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

1999 **Łódź** **str. 21**

O WIELOŚCIANACH NEWTONA AUTOMORFIZMÓW PIERŚCIENIA WIELOMIANÓW TRZECH ZMIENNYCH

Ilona Nowosad (Toruń)

Niech k będzie ciałem charakterystyki zero.

Jeśli σ jest automorfimem pierścienia $k[x, y]$, wielomianów dwóch zmiennych nad k, to dobrze wiadomo (patrz na przykład [1]), że wielokąty Newtona wielomianów $\sigma(x)$ i $\sigma(y)$ są albo odcinkami albo trójkątami. W jednym i drugim przypadku wszystkie wierzchołki leżą na osiach układu współrzędnych. Każdy wierzchołek ma więc co najmniej jedną zerową współrzędną.

W roku 1991 Ofer Hadas [2] udowodnił, że taką samą własność posiadają wszystkie wierzchołki wielościanów Newtona automorfizmów pierścieni wielomianów dowolnej skończonej liczby zmiennych. Celem niniejszego artykułu jest przedstawienie dokładnego dowodu wyniku Hadasa w przypadku trzech zmiennych. Podamy zatem dowód następującego twierdzenia.

Twierdzenie 1 ([2]). *Jeśli σ jest automorfizmem pierścienia wielomianów $k[x_1, x_2, x_3]$, to każdy wierzchołek wielościanów Newtona wielomianów $\sigma(x_1)$, $\sigma(x_2)$, $\sigma(x_3)$, ma co najmniej jedną zerową współrzędną.*

Istotną rolę w dowodzie tego twierdzenia odgrywać będą pewne specjalne własności derywacji lokalnie nilpotentnych.

1. Definicje, oznaczenia i proste fakty. Pierścień wielomianów $k[x_1, x_2, x_3]$ oznaczać będziemy przez $k[X]$. Przez Ω oznaczać będziemy zbiór wszystkich trójek nieujemnych liczb całkowitych. Jeśli $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ należy do zbioru Ω, to przez X^α oznaczamy jednomian $x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$.

Załóżmy, że $f \in k[X]$. Wówczas f ma jednoznaczne przedstawienie w postaci

$$f = \textstyle\sum_{\alpha \in \Omega} f_\alpha X^\alpha,$$

gdzie elementy f_α należą do ciała k i przy tym prawie wszystkie są równe zero. Zbiór tych wszystkich elementów $\alpha \in \Omega$, dla których $f_\alpha \neq 0$, oznaczamy przez S_f i nazywamy *nośnikiem wielomianu* f. *Wielościanem Newtona* wielomianu f, oznaczanym przez $N(f)$, nazywamy najmniejszy zbiór wypukły w $\mathbb{R}^3$ zawierający zbiór $S_f \cup \{(0,0,0)\}$.

Przypomnijmy, że *derywacją* pierścienia $k[X]$ nazywamy każde k-liniowe odwzorowanie $d : k[X] \to k[X]$ takie, że

$$d(uv) = d(u)v + ud(v), \quad \text{dla } \ u, v \in k[X].$$

Niech d będzie derywacją pierścienia $k[X]$. Wówczas przez $\operatorname{Nil}(d)$ oznaczamy zbiór

$$\{f \in k[X];\ \exists_{n \in \mathbb{N}}\ d^n(f) = 0\}.$$

Łatwo sprawdzić, że zbiór ten jest podpierścieniem pierścienia $k[X]$ zawierającym ciało k. Mówimy, że derywacja d jest *lokalnie nilpotentna* jeśli $\operatorname{Nil}(d) = k[X]$. Wykorzystamy kilka następujących znanych własności derywacji lokalnie nilpotentnych.

Stwierdzenie 2.

(1) *Derywacja d jest lokalnie nilpotentna wtedy i tylko wtedy, gdy zmienne x_1, x_2 i x_3 należą do* $\operatorname{Nil}(d)$.

