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

2000 **Łódź** **str. 27**

TWIERDZENIE ZAKSA O PODPIERŚCIENIACH DEDEKINDA PIERŚCIENIA WIELOMIANÓW

Janusz Zieliński (Toruń)

Wstęp

Niech k będzie ciałem nieskończonym i niech $k[x_1, \ldots, x_n]$ będzie pierścieniem wielomianów n zmiennych nad k. W niniejszej pracy udowodnimy następujące twierdzenie.

Twierdzenie. *Niech $k \subset R \subset k[x_1, \ldots, x_n]$. Jeśli R jest pierścieniem Dedekinda, to jest pierścieniem wielomianów jednej zmiennej.*

Twierdzenie to po raz pierwszy pojawiło się w pracy Zaksa [7]. Inny jego dowód podał Eakin (patrz [3]). Przypomnijmy ([1], [2]), że pierścieniem Dedekinda nazywamy każdy pierścień bez właściwych dzielników zera, który jest noetherowski, normalny (czyli całkowicie domknięty w swoim ciele ułamków) i jego wymiar Krulla wynosi 1 (czyli niezerowe ideały pierwsze w tym pierścieniu są maksymalne). Odnotujmy, że w dowodzie nie wykorzystujemy nigdzie założenia o noetherowskości. Elementarnymi przykładami pierścieni Dedekinda są dziedziny ideałów głównych (na przykład pierścień liczb całkowitych $\mathbb{Z}$ oraz pierścień wielomianów $k[x]$). W takim przypadku analogiczne twierdzenie znane było wcześniej (patrz [4]). Twierdzenie

Zaksa jest prawdziwe także dla ciał skończonych, jednak wówczas dowód (patrz [7]) jest nieco inny. Przypadek ciał nieskończonych ma liczne zastosowania. Wynika z niego między innymi, że pierścień stałych niezerowego różniczkowania pierścienia wielomianów dwóch zmiennych nad ciałem charakterystyki zero jest izomorficzny z pierścieniem wielomianów jednej zmiennej. Zostało to udowodnione w pracy [6]. Inne twierdzenia, które wynikają z twierdzenia Zaksa, znaleźć można w [5]. Dowód który prezentujemy, oparty jest w znacznej mierze na oryginalnej pracy Zaksa [7]. Całkowicie nowy jest tylko lemat 1.

Lematy pomocnicze

W poniższych dwóch lematach niech k będzie dowolnym ciałem i niech $k[x]$ będzie pierścieniem wielomianów jednej zmiennej nad k. Jeśli R jest pierścieniem bez właściwych dzielników zera, to przez R_0 oznaczamy ciało ułamków pierścienia R.

Lemat 1. *Niech $R \subset k[x]$ będzie podpierścieniem zawierającym ciało k. Jeśli $R_0 = k(w)$ dla pewnego wielomianu $w \in R$, to $R = k[w]$.*

Dowód. Oczywiście $k[w] \subset R$. Wystarczy zatem pokazać inkluzję odwrotną. Załóżmy, że istnieje $f \in R \setminus k[w]$. Przez n oznaczmy stopień wielomianu w. Pokażemy, że w pierścieniu R istnieje wielomian g, który nie należy do $k[w]$, a jego stopień nie jest krotnością liczby n. Jeśli stopień wielomianu f nie jest podzielny przez n, to przyjmujemy $g = f$. Jeśli $\deg f = mn$ dla pewnego naturalnego m, to odejmując od wielomianu f wielomian w^m pomnożony przez odpowiedni współczynnik z ciała k otrzymujemy pewien wielomian $f_1 \in R$ stopnia niższego od mn. Gdyby wielomian f_1 należał do pierścienia $k[w]$, to do pierścienia tego musiałby też należeć wielomian f. Zatem $f_1 \in R \setminus k[w]$. Jeśli $\deg f_1$ nie jest podzielne przez n, to przyjmujemy $g = f_1$. Jeśli $\deg f_1$ jest krotnością liczby n, to analogicznie jak powyżej znajdujemy wielomian f_2. W wyniku tej rekurencyjnej procedury otrzymujemy ciąg (f_r) wielomianów, które nie należą do $k[w]$, o malejących stopniach. Ponieważ każdy wielomian stopnia niższego od 1 należy do $k[w]$ (bowiem $k \subset k[w]$), zatem ta procedura musi się zakończyć na pewnym wielomianie f_s. Wówczas $\deg f_s$ nie jest krotnością liczby n i przyjmujemy $g = f_s$. Ponieważ $R_0 = k(w)$, więc istnieją takie wielomiany F oraz G jednej zmiennej o współczynnikach w ciele k, że zachodzi równość

