ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XIV (1972)

Ministerstwo Nauki i Szkolnictwa Wyższego

T. JÓZEFIAK (Bydgoszcz)

Kariera twierdzenia Hilberta o syzygiach

Ponad 80 lat temu Hilbert napisał pracę [1], która wywarła bardzo duży wpływ na rozwój wielu dziedzin algebry. W pracy tej pojawiło się twierdzenie Hilberta o bazie — obecnie jedno z podstawowych twierdzeń algebry przemiennej. Tam też została po raz pierwszy użyta funkcja charakterystyczna Hilberta, która odgrywa ważną rolę w geometrii algebraicznej. W pracy z 1890 r. Hilbert udowodnił jeszcze jedno twierdzenie, noszące teraz jego imię: twierdzenie o syzygiach, którym chciałbym się zająć w niniejszym artykule.

Czytelnika zapewne zaintryguje rzadko dziś słyszane w kręgach matematycznych słowo „syzygia" (gr. *συζυγια*, które znaczy — związek, relacja). Znaczenie tego pojęcia było jednak dobrze znane algebraikom XIX wieku jako jeden z terminów modnej wówczas teorii niezmienników: oznaczało relację algebraiczną pomiędzy niezmiennikami algebraicznymi. Twierdzenie Hilberta było udowodnione właśnie dla potrzeb tej teorii i na pozór dziwną może się wydać informacja, że twierdzenie o syzygiach jest twierdzeniem algebry homologicznej — młodej gałęzi algebry, powstałej niewiele ponad 20 lat temu.

Poniżej chciałbym przedstawić zarówno oryginalne, jak i współczesne sformułowanie twierdzenia o syzygiach oraz zwrócić uwagę na pewne szczegóły pracy Hilberta, które dały początek oddzielnemu nurtowi w algebrze homologicznej.

Zacznijmy od układu m równań liniowych jednorodnych o p niewiadomych:

$$(*)\qquad \begin{aligned} f_1^{(1)}X_1+f_1^{(2)}X_2+\ldots+f_1^{(p)}X_p &= 0,\\ f_2^{(1)}X_1+f_2^{(2)}X_2+\ldots+f_2^{(p)}X_p &= 0,\\ &\cdots\cdots\cdots\cdots\cdots\\ f_m^{(1)}X_1+f_m^{(2)}X_2+\ldots+f_m^{(p)}X_p &= 0. \end{aligned}$$

Jeśli współczynniki $f_j^{(i)}$ należą do ciała k, to wyznaczenie wszystkich rozwiązań tego układu jest proste. Zbiór rozwiązań tworzy w k^p podprzestrzeń liniową wymiaru p — rząd $(f_j^{(i)})$ i łatwo tę podprzestrzeń znaleźć.

Inaczej wygląda sytuacja, gdy ciało k zastąpić dowolnym przemiennym pierścieniem R (z jedynką 1). Naturalne jest pytanie dotyczące struktury zbioru rozwiązań układu (*). Otóż w zbiorze tym można zdefiniować dwa działania. Suma $f+g=(f_1+g_1,\ldots,f_p+g_p)$ dwóch rozwiązań $f=(f_1,\ldots,f_p)$ i $g=(g_1,\ldots,g_p)$ układu (*) jest znowu rozwiązaniem tego układu. Ponadto dla dowolnego $r\in R$, $r\cdot f=(rf_1,\ldots,rf_p)$ jest też rozwiązaniem układu równań (*). Działania $+$ i $\cdot$ mają następujące formalne własności:

1° zbiór M wszystkich rozwiązań układu (*) jest grupą przemienną ze względu na działanie $+$,

2° dla dowolnych $r, r_1, r_2\in R$, $f, g\in M$ mamy

$$r\cdot(f+g)=r\cdot f+r\cdot g,$$

$$(r_1r_2)\cdot f=r_1\cdot(r_2\cdot f),$$

$$1\cdot f=f.$$

Zbiór wszystkich rozwiązań układu równań (*) ma więc pewną strukturę algebraiczną zwaną *modułem*. Jest to oczywiście uogólnienie pojęcia przestrzeni liniowej nad ciałem.