(2) *Niech $f, g \in k[X]$. Jeśli derywacja d jest lokalnie nilpotentna i $d(f) = fg$, to $d(f) = 0$.*

(3) *Niech $0 \neq f \in k[X]$. Jeśli d jest derywacją pierścienia $k[X]$, to odwzorowanie $fd : k[X] \to k[X]$, określone wzorem $fd(u) = f \cdot d(u)$ (dla $u \in k[X]$), jest również derywacją. Derywacja fd jest lokalnie nilpotentna wtedy i tylko wtedy, gdy derywacja d jest lokalnie nilpotentna i $d(f) = 0$.*

(4) *Jeśli $\sigma : k[X] \to k[X]$ jest automorfizmem i $d : k[X] \to k[X]$ jest derywacją, to odwzorowanie $D = \sigma d \sigma^{-1}$ jest derywacją. Derywacja D jest lokalnie nilpotentna wtedy i tylko wtedy, gdy derywacja d jest lokalnie nilpotentna.*

Dowody znajdziemy na przykład w [3]. ⊠

Załóżmy teraz, że $p = (p_1, p_2, p_3)$ jest ustalonym niezerowym punktem w $\mathbb{R}^3$.

Niech $s \in \mathbb{R}$. Mówimy, że niezerowy wielomian $f = \sum_{\alpha \in \Omega} f_\alpha X^\alpha \in k[X]$ jest *p-formą stopnia s* jeśli każdy punkt $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ należący do nośnika S_f spełnia warunek $\alpha p = s$, gdzie przez αp oznaczamy liczbę $\alpha_1 p_1 + \alpha_2 p_2 + \alpha_3 p_3$. Zakładamy dodatkowo, że wielomian zerowy jest również p-formą stopnia s. Zbiór wszystkich p-form stopnia s oznaczamy przez $A_p^{(s)}$. Zbiór ten jest k-podprzestrzenią liniową przestrzeni $k[X]$.

Łatwo sprawdzić, że jeśli $s, t \in \mathbb{R}$, to $A_p^{(s)} \cdot A_p^{(t)} \subseteq A_p^{(s+t)}$. Ponadto

$$k[X] = \bigoplus_{s\in\mathbb{R}} A_p^{(s)},$$

(suma prosta k-podprzestrzeni liniowych). Z każdym więc punktem $p \in \mathbb{R}^3$ stowarzyszona jest gradacja pierścienia $k[X]$ określona w powyższy sposób. Gradację taką nazywać będziemy *p-gradacją*. Dowolny wielomian $f \in k[X]$ ma jednoznaczne *p-przedstawienie*

$$f = \sum_{s\in\mathbb{R}} f^{(s)},$$

gdzie każde $f^{(s)}$ jest p-formą stopnia s zwaną *p-składową jednorodną stopnia s* wielomianu f. Jeśli $f \neq 0$, to $\deg_p(f)$ oznacza *p-stopień* wielomianu f, tzn. największą liczbę rzeczywistą s taką, że $f^{(s)} \neq 0$. Jeśli $f \neq 0$, to niezerową p-składową najwyższego stopnia wielomianu f oznaczać będziemy przez f^*. Umawiamy się ponadto, że $0^* = 0$.

Niech $\tau \in \mathbb{R}$ i niech $d : k[X] \to k[X]$ będzie derywacją. Mówimy, że derywacja ta jest *p-jednorodna stopnia τ*, jeśli

$$d\left(A_p^{(s)}\right) \subseteq A_p^{(s+\tau)}, \qquad \text{dla każdego } s \in \mathbb{R}.$$

Stwierdzenie 3. *Derywacja $d : k[X] \to k[X]$ jest p-jednorodna stopnia τ wtedy i tylko wtedy, gdy $d(x_i) \in A_p^{(p_i+\tau)}$ dla $i = 1, 2, 3$.*

Dowód jest prostym sprawdzeniem. Patrz [3] strona 21. ⊠

Dobrze wiadomo, że każda derywacja pierścienia $k[X]$ jest jednoznacznie wyznaczona przez swoje wartości na zmiennych x_1, x_2 i x_3. Załóżmy zatem, że

$$d(x_1) = f_1, \quad d(x_2) = f_2, \quad d(x_3) = f_3,$$

gdzie $f_1, f_2, f_3 \in k[X]$. Jeśli $\tau \in \mathbb{R}$, to przez d_τ oznaczać będziemy derywację pierścienia $k[X]$ zdefiniowaną równościami:

$$d_\tau(x_1) = f_1^{(p_1+\tau)}, \quad d_\tau(x_2) = f_2^{(p_2+\tau)}, \quad d_\tau(x_3) = f_3^{(p_3+\tau)}.$$

Ze stwierdzenia 3 wynika, że d_τ jest derywacją p-jednorodną stopnia τ. Jest oczywiste, że

$$d = \sum_{\tau\in\mathbb{R}} d_\tau,$$

przy czym $d_\tau = 0$ dla prawie wszystkich τ. Każda zatem niezerowa derywacja pierścienia $k[X]$ jest skończoną sumą niezerowych derywacji p-jednorodnych postaci d_τ. Jeśli τ jest największą liczbą rzeczywistą taką, że $d_\tau \neq 0$, to derywację d_τ nazywać będziemy *główną p-składową* derywacji d. Łatwo udowodnić następujące

Stwierdzenie 4. *Główna p-składowa derywacji lokalnie nilpotentnej jest derywacją lokalnie nilpotentną.* ⊠

3. Kilka faktów o derywacji jakobianowej.

Jeśli w_1, w_2, w_3 są wielomianami należącymi do pierścienia $k[X] = k[x_1, x_2, x_3]$, to przez $J(w_1, w_2, w_3)$ oznaczamy jakobian tych wielomianów, tzn. wyznacznik macierzy $[\partial w_i / \partial x_j]$.

Załóżmy, że wielomiany $w_1, w_2 \in k[X]$ są ustalone i rozpatrzmy odwzorowanie $d_{w_1,w_2} : k[X] \to k[X]$ określone wzorem

$$d_{w_1,w_2}(f) = J(w_1, w_2, f),$$

dla wszystkich $f \in k[X]$. Odwzorowanie to jest derywacją. Jest to tzw. *derywacja jakobianowa.* Derywacje jakobianowe odgrywać będą ważną rolę w dowodzie twierdzenia 1.

Stwierdzenie 5. *Jeśli $w_1 \in k[x_1]$ oraz $w_2 \in k[x_1, x_2]$, to derywacja jakobianowa d_{w_1,w_2} jest lokalnie nilpotentna.*

Dowód. Jeśli $w_1 \in k[x_1]$ oraz $w_2 \in k[x_1, x_2]$, to derywacja d_{w_1,w_2} ma postać $f \cdot d$, gdzie $d = \partial/\partial x_3$ oraz $f = (\partial w_1/\partial x_1)(\partial w_2/\partial x_2)$. Derywacja d jest oczywiście lokalnie nilpotentna oraz $d(f) = 0$ (gdyż $f \in k[x_1, x_2]$). Teza wynika zatem ze stwierdzenia 2(3). ⊠

Stwierdzenie 6. *Niech $w_1, w_2 \in k[X]$ i niech $\sigma : k[X] \to k[X]$ będzie automorfizmem. Jeśli derywacja d_{w_1,w_2} jest lokalnie nilpotentna, to derywacja $d_{\sigma(w_1),\sigma(w_2)}$ również jest lokalnie nilpotentna.*

Dowód. Zauważmy, że

$$d_{\sigma(w_1),\sigma(w_2)} = J(\sigma) \cdot \sigma \cdot d_{w_1,w_2} \cdot \sigma^{-1},$$

gdzie $J(\sigma)$ jest jakobianem wielomianów $\sigma(x_1), \sigma(x_2), \sigma(x_3)$. Niech $\Delta = \sigma d_{w_1,w_2} \sigma^{-1}$. Derywacja Δ jest (na mocy stwierdzenia 2(4)) lokalnie nilpotentna. Ponieważ σ jest automorfizmem, więc $J(\sigma)$ jest elementem ciała k i stąd $\Delta(J(\sigma)) = 0$. Zatem ze stwierdzenia 2(3) wynika, że derywacja $d_{\sigma(w_1),\sigma(w_2)} = J(\sigma)\Delta$ jest lokalnie nilpotentna. ⊠

Niech teraz $p = (p_1, p_2, p_3)$ będzie ustalonym punktem w $\mathbb{R}^3$. Rozważmy p-gradację na $k[X]$, opisaną w poprzednim rozdziale.

Pochodna cząstkowa $\frac{\partial}{\partial x_i}$ jest p-jednorodną derywacją stopnia $-p_i$ (wynika to na przykład ze stwierdzenia 3). Stąd wynika, że jeśli w_1, w_2, $w_3 \in k[X]$ są p-formami stopni odpowiednio s_1, s_2 i s_3, to jakobian $J(w_1, w_2, w_3)$ jest p-formą stopnia $s_1 + s_2 + s_3 - p_1 - p_2 - p_3$. Korzystając z tego faktu nie jest trudno wykazać następujące dwa stwierdzenia.

Stwierdzenie 7. *Niech $w_1, w_2 \in k[X]$. Jeśli w_1 jest p-formą stopnia s_1 oraz w_2 jest p-formą stopnia s_2, to derywacja d_{w_1,w_2} jest p-jednorodna stopnia $s_1 + s_2 - p_1 - p_2 - p_3$.* ⊠

Stwierdzenie 8. *Niech* $w_1, w_2 \in k[X]$. *Oznaczmy przez* D *derywację* d_{w_1,w_2} *i niech*

$$\tau = \deg_p(w_1) + \deg_p(w_2) - p_1 - p_2 - p_3.$$

Rozpatrzmy derywację D_τ *zdefiniowaną w rozdziale* 2. *Mamy wówczas:*

(1) $D_\tau = d_{w_1^*, w_2^*}$*;*

(2) *jeśli* $D_\tau \neq 0$*, to derywacja* D_τ *jest główną* p*-składową derywacji* D. $\boxtimes$

Z powyższych stwierdzeń wynika:

Stwierdzenie 9. *Niech* $\sigma : k[X] \to k[X]$ *będzie automorfizmem. Niech* $w_1 \in k[x_1]$, $w_2 \in k[x_1, x_2]$. *Oznaczmy przez* D *derywację* $d_{\sigma(w_1),\sigma(w_2)}$ *i niech*

$$\tau = \deg_p \sigma(w_1) + \deg_p \sigma(w_2) - p_1 - p_2 - p_3.$$

Wówczas derywacja D_τ *jest lokalnie nilpotentna. Ponadto,* $D_\tau = d_{\sigma(w_1)^*, \sigma(w_2)^*}$. $\boxtimes$

4. Jakobianowe derywacje dla jednomianów.

Jeśli $\alpha_1, \alpha_1, \alpha_3 \in \Omega$, to dobrze wiadomo, że

$$J(X^{\alpha_1}, X^{\alpha_2}, X^{\alpha_3}) = \det(\alpha_1, \alpha_2, \alpha_3) X^{\alpha_1 + \alpha_2 + \alpha_3 - 1},$$

gdzie $1 = (1, 1, 1) \in \Omega$. Z faktu tego otrzymujemy:

Stwierdzenie 10. *Niech* $D = d_{X^{\alpha_1}, X^{\alpha_2}}$*, gdzie* $\alpha_1, \alpha_2 \in \Omega$. *Wówczas dla* $\beta \in \Omega$ *oraz* $m \in \mathbb{N}$ *zachodzi równość*

$$D^m \left(X^\beta\right) = \left(\prod_{l=0}^{m-1} \det(\alpha_1, \alpha_2, \beta + l\gamma)\right) X^{\beta + m\gamma},$$

gdzie $\gamma = \alpha_1 + \alpha_2 - (1, 1, 1)$. $\boxtimes$

Jeśli B jest podzbiorem w $\mathbb{R}^3$, to przez $L(B)$ oznaczamy $\mathbb{R}$-podprzestrzeń przestrzeni R^3 generowaną przez B. Przez e_1, e_2 i e_3 oznaczamy odpowiednio wektory $(1, 0, 0)$, $(0, 1, 0)$ i $(0, 0, 1)$.

Stwierdzenie 11 ([2]). *Niech* $D = d_{X^{\alpha_1}, X^{\alpha_2}}$*, gdzie* $\alpha_1, \alpha_2 \in \Omega$. *Załóżmy, że ciągi* α_1, α_2 *są liniowo niezależne nad* $\mathbb{Q}$. *Jeśli derywacja* D *jest lokalnie nilpotentna, to przestrzeń* $L(\alpha_1, \alpha_2)$ *jest jedną z płaszczyzn osiowych, tzn. istnieje* $i \in \{1, 2, 3\}$ *takie, że*

$$L(\alpha_1, \alpha_2) = L\left(\{e_1, e_2, e_3\} \setminus \{e_i\}\right).$$

Dowód. Istnieje liczba naturalna m taka, że $D^m(x_i) = 0$ dla wszystkich $i = 1, 2, 3$. Dla każdego zatem $i \in \{1, 2, 3\}$ istnieje (na mocy stwierdzenia 10) nieujemna liczba całkowita l_i taka, że

$$0 = \det\left(\alpha_1, \alpha_2, e_i + l_i\gamma\right) = \det\left(\alpha_1, \alpha_2, e_i - l_i 1\right).$$

Stąd oraz z założenia o liniowej niezależności wynika, że

$$(1) \qquad e_i - l_i 1 \in L(\alpha_1, \alpha_2), \quad \text{dla} \;\; i = 1, 2, 3.$$

Wykażemy teraz, że $\det(\alpha_1, \alpha_2, 1) \neq 0$. W tym celu rozpatrzmy $t \in \{1, 2, 3\}$ spełniające warunek $e_t \notin L(\alpha_1, \alpha_2)$. Takie t oczywiście istnieje. Wówczas

$$\det(\alpha_1, \alpha_2, e_t) \neq 0,$$

$$0 = \det(\alpha_1, \alpha_2, e_t - l_t 1) = \det(\alpha_1, \alpha_2, e_t) - l_t \det(\alpha_1, \alpha_2, 1).$$

Skoro więc $\det(\alpha_1, \alpha_2, e_t) \neq 0$, to musi być $\det(\alpha_1, \alpha_2, 1) \neq 0$.

Spójrzmy teraz na następujący ciąg równości.

$$\begin{aligned} 0 &= \textstyle\sum_{i=1}^{3} \det(\alpha_1, \alpha_2, e_i - l_i 1) \\ &= \det(\alpha_1, \alpha_2, \textstyle\sum_{i=1}^{3} e_i) - \det(\alpha_1, \alpha_2, 1)(\textstyle\sum_{i=1}^{3} l_i) \\ &= \det(\alpha_1, \alpha_2, 1)(1 - \textstyle\sum_{i=1}^{3} l_i). \end{aligned}$$

Z równości tych wynika, że

$$l_1 + l_2 + l_3 = 1.$$

Liczby l_1, l_2, l_3 są całkowite i nieujemne. Istnieje zatem $i \in \{1, 2, 3\}$ takie, że $l_i = 1$ oraz $l_j = 0$ dla wszystkich $j \neq i$. Stąd oraz z (1) wynika, że wektory e_i, dla $i \neq j$, należą do przestrzeni $L(\alpha_1, \alpha_2)$. Zatem $L(\alpha_1, \alpha_2) = L(\{e_1, e_2, e_3\} \setminus \{e_i\})$. ⊠

5. Lematy o automorfizmach.

Niech $p = (p_1, p_2, p_3) \in \mathbb{R}^3$. W tym rozdziale zakładać będziemy, że liczby p_1, p_2, p_3 są liniowo niezależne nad $\mathbb{Q}$. Przy takim założeniu każda p-forma jest jednomianem.

Dla danego automorfizmu $\sigma : k[X] \to k[X]$ niech $\gamma_{p,\sigma} : k[X] \setminus \{0\} \to \Omega$ będzie funkcją przyporządkowującą każdemu niezerowemu wilomianowi $f \in k[X]$ jedyny element $\alpha \in \Omega$ taki, że niezerowa p-składowa najwyższego stopnia wielomianu $\sigma(f)$ jest stowarzyszona z jednomianem X^α. Innymi słowy:

$$\gamma_{p,\sigma}(f) = \alpha, \quad \text{jeśli} \;\; \sigma(f)^* = cX^\alpha, \quad \text{dla pewnego} \;\; c \in k \setminus \{0\}.$$

Jeśli s jest nieujemną liczbą całkowitą to przez $\mathbb{W}_s$ oznaczać będziemy zbiór wszystkich wielomianów z pierścienia $k[x_1, x_2]$ stopnia $\leqslant s$. Zbiór $\mathbb{W}_s$ jest przestrzenią liniową nad ciałem k wymiaru $\binom{s+2}{2}$.

Lemat 12. *Niech $p = (p_1, p_2, p_3) \in \mathbb{R}^3$ będzie takim punktem, że liczby p_1, p_2, p_3 są liniowo niezależne nad $\mathbb{Q}$. Niech $\sigma : k[X] \to k[X]$ będzie automorfizmem i niech $\gamma = \gamma_{p,\sigma}$. Wówczas, dla każdej nieujemnej liczby całkowitej s, zbiór $\gamma(\mathbb{W}_s \setminus \{0\})$ jest skończony i posiada dokładnie $\binom{s+2}{2}$ elementów.*

Dowód. Ustalmy nieujemną liczbę całkowitą s i niech

$$A_s = \sigma(\mathbb{W}_s), \quad B_s = \gamma(\mathbb{W}_s \setminus \{0\}).$$

Zbiór A_s jest oczywiście przestrzenią liniową nad k izomorficzną z $\mathbb{W}_s$; jej wymiar jest więc równy $\binom{s+2}{2}$. Wystarczy pokazać, że $|B_s| = \dim_k A_s$, gdzie $|B_s|$ oznacza moc zbioru B_s.

Niech $Q_1, \dots, Q_t \in A_s$ będą wielomianami o niestowarzyszonych najwyższych p-formach, odpowiadających elementom zbioru B_s. Wówczas jednomiany $Q_1^*, \dots, Q_t^*$ są liniowo niezależne nad k i jest oczywiste, że wtedy wielomiany $Q_1, \dots, Q_t \in A_t$ są również liniowo niezależne nad k. Zatem $|B_s| \leqslant \dim_k A_s$. Stąd w szczególności wynika, że zbiór B_s jest skończony.

Załóżmy, że $|B_s| = m$. Niech $B_s = \{v_1, \dots, v_m\}$ i niech $f_1, \dots, f_s \in \mathbb{W}_s \setminus \{0\}$ będą takimi wielomianami, że

$$\sigma(f_1)^* = X^{v_1}, \quad \dots, \quad \sigma(f_m)^* = X^{v_m}.$$

Oznaczmy: $Q_1 = \sigma(f_1), \dots, Q_m = \sigma(f_m)$. Wielomiany $Q_1, \dots, Q_m$ należą do A_s i mają parami niestowarzyszone najwyższe p-formy. Są zatem, jak pokazaliśmy powyżej, liniowo niezależne nad k.

Wykażemy, że wielomiany te generują przestrzeń A_s. Niech $0 \neq Q \in A_s$. Istnieje wówczas $v \in B_s$ takie, że $cX^v = Q^*$, dla pewnego $c \in k \setminus \{0\}$. Wybierzmy spośród $Q_1, \dots, Q_m$ ten wielomian, którego najwyższa forma jest stowarzyszona z X^v, pomnóżmy go przez c i odejmijmy od Q. Otrzymujemy wielomian Q' taki, że $Q' \in A_s$ i $\deg Q' < \deg Q$. Powtarzając tę procedurę obniżamy stopień kolejnych wielomianów, otrzymując ostatecznie zero. Wielomian Q jest więc kombinacją liniową wielomianów $Q_1, \dots, Q_m$. Wielomiany $Q_1, \dots, Q_m$ tworzą więc bazę przestrzeni A_s. Zatem $|B_s| = m = \dim_k A_s = \binom{s+2}{2}$. ⊠

Lemat 13. *Niech $p = (p_1, p_2, p_3) \in \mathbb{R}^3$ będzie takim punktem, że liczby p_1, p_2, p_3 są liniowo niezależne nad $\mathbb{Q}$. Niech $\sigma : k[X] \to k[X]$ będzie automorfizmem i niech $\gamma = \gamma_{p,\sigma}$. Wówczas, dla każdego wielomianu $f \in k[x_1] \setminus \{0\}$ istnieje wielomian $g \in k[x_1, x_2]$ taki, że wektory $\gamma(f)$ i $\gamma(g)$ są $\mathbb{Q}$-niezależne.*

Dowód. Niech $0 \neq f \in k[x_1]$, niech $\alpha = \gamma(f)$ i oznaczmy przez B zbiór $\gamma\left(k[x_1, k_2] \setminus \{0\}\right)$. Zbiór B jest podzbiorem $\mathbb{Z}$-modułu $\mathbb{Z}^3$. Niech M będzie $\mathbb{Z}$-podmodułem w $\mathbb{Z}^3$ generowanym przez B. Ponieważ $\mathbb{Z}^3$ jest modułem noetherowskim, więc $\mathbb{Z}$-moduł M jest skończenie generowany. Istnieje więc skończony podzbiór $\{b_1, \dots, b_r\}$ zbioru B generujący (nad $\mathbb{Z}$) moduł M.

Przypuśćmy, że żądany wielomian $g \in k[x_1, x_2]$ nie istnieje. Wówczas dla każdego $b \in B$ istnieje liczba wymierna t_b taka, że $b = t_b\alpha$. W szczególności takie liczby wymierne istnieją dla generatorów $b_1, \dots, b_r$. Niech m będzie najmniejszą wspólną wielokrotnością mianowników wszystkich liczb wymiernych $t_{b_1}, \dots, t_{b_s}$. Wtedy dla każdego $b \in M$, istnieje liczba całkowita z_b taka, że $b = z_b(1/m)\alpha$. Moduł M jest więc podmodułem cyklicznego modułu $\mathbb{Z}v$, gdzie $v = (1/m)\alpha$.

Załóżmy teraz, że $s \in \mathbb{N}$. Rozważmy zbiór $B_s = \gamma\left(\mathbb{W}_s \setminus \{0\}\right)$, którym zajmowaliśmy się w lemacie 12 i rozważmy nośniki wielomianów $\sigma(x_1)$ i $\sigma(x_2)$. Niech $S = \{0\} \cup S_{\sigma(x_1)} \cup S_{\sigma(x_2)}$.

Istnieje kula $K(0, \rho)$ w $\mathbb{R}^3$ zawierająca zbiór S. Wtedy zbiór B_s zawarty jest w kuli $K(0, s\rho)$, a zatem $B_s \subseteq K(0, s\rho) \cap \mathbb{Z}v$. Jest oczywiste, że w kuli $K(0, s\rho)$

jest co najwyżej $2sm\rho$ punktów należących do $\mathbb{Z}v$. Zatem $|B_s| \leqslant 2sm\rho$. Z drugiej jednak strony wiemy, na mocy lematu 12, że $|B_s| = \binom{s+2}{2}$. Zatem

$$\tfrac{s^2}{2} < \tbinom{s+2}{2} = |B_d| \leqslant 2sm\rho,$$

a stąd $s \leqslant 4m\rho$, co jest sprzeczne z dowolnością $s \in \mathbb{N}$. ⊠

6. Dowód twierdzenia 1. Mamy dany automorfizm $\sigma : k[X] \to k[X]$. Należy wykazać, że każdy wierzchołek wielościanu Newtona $N(\sigma(x_i))$, dla $i = 1, 2, 3$, ma co najmniej jedną zerową współrzędną. Dla ustalenia uwagi przyjmijmy $i = 1$.

Niech $\alpha \neq 0$ będzie wierzchołkiem wielościanu $N(\sigma(x_1))$. Jest oczywiste, że istnieje płaszczyzna w $\mathbb{R}^3$ przechodząca przez wierzchołek α i nie posiadająca innych (oprócz α) punktów wspólnych z $N(\sigma(x_1))$. Niech $p = (p_1, p_2, p_3)$ będzie wektorem kierunkowym tej płaszczyzny. Płaszczyznę można tak dobrać, że liczby p_1, p_2, p_3 są liniowo niezależne nad $\mathbb{Q}$. Wówczas $\deg_p X^\alpha$ jest albo największą albo najmniejszą liczbą w zbiorze wszystkich liczb postaci $\deg_p X^\beta$, gdzie $\beta \in S_{\sigma(x_1)}$. Zamieniając ewentualnie p na $-p$ możemy założyć, że jest liczbą największą. Składowa p-jednorodna wielomianu $\sigma(x_1)$ jest wtedy stowarzyszona z jednomianem X^α, a zatem $\gamma(x_1) = \alpha$, gdzie $\gamma = \gamma_{p,\sigma}$ jest funkcją wprowadzoną w poprzednim rozdziale.

Spełnione są założenia lematu 13. Na mocy tego lematu istnieje wielomian $g \in k[x_1, x_2]$ taki, że wektory $\alpha = \gamma(x_1)$ i $\gamma(g)$ są liniowo niezależne nad $\mathbb{Q}$. Niech $\beta = \gamma(g)$.

Ponieważ $x_1 \in k[x_1]$ i $g \in k[x_1, x_2]$, więc (patrz stwierdzenie 9) derywacja jakobianowa $d_{\sigma(x_1)^*, \sigma(g)^*}$ jest lokalnie nilpotentna. Stąd wynika, że derywacja d_{X^α, X^β} jest również lokalnie nilpotentna. Wektory α i β są liniowo niezależne nad $\mathbb{Q}$. Stwierdzenie 11 implikuje więc, że przestrzeń $L(\alpha, \beta)$ jest płaszczyzną osiową w $\mathbb{R}^3$. Zatem co najmniej jedna współrzędna wierzchołka α jest zerowa. To kończy dowód twierdzenia. ⊠

References

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

[2] O. Hadas, *On the vertices of Newton polytopes associated with an automorphism of the ring of polynomials*, J. Pure Appl. Algebra, **76**(1991) 81-86.

[3] A. Nowicki, *Polynomial derivations and their rings of constants*, UMK, Toruń, 1994.

On the Newton polytopes of polynomial automorphisms in three variables

Summary. We present a proof of the following theorem of Hadas. If σ is an automorphisms of the polynomial ring $k[x_1, x_2, x_3]$ (where k is a field of characteristic zero), then every vertex of the Newton polytopes of $\sigma(x_1)$, $\sigma(x_2)$ and $\sigma(x_3)$ has at least one zero coordinate.

Łódź, 11 – 15 stycznia, 1999 r.