$$\frac{g}{1} = \frac{F(w)}{G(w)}.$$

Zatem $g \cdot G(w) = F(w)$. Otrzymujemy sprzeczność, bo stopień prawej strony ostatniej równości jest podzielny przez n, a stopień lewej strony nie. □

Lemat 2. *Niech R będzie takim pierścieniem, że $k \subset R \subset k[x]$. Jeśli $R_0 \cap k[x] = R$, to istnieje $u \in R$ takie, że $R = k[u]$.*

Dowód. Jeśli dla każdego $r \in R$ zachodzi nierówność $\deg_x r < 1$, to $R \subset k$, a w konsekwencji $R = k$ i wówczas $R = k[1]$. Załóżmy więc, że w pierścieniu R istnieje wielomian dodatniego stopnia. Niech $u(x) \in R$ będzie wielomianem, który jest najniższego dodatniego stopnia w pierścieniu R. Oczywiście taki wielomian nie jest wyznaczony jednoznacznie, wybieramy jeden z wielomianów o danej własności. Oznaczmy stopień wybranego wielomianu $u(x)$ przez m. Rozważmy pierścień wielomianów $R_0[z]$, gdzie z jest nową zmienną niezależną nad $k(x)$. Pokażemy, że wielomian $u(z) - u(x)$ jest nierozkładalny w $R_0[z]$. Załóżmy, że jest on rozkładalny. Niech

$$u(z) - u(x) = p_1(x,z) \cdot p_2(x,z), \tag{1}$$

gdzie $p_1(x,z), p_2(x,z) \in R_0[z]$.

Piszemy przy wielomianach p_1 oraz p_2 zmienną x z przyczyn technicznych. Formalnie przy tym rozkładzie rozważa się je jako wielomiany zmiennej z. Jednak współczynniki tych wielomianów należą do R_0, czyli są funkcjami wymiernymi zmiennej x. Uwzględnienie tej zmiennej będzie przydatne w dowodzie. Będziemy zmierzali do tego, by zmienna x występowała w p_1 oraz p_2 w postaci wielomianowej, na razie nie jest to jeszcze zagwarantowane. Współczynnik przy najwyższej potędze zmiennej z z lewej strony równości (1) jest elementem ciała k. Możemy więc bez zmniejszenia ogólności rozumowania założyć, że również współczynniki przy najwyższej potędze zmiennej z w wielomianach p_1 oraz p_2 należą do ciała k (możemy zawsze jeden z tych wielomianów pomnożyć, a drugi podzielić przez odpowiedni element z ciała R_0). Pokażemy, że przy tym założeniu wielomiany $p_1(x,z)$ oraz $p_2(x,z)$ należą do pierścienia $k[x,z]$. Rozważmy równość (1) w pierścieniu $k(x)[z]$. Niech $r = \deg_z p_1$ oraz $s = \deg_z p_2$. Niech $h_r(x) \in k[x]$ będzie naj mniejszym wspólnym mianownikiem współczynników wielomianu $p_1 \in R_0[z]$ oraz $f_s(x) \in k[x]$ będzie najmniejszym wspólnym mianownikiem współczynników wielomianu $p_2 \in R_0[z]$. Zatem możemy zapisać:

$$p_1(x,z) = \frac{1}{h_r(x)} \left(h_0(x) + h_1(x)z + \ldots + ch_r(x)z^r\right), \tag{2}$$

$$p_2(x,z) = \frac{1}{f_s(x)} \left(f_0(x) + f_1(x)z + \ldots + df_s(x)z^s\right), \tag{3}$$

gdzie $h_0, \ldots, h_r, f_0, \ldots, f_s \in k[x]$, $\operatorname{nwd}(h_0, \ldots, h_r) = 1$, $\operatorname{nwd}(f_0, \ldots, f_s) = 1$ oraz $c, d \in k$. Wówczas

$$h_r(x)f_s(x)\left(u(z) - u(x)\right) = \left(h_0(x) + \ldots + ch_r(x)z^r\right)\left(f_0(x) + \ldots + df_s(x)z^s\right).$$

Ponieważ obydwa czynniki występujące po prawej stronie tej równości są wielomianami pierwotnymi (to znaczy współczynniki każdego z nich są względnie pierwsze), więc z lematu Gaussa wynika, że ich iloczyn jest wielomianem pierwotnym. Zatem wielomian występujący po lewej stronie tej równości jest wielomianem pierwotnym. W szczególności $h_r(x), f_s(x) \in k$, z równości (2) i (3) wynika więc, że $p_1(x,z)$, $p_2(x,z) \in k[x,z]$. Dowiedliśmy tym samym, że współczynniki wielomianów $p_1, p_2 \in R_0[z]$ należą do $k[x]$, a w konsekwencji do $R_0 \cap k[x] = R$. Będziemy teraz chwilowo

rozważać p_1 oraz p_2 jako wielomiany w pierścieniu $k[x,z]$. Niech (i_1,j_1), (i_2,j_2) będą odpowiednio stopniami tych wielomianów w porządku leksykograficznym. Rozumiemy przez to, że rozważamy wszystkie pary wykładników przy wszystkich jednomianach (o niezerowym współczynniku) z danego wielomianu i porządkujemy je liniowo leksykograficznie. Zatem i_1 jest najwyższym wykładnikiem przy zmiennej x w wielomianie p_1, a j_1 jest najwyższym wykładnikiem przy zmiennej z w tych jednomianach wielomianu p_1, w których x występuje w potędze i_1. Wówczas stopień iloczynu $p_1(x,z)\cdot p_2(x,z)$ wynosi (i_1+i_2, j_1+j_2). Ale stopień tego iloczynu jest równy stopniowi wielomianu $u(z)-u(x)$, czyli wynosi $(m,0)$. Zatem $j_1=0$ oraz $j_2=0$. Zbadamy teraz, jaki wielomian zmiennej x stoi w wielomianie p_1 przy z^0. Wielomian $p_1(x,z)$ ma stopień $(i_1,0)$, więc występuje w nim jednomian $a_{i_1}x^{i_1}$ dla pewnego niezerowego $a_{i_1}\in k$. Z wartości tego stopnia wynika też, że szukany współczynnik przy z^0 równy jest $a_{i_1}x^{i_1}+\ldots+a_1x+a_0$. Ponieważ dowiedliśmy, że współczynniki wielomianu p_1 należą do R, więc uzyskujemy, że do R należy pewien wielomian o stopniu (ze względu na zmienną x) równym i_1. Ponieważ $i_1\geqslant 0$, $i_2\geqslant 0$ oraz $i_1+i_2=m$, więc z minimalności liczby m wynika, że $i_1=0$ lub $i_1=m$. W tym drugim przypadku $i_2=0$, zatem stopień jednego z wielomianów $p_1(x,z)$, $p_2(x,z)$ wynosi $(0,0)$. Stąd jeden z tych wielomanów należy do ciała k. To dowodzi nierozkładalności wielomianu $u(z)-u(x)$ w pierścieniu $R_0[z]$. Ponieważ element x jest pierwiastkiem nierozkładalnego nad R_0 wielomianu $u(z)-u(x)$, więc zachodzi równość $[R_0(x):R_0]=m$, gdzie lewa strona oznacza stopień odpowiedniego rozszerzenia ciał. Oczywiście $R_0(x)=k(x)$, bo $k\subset R\subset k[x]$, zatem $[k(x):R_0]=m$. Element x jest również pierwiastkiem wielomianu $u(y)-u(x)\in k(u)[y]$, więc również zachodzi nierówność $[k(x):k(u)]\leqslant m$, przy czym w sposób analogiczny jak powyżej skorzystaliśmy z tego, że $(k(u))(x)=k(x)$. Ponieważ $u\in R$, więc $u\in R_0$. Zatem zachodzą inkluzje $k(u)\subset R_0\subset k(x)$ oraz wynikająca z nich równość

$$[k(x):k(u)]=[k(x):R_0]\cdot[R_0:k(u)].$$

Uzyskujemy z niej nierówność $m\geqslant m\cdot[R_0:k(u)]$. Stąd $1\geqslant[R_0:k(u)]$, bo m jest dodatnie. Zatem $[R_0:k(u)]=1$, gdyż stopień rozszerzenia ciał jest zawsze dodatni. Stąd $R_0=k(u)$ i z lematu 1 wynika, że $R=k[u]$. □

Zakładamy odtąd, że k jest ciałem nieskończonym. Dowód następnego lematu jest oparty na dowodzie lematu 1 z pracy [7]. Zaks dowodzi, że stopień transcendencji ciała ułamków pierścienia R nad ciałem k wynosi 1. Z poniższego lematu też można to łatwo wywnioskować, jednak ta słabsza teza lematu 3 wystarcza do dowodu głównego twierdzenia.

Lemat 3. *Niech R będzie takim pierścieniem, że $k\subset R\subset k[x_1,\ldots,x_n]$. Jeśli wymiar Krulla pierścienia R wynosi 1, to R jest podpierścieniem pierścienia wielomianów jednej zmiennej.*

Dowód. Niech m będzie najmniejszą liczbą naturalną taką, że R jest podpierścieniem pierścienia wielomianów m zmiennych $k[y_1,\ldots,y_m]$. Jeśli $m=1$, to teza lematu jest spełniona. Niech więc $m>1$. Pokażemy, że to założenie prowadzi

do sprzeczności. Niech a będzie dowolnym elementem ciała k. Rozważmy homomorfizm

$$f_a : R \longrightarrow k[y_1, \ldots, y_m]$$

określony wzorem $f_a(r) = r(y_1, \ldots, y_{m-1}, a)$ dla $r(y_1, \ldots, y_m) \in R$. Ponieważ jądro homomorfizmu jest ideałem pierwszym, a wymiar Krulla pierścienia R wynosi 1, wiec albo $\ker f_a = 0$, albo $\ker f_a$ jest ideałem maksymalnym w R. Pierwszy przypadek nie może zajść, bo wówczas R zanurzałoby się w pierścień $k[y_1, \ldots, y_{m-1}]$, co byłoby sprzeczne z minimalnością liczby m. Zatem zachodzi drugi przypadek. Pierścień ilorazowy $R/\ker f_a$ jest więc ciałem. Jest on izomorficzny z obrazem zbioru R przy homomorfizmie f_a. Zatem każdy niezerowy element w obrazie jest odwracalny. Jedynymi odwracalnymi elementami w pierścieniu $k[y_1, \ldots, y_{m-1}]$ są elementy z ciała k. Otrzymujemy więc, że dla dowolnych $r \in R$ i $a \in k$ zachodzi $r(y_1, \ldots, y_{m-1}, a) \in k$. Ponieważ m jest minimalne i większe od 1, wiec nie może zachodzić inkluzja $R \subset k[y_m]$. Istnieje zatem $r \in R \setminus k[y_m]$. Niech

$$r = \sum b_{i_1 \ldots i_m} y_1^{i_1} \cdots y_m^{i_m} = \sum \left(\sum b_{i_1 \ldots i_m} y_m^{i_m} \right) y_1^{i_1} \cdots y_{m-1}^{i_{m-1}},$$

gdzie wszystkie elementy $b_{i_1 \ldots i_m}$ należą do k. Nie mogą wszystkie elementy postaci $\sum b_{i_1 \ldots i_m} y_m^{i_m}$ być wielomianami zerowymi, bo wówczas $r = 0$ wbrew temu, że $r \notin k[y_m]$. Co więcej, nie może się zdażyć tak, by tylko element $\sum b_{0 \ldots 0 i_m} y_m^{i_m}$ był niezerowy, bo wtedy $r = \sum b_{0 \ldots 0 i_m} y_m^{i_m} \in k[y_m]$. Zatem istnieją liczby całkowite $j_1, \ldots, j_{m-1}$ nie wszystkie równe zeru takie, że wielomian $\sum b_{j_1 \ldots j_{m-1} i_m} y_m^{i_m}$ jest różny od zera. Oznaczmy ten wielomian przez $b(y_m)$. Ponieważ jest on niezerowy, więc ma tylko skończoną liczbę pierwiastków. Ciało k jest nieskończone, więc istnieje takie $a \in k$, że $b(a) \neq 0$. Zatem $r(y_1, \ldots, y_{m-1}, a) \notin k$, bo przy tej ewaluacji przy jednomianie $y_1^{j_1} \cdots y_{m-1}^{j_{m-1}}$ stoi różny od zera współczynnik z ciała k. Jest to sprzeczne z warunkiem otrzymanym uprzednio, co dowodzi, że $m = 1$. □

Możemy teraz przystąpić do dowodu głównego twierdzenia.

Dowód twierdzenia Zaksa

Na mocy lematu 3 możemy założyć, że $R \subset k[x]$. Niech $S = R_0 \cap k[x]$. Wówczas S jest pierścieniem, bo jest przekrojem pierścieni. Ponieważ zachodzą inkluzje $R \subset R_0$ oraz $R \subset k[x]$, więc $R \subset S$. Zatem $R_0 \subset S_0$. Ponadto $S \subset R_0$ oraz R_0 jest ciałem, więc zachodzi również inkluzja $S_0 \subset R_0$ i ostatecznie $S_0 = R_0$. Ponieważ ciało k jest zawarte zarówno w pierścieniu $k[x]$ jak i w ciele R_0, więc mamy następujące zawierania

$$k \subset S \subset k[x].$$

Ponadto z równości $S_0 = R_0$ wynika, że $S = S_0 \cap k[x]$. Z lematu 2 otrzymujemy więc, że $S = k[v]$ dla pewnego $v \in S$. Zatem $R \subset k[v]$ oraz $R_0 = S_0 = k(v)$. W szczególności $v = \frac{r}{s}$ dla pewnych $r, s \in R$. Otrzymujemy stąd równość $vs - r = 0$.

Ponieważ $s \in R \subset k[v]$, więc $s = f(v)$, gdzie f jest wielomianem jednej zmiennej o współczynnikach w ciele k. Wówczas element v jest pierwiastkiem wielomianu $x \cdot f(x) - r \in R[x]$. Jest to wielomian unormowany nad R, bo współczynnik przy najwyższej potędze zmiennej x należy do ciała k, zatem w pierścieniu R jest odwracalny. Zatem v jest elementem całkowitym nad R. Ponieważ v należy do R_0, a pierścień R jest normalny, więc v należy do R. Stąd $R = k[v]$. □

References

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[2] S. Balcerzyk, T. Józefiak, *Pierścienie przemienne*, Państwowe Wydawnictwo Naukowe, Warszawa, 1985.

[3] P. Eakin, *A note of finite dimensional subrings of polynomial rings*, Proc. Amer. Math. Soc. **31** (1972) 75–80.

[4] A. Evyatar, A. Zaks, *Rings of polynomials*, Proc. London Math. Soc. **22** (1969) 582–586.

[5] A. Nowicki, *Polynomial derivations and their rings of constants*, N. Copernicus University Press, Toruń, 1994.

[6] A. Nowicki, M. Nagata, *Rings of constants for k–derivations in* $k[x_1, \ldots, x_n]$, J. Math. Kyoto Univ. **28** (1988) 111–118.

[7] A. Zaks, *Dedekind subrings of* $k[x_1, \ldots, x_n]$ *are rings of polynomials*, Israel J. Math. **9** (1971) 285–289.

Zaks theorem on a Dedekind subrings of the polynomial rings

Summary. In this note we give a proof of a theorem of Zaks concerning Dedekind subrings of polynomial rings over an infinite field.

Łódź, 10 – 14 stycznia 2000 r.