W jakim języku i w jaki sposób można badać strukturę modułu M wszystkich rozwiązań układu (*)? Hilbert zajmował się tym problemem we wspomnianej na początku pracy [1]. Przedmiotem jego zainteresowania jest pierścień wielomianów z gradacją nad ciałem, tzn. pierścień $R=k[x_1,\ldots,x_n]$. Fakt, że pierścień R rozpatruje się jako pierścień z gradacją oznacza, że wyróżnione są w R zbiory R_q, $q\geqslant 0$ (zwane *zbiorami jednorodnych elementów stopnia* q), które są grupami ze względu na dodawanie w R i ponadto

$$R=\bigoplus_{q\geqslant 0}R_q$$

jest sumą prostą wszystkich R_q oraz $R_p\cdot R_q\subset R_{p+q}$. W przypadku pierścienia wielomianów za elementy zbioru R_q przyjmuje się po prostu formy stopnia q (inaczej — *wielomiany jednorodne stopnia* q). Ze względu na tę dodatkową strukturę gradacji w pierścieniu R Hilbert rozpatruje jedynie takie układy postaci (*), w których współczynniki $f_j^{(i)}$ są formami dodatniego stopnia. Stąd wynika, że każde rozwiązanie układu (*) jest sumą rozwiązań jednorodnych, a więc moduł rozwiązań M jest modułem z gradacją nad R, tzn. można przedstawić M jako sumę prostą $M=\bigoplus_{q\geqslant 1}M_q$, gdzie M_q składa się z rozwiązań jednorodnych stopnia q; oczywiście wówczas $R_p\cdot M_q\subset M_{p+q}$. Moduł M Hilbert nazywa *pierwszym modułem syzygii układu* (*).

Najpierw dowodzi Hilbert (korzystając z wcześniej sformułowanego twierdzenia o bazie), że moduł syzygii M jest skończenie generowany, tzn. istnieje skończony zbiór rozwiązań jednorodnych

$$g^{(1)} = (g_1^{(1)}, g_2^{(1)}, \ldots, g_p^{(1)}),$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$g^{(r)} = (g_1^{(r)}, g_2^{(r)}, \ldots, g_p^{(r)})$$

układu (*) mający tę własność, że każde inne jednorodne rozwiązanie g układu (*) jest kombinacją liniową rozwiązań $g^{(1)}, \ldots, g^{(r)}$ o współczynnikach będących formami z pierścienia $k[x_1, \ldots, x_n]$, tzn. $g = A_1 g^{(1)} + \ldots + A_r g^{(r)}$, gdzie A_i są formami. Wybierzmy rozwiązania $g^{(1)}, \ldots, g^{(r)}$ tak, by żadne z nich nie było kombinacją liniową pozostałych. Za pomocą rozwiązań $g^{(1)}, \ldots, g^{(r)}$ Hilbert tworzy nowy układ p równań jednorodnych o r niewiadomych:

$$(**) \qquad \begin{aligned} g_1^{(1)} Y_1 + g_1^{(2)} Y_2 + \ldots + g_1^{(r)} Y_r &= 0, \\ g_2^{(1)} Y_1 + g_2^{(2)} Y_2 + \ldots + g_2^{(r)} Y_r &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ g_p^{(1)} Y_1 + g_p^{(2)} Y_2 + \ldots + g_p^{(r)} Y_r &= 0. \end{aligned}$$

Jeśli współczynniki $g_j^{(i)}$ pochodzą z ciała i rozwiązania $g^{(1)}, \ldots, g^{(r)}$ tworzą bazę zbioru rozwiązań układu (*), to układ (**) nie ma rozwiązań niezerowych.

W przypadku rozpatrywanym przez Hilberta tak być nie musi, ale Hilbert dowodzi znowu, że rozwiązania układu (**) tworzą skończenie generowany moduł z gradacją nad pierścieniem $k[x_1, \ldots, x_n]$ (*drugi moduł syzygii układu* (*)). Wybierając skończony zbiór jednorodnych generatorów, z których powstają przez kombinacje liniowe wszystkie rozwiązania układu (**), i postępując analogicznie jak poprzednio, możemy utworzyć metodą opisaną powyżej trzeci układ równań (***). Jeśli trