzenie 9.5. *Istnieje α-system $\mathbb{H}$ taki, że dla każdego $s \in \{1, \ldots, p\}$ zachodzi równość $w(\mathbb{H}, s) = 0$.* $\boxtimes$

Zanotujmy następujący lemat.

Lemat 9.6 ([2]). *Niech e, n będą liczbami naturalnymi takimi, że $en \leqslant N$. Niech $u, v \in k(f, g)$. Załóżmy, że $u \in \overline{A}_n$, $v \in A_{en}$ oraz $u^e - v \in \overline{L}_{en-n-1}$ (przy czym zakładamy, że $\overline{L}_{-1} = 0$). Wtedy $u \in A_n$.*

Dowodem tego lematu zajmiemy się w ostatnim rozdziale, w którym udowodnimy pewien fakt ogólniejszy (Stwierdzenie 11.1). Teraz pokażemy jak przy pomocy Lematu 9.6 można udowodnić następujące stwierdzenie.

Stwierdzenie 9.7. *Istnieje α-system $\mathbb{H} = (h_1, \ldots, h_{N-1})$ taki, że każdy element postaci $h_{c(s)}$ (dla $s = 1, \ldots, p$) należy do pierścienia $k[f, g]$.*

Dowód. Niech $\mathbb{H}$ będzie α-systemem takim, jak w Stwierdzeniu 9.5. Pokażemy, że jeżeli $s \in \{1, \ldots, p\}$, to $h_{c(s)} \in k[f, g]$.

Załóżmy najpierw, że $s = p$. Niech $u = h_{c(p)}$, $v = h_{c(p+1)} = h_N = 0$, $e = e_p$, $n = c(p)$. Wtedy $u, v \in k(f, g)$, $en = e_p c(p) = c(p+1) = N$, $u \in \overline{A}_n$ oraz równość $N = (k(g)(f) : k(g))$ implikuje, że $v = 0 \in A_N = A_{en}$. Ponadto (na mocy Wniosku 8.3 i Definicji 8.4),

$$u^e - v = h_{c(p)}^e - h_{c(p+1)} = w_2 h_{c(p)}^{e-2} + \cdots + w_{e-1} h_{c(p)} + w_e,$$

gdzie $w_2, \ldots, w_e$ są pewnymi elementami należącymi do $\overline{L}_{c(p)-1}$. Stąd wynika, że

$$u^e - v \in \overline{L}_{c(p)-1} (\overline{L}_{c(p)})^{e-2} \subseteq \overline{L}_{ec(p)-c(p)-1} = \overline{L}_{en-n-1}.$$

Spełnione są więc wszystkie założenia Lematu 9.6. Zatem $h_{c(p)} = u \in A_n \subseteq k[f, g]$.

Niech teraz $s + 1 \leqslant p$ i załóżmy, że $h_{c(s+1)} \in k[f, g]$. Oznaczmy: $u = h_{c(s)}$, $v = h_{c(s+1)}$, $e = e_s$ i $n = c(s)$. Wtedy $en = e_s c(s) = c(s+1) \leqslant c(p) < N$, $u \in \overline{A}_n$ oraz $v \in k[f, g] \cap \overline{A}_{c(s+1)} = A_{c(s+1)} = A_{en}$ (patrz Stwierdzenie 2.1). Tak samo, jak powyżej (dzięki temu, że $w(\mathbb{H}, s) = 0$) pokazujemy, że $u^e - v \in \overline{L}_{c(s)e_s - c(s)-1} = \overline{L}_{en-n-1}$. Spełnione są więc znowu wszystkie założenia Lematu 9.6. Zatem $h_{c(s)} = u \in A_n \subseteq k[f, g]$ $\boxtimes$

10 Istnienie β-systemu

Teraz możemy już udowodnić zapowiedziane wcześniej twierdzenie o istnieniu β-systemu.

Dowód Twierdzenia 3.4. Niech $\mathbb{H} = (h_1, \ldots, h_{N-1})$ będzie α-systemem takim, jak w Stwierdzeniu 9.7. Niech

$$\mathbb{H}' = \{h_{c(1)}^{j_1} \cdots h_{c(p)}^{j_p};\ 0 \leqslant j_s < e_s \ \text{ dla } s = 1, \ldots, p\},$$

$$\mathbb{J} = \{j_1 c(1) + \cdots + j_p c(p);\ 0 \leqslant j_s < e_s \ \text{ dla } s = 1, \ldots, p\}.$$

Ponieważ $h_{c(1)}, \ldots, h_{c(p)} \in k[f, g]$, więc $\mathbb{H}' \subset k[f, g]$. Każdy element postaci $h_{c(1)}^{j_1} \cdots h_{c(p)}^{j_p}$ należy oczywiście do zbioru $A_{j_1 c(1) + \cdots + j_p c(p)}$. Pokażemy, że elementy zbioru $\mathbb{H}'$ można ustawić w różnowyrazowy ciąg $(h'_0 = 1, h'_1, \ldots, h'_{N-1})$, który będzie β-systemem. W tym celu wystarczy udowodnić następujące cztery własności:

(1) Każdy element zbioru $\mathbb{J}$ jest mniejszy od N.

(2) Elementy zbioru $\mathbb{J}$ są parami różne.

(3) Moc zbioru $\mathbb{J}$ jest równa N.

(4) Stopnie wielomianów należących do $\mathbb{H}'$ są parami nieprzystające modulo $\deg g$.

Dowód (1). Wiemy (patrz Stwierdzenie 7.3), że $e_s c(s) = c(s+1)$, dla $s = 1, \ldots, p$. Wiemy także, że $c(p+1) = N$. Mamy zatem:

$$\begin{aligned} j_1 c(1) + \cdots + j_p c(p) &< e_1 c(1) + j_2 c(2) + \cdots + j_p c(p) \\ &= c(2) + j_2 c(2) + \cdots + j_p c(p) \\ &\leqslant e_2 c(2) + j_3 c(3) + \cdots + j_p c(p) \\ &= c(3) + j_3 c(3) + \cdots + j_p c(p) \\ &\vdots \\ &\leqslant e_p c(p) = c(p+1) = N. \end{aligned}$$

Dowód (2). Niech

$$j_1 c(1) + \cdots + j_p c(p) = i_1 c(1) + \cdots + i_p c(p), \tag{10.1}$$

gdzie $i_1, j_1 < e_1, \ldots, i_p, j_p < e_p$. Ponieważ $c(1) = 1$, $c(2) = e_1$, $c(3) = e_1 e_2$, $\ldots$, $c(p) = e_1 \cdots e_{p-1}$ (patrz Wniosek 7.7), więc z równości (10.1) wynika, że liczba $|i_1 - j_1|$ jest podzielna przez e_1, a zatem $i_1 = j_1$ (ponieważ $i_1, j_1 < e_1$). Mamy teraz nową równość $j_2 c(2) + \cdots + j_p c(p) = i_2 c(2) + \cdots + i_p c(p)$, z której wynika (po podzieleniu obu stron przez e_1), że liczba $|i_2 - j_2|$ jest podzielna przez e_2, czyli $i_2 = j_2$. Powtarzając to postępowanie stwierdzmy, że $i_s = j_s$ dla wszystkich $s = 1, \ldots, p$.

Dowód (3). Z (2) wynika, że zbiór $\mathbb{J}$ ma dokładnie $e_1 \cdots e_p = N$ liczb.

Dowód (4). Niech

$$a = h_{c(1)}^{i_1} \cdots h_{c(p)}^{i_p}, \quad b = h_{c(1)}^{j_1} \cdots h_{c(p)}^{j_p},$$

gdzie $0 \leqslant i_s, j_s < e_e$ dla $s = 1, \ldots, p$ i załóżmy, że $\deg a \equiv \deg b \pmod{\deg g}$. Wtedy

$$(i_1 d_{c(1)} + \cdots + i_p d_{c(p)}) - (j_1 d_{c(1)} + \cdots + j_p d_{c(p)}) \in (d_0),$$

a zatem $|i_p - j_p| d_{c(p)} \in D_{p-1}$ i z własności minimalności liczby e_p otrzymujemy równość $i_p = j_p$. W podobny sposób stwierdzamy następnie, że $i_{p-1} = j_{p-1}$. Powtarzając to postępowanie widzimy, że $a = b$. To kończy dowód własności (4) oraz dowód Twierdzenia 3.4. $\boxtimes$

11 Dowód Lematu 9.6

Pozostał nam do udowodnienia Lemat 9.6. Zrobimy to w tym rozdziale. W tym celu udowodnimy najpierw następujące stwierdzenie.

Stwierdzenie 11.1. *Niech $R \subset P$ będą pierścieniami przemiennymi zawierającymi ciało $\mathbb{Q}$ liczb wymiernych. Niech $F \in P[x]$ będzie wielomianem monicznym stopnia $n \geqslant 1$ i niech $e \geqslant 1$ będzie liczbą naturalną. Rozpatrzmy wielomian*

$$F^e = x^{ne} + b_{ne-1}x^{ne-1} + b_{ne-2}x^{ne-2} + \cdots + b_0.$$

Jeżeli $b_{ne-1}, b_{ne-2}, \ldots, b_{ne-n} \in R$, to $F \in R[x]$.

Dowód tego stwierdzenia poprzedzimy pewnymi lematami. Niech n, e będą dodatnimi liczbami całkowitymi i niech

$$\mathbb{L}(n,e) = \{(i_n, \ldots, i_0) \in \mathbb{Z}^{n+1};\ i_n + \cdots + i_0 = e,\ i_s \geqslant 0 \ \text{ dla } \ s = 0, \ldots, n\}.$$

Na zbiorze $\mathbb{L}(n,e)$ określamy relację $\leqslant$, częściowego porządku, w następujący sposób:

$$(i_n, \ldots, i_0) \leqslant (j_n, \ldots, j_0) \Longleftrightarrow \begin{cases} i_n & \leqslant & j_n \\ i_{n-1} + i_n & \leqslant & j_n + j_{n-1} \\ & \vdots & \\ i_0 + \cdots + i_{n-1} + i_n & \leqslant & j_n + j_{n-1} + \cdots + j_0. \end{cases}$$

Niech $\varphi : \mathbb{L}(n,e) \longrightarrow \mathbb{N} \cup \{0\}$ będzie funkcją zdefiniowaną wzorem

$$\varphi(i_n, \ldots, i_0) = ni_n + (n-1)i_{n-1} + \cdots + 1i_1 + 0i_0.$$

Wówczas zachodzi następujący oczywisty lemat.

Lemat 11.2. *Niech $i, j \in \mathbb{L}(n, e)$. Wtedy:*
(1) *$i \leqslant j \Rightarrow \varphi(i) \leqslant \varphi(j)$;*
(2) *$i < j \Rightarrow \varphi(i) < \varphi(j)$;*
(3) *Jeżeli $i \neq j$ oraz $\varphi(i) = \varphi(j)$, to elementy i, j nie są porównywalne względem $\leqslant$.* ⊠

W zbiorze $\mathbb{L}(n, e)$ wyróżniamy elementy $\pi_{n-1}, \ldots, \pi_0$, gdzie

$$\begin{aligned}
\pi_{n-1} &= (e-1, 1, 0, 0, \ldots, 0, 0),\\
\pi_{n-2} &= (e-1, 0, 1, 0, \ldots, 0, 0),\\
&\vdots\\
\pi_1 &= (e-1, 0, 0, 0, \ldots, 1, 0),\\
\pi_0 &= (e-1, 0, 0, 0, \ldots, 0, 1).
\end{aligned}$$

Poniższy lemat też jest łatwy do udowodnienia.

Lemat 11.3. *Niech $i = (i_n, \ldots, i_0) \in \mathbb{L}(n, e)$ i niech $s \in \{0, 1, \ldots, n\}$. Wtedy:*
(1) *jeżeli $i_s > 1$, to $\varphi(\pi_s) > \varphi(i)$;*
(2) *jeżeli $i_r > 0$ dla pewnego $r < s$, to $\varphi(\pi_s) > \varphi(i)$.* ⊠

Dowód Stwierdzenia 11.1. Niech $F = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, gdzie $a_{n-1}, \ldots, a_0$ są elementami należącymi do P. Mamy wówczas:

$$F^e = \sum_{i_n + \cdots + i_0 = e} \langle i_n, \ldots, i_0 \rangle a_{n-1}^{i_{n-1}} \cdots a_0^{i_0} x^{\varphi(i_n, \ldots, i_0)}, \tag{11.1}$$

gdzie $\langle i, \ldots, i_0 \rangle = e!(i_n! \cdots i_0!)^{-1}$. Musimy pokazać, że elementy $a_{n-1}, \ldots, a_0$ należą do pierścienia R. Zastosujemy indukcję matematyczną.

Pokażemy najpierw, że $a_{n-1} \in R$. W tym celu zbadajmy w (11.1) współczynnik stojący przy x^{ne-1}. Ponieważ $ne - 1 = \varphi(\pi_{n-1})$, więc mamy we wzorze (11.1) składnik

$$\langle e-1, 1, 0, \ldots, 0 \rangle a_{n-1}^1 x^{ne-1}.$$

Niech $i = (i_n, \ldots, i_0)$ będzie takim elementem zbioru $\mathbb{L}(n, e)$, że $\varphi(i) = ne - 1 = \varphi(\pi_{n-1})$. Jeżeli $i_{n-1} > 1$, to $\varphi(i) < \varphi(\pi_{n-1})$ (patrz Lemat 11.3). Mogą więc tylko zachodzić dwa przypadki: $i_{n-1} = 1$ lub $i_{n-1} = 0$.

Załóżmy, że $i_{n-1} = 1$. Wtedy $i_n = e - 1$. Istotnie, gdyby bowiem zachodziła nierówność $i_n < e - 1$, to $i_r > 0$ dla pewnego $r < n - 1$ i wtedy (na mocy Lematu 11.3) otzymujemy sprzeczność $\varphi(\pi_{n-1}) = \varphi(i) < \varphi(\pi_{n-1})$. Zatem w tym przypadku $i = \pi_{n-1}$.

Załóżmy więc, że $i_{n-1} = 0$. Jeżeli $i_n = e$, to $i = (e, 0, \ldots, 0)$ i wtedy $\varphi(i) = ne > ne - 1$. Jeżeli $i_n < e$, to $i_r > 0$ dla pewnego $r < n - 1$ i stąd (znowu na mocy Lematu 11.3) mamy $\varphi(i) < \varphi(\pi_{n-1})$.

Wykazaliśmy zatem, że jeżeli $\varphi(i) = ne - 1$, to $i = \pi_{n-1}$. To implikuje, że

$$a_{n-1} = e^{-1} e a_{n-1} = e^{-1} \langle e-1, 1, 0, \ldots, 0 \rangle a_{n-1}^1 = e^{-1} b_{en-1} \in R.$$

Załóżmy teraz, że $a_{n-1}, \ldots, a_{n-s+1} \in R$, dla pewnego $s \in \{2, 3, \ldots, n\}$. Pokażemy, że wtedy $a_{n-s} \in R$. W tym celu zbadajmy w (11.1) współczynnik stojący przy x^{ne-s}. Ponieważ $ne - s = \varphi(\pi_{n-s})$, więc mamy we wzorze (11.1) składnik

$$\langle e-1, 0, \ldots, 0, 1, 0, \ldots, 0\rangle a_{n-s}^1 x^{ne-s}.$$

Jednomian x^{ne-s} może występować w (11.1) jeszcze kilka razy. Niech $i = (i_n, \ldots, i_0)$ będzie takim elementem zbioru $\mathbb{L}(n, e)$, że $\varphi(i) = ne - s = \varphi(\pi_{n-s})$. Widzimy, na mocy Lematu 11.3, że wtedy $i_{n-s-1} = \cdots = i_0 = 0$. Ponadto, $i_{n-s} = 0$ lub $i_{n-s} = 1$.

Załóżmy, że $i_{n-s} = 1$. Jeżeli $i_n = e - 1$, to $i = \pi_{n-s}$. Niech więc $i_n < e - 1$. Mamy wtedy:

$$\begin{aligned}
\varphi(i) &= ni_n + (n-1)i_{n-1} + \cdots + (n-s+1)i_{n-s+1} + (n-s) \\
&\leqslant ni_n + (n-1)(i_{n-1} + \cdots + i_{n-s+1}) + n - s \\
&= (n-1)(i_n + i_{n-1} + \cdots + i_{n-s+1}) + i_n + n - s \\
&= (n-1)(e-1) + i_n + n - s \\
&< (n-1)(e-1) + (e-1) + n - s \\
&= ne - s = \varphi(\pi_{n-s}).
\end{aligned}$$

Zatem, jeżeli $i_{n-s} = 1$, to $i = \pi_{n-s}$.

Niech teraz $i_{n-s} = 0$. Wtedy przed x^{ne-s} stoi współczynnik będący iloczynem elementów $a_{n-1}, \ldots, a_{n-s+1}$ podniesionych do pewnych potęg i pomnożonych przez liczbę całkowitą. Widzimy więc, . ze wtedy

$$b_{ne-s} = \langle e-1, 0, \ldots, 0, 1, 0, \ldots, 0\rangle a_{n-s} + \gamma(a_{n-1}, \ldots, a_{n-s+1}),$$

gdzie γ jest pewnym wielomianem o całkowitych współczynnikach. Stąd (na mocy założenia indukcyjnego) wynika, że $a_{n-s} \in R$ i to kończy dowód Stwierdzenia 11.1. ⊠

Dowód Lematu 9.6. Niech $R = k[g]$ i $P = k(g)$. Wtedy $R \subset P$ są pierścieniami przemiennymi zawierającymi $\mathbb{Q}$. Z założenia wynika, że

$$\begin{aligned}
u &= F(f), \text{ gdzie } F = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad \in k(g)[x] = P[X], \\
v &= H(f), \text{ gdzie } H = x^{ne} + b_{ne-1}x^{ne-1} + \cdots + b_0 \in k[g][x] = R[x].
\end{aligned}$$

Wtedy $u^e - v = (F^e - H)(f)$, gdzie

$$F^e - H = c_{ne-1}x^{ne-1} + \cdots + c_0 \in k(g)[x] = P[x].$$

Ponieważ $ne - 1 < ne \leqslant N$ oraz $(k(g)(f) : k(g)) = N$, więc z tego, że $(F^e - H)(f) \in \overline{L}_{en-n-1}$ wynika, że współczynniki $c_{en-1}, c_{en-2}, \ldots, c_{en-n}$ są równe zero. To oznacza, że wielomian F^e ma współczynniki przy $x^{ne-1}, \ldots, x^{ne-n}$ takie, jak wielomian H, a więc współczynniki należące do $R = k[g]$. Stąd (na mocy Stwierdzenia 11.1) $F \in k[g][x]$, a więc $u = F(f) \in k[g][f] = k[f, g]$. Zatem $u \in \overline{A}_n \cap k[f, g] = A_n$. To kończy dowód naszego lematu. ⊠

References

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

[2] S. Abhyankar, T. T. Moh, *Newton–Puiseux expansion and generalized Tchirnhausen transformation*, II, J. reine angew. Math., **261**(1973), 29–54.

[3] S. Abhyankar, T. T. Moh, *Embeddings of the line in the plane*, J. reine angew. Math., **276**(1975), 148 – 166.

[4] H. Bass, E. H. Connell, D. Wright, *The jacobian conjecture: Reduction of degree and formal expansion of the inverse* Bull. Amer. Math. Soc., **7**(1982), 287 – 330.

[5] R. Ganong, *On plane curves with one place at infinity*, J. Reine Angew. Math. **307/308**(1979), 173 – 193.

[6] M. Kang, *On Abhyankar-Moh's epimorphism theorem*, Amer. J. Math., **113** (1991), 399–421.

[7] M. Miyanishi, *Analytic irreducibility of certain curves on a nonsingular affine rational surface*, Proceedings of the International Symposium on Algebraic Geometry, Kyoto 1977, Kinokuniya, Tokyo, 1978, 575–587.

[8] M. Miyanishi, *Curves on rational and unirational surfaces,* Lect.Notes **60**, Tata Institute, Bombay, 1978.

[9] A. Płoski, *Pierwiastki aproksymatywne wielomianów według S.S. Abhyankara i T.T. Moha*, XIV Konferencja Szkoleniowa z Teorii Zagadnień Ekstremalnych, Materiały, Uniwersytet Łódzki, 1993, 45–52.

[10] A. Płoski, *Twierdzenia podstawowe o pierwiastkach aproksymatywnych wielomianów*, XV Konferencja Szkoleniowa z Analizy i Geometrii Zespolonej, Uniwersytet Łódzki, 1994, 51–61.

[11] D. R. Richman, *On the computation of minimal polynomials*, J. Algebra, **103**(1986), 1–17.

[12] L. Rudolph, *Embeddings of the line in the plane*, J. reine angew. Math., **337**(1982), 113–118.

[13] B. Segre, *Corrispondenze di Mobius e transformazioni Cremoniane intere*, Atti della Academia selle Scienze di Torino, Classe di Scienzo Fisiche, Mat. e Natural, **91**(1956-57), 3–19.

Richman's proof of the Abhyankar-Moh theorem

Summary. Let $k[t]$ be the polynomial ring in t over a field k of characteristic zero. Let $f, g \in k[t] \setminus k$ and assume that $k[f, g] = k[t]$. Then $\deg f \mid \deg g$ or $\deg g \mid \deg f$. In the paper a proof (after D. R. Richman 1986) of this fact is given.

Bronisławów, 9–13 stycznia, 1995 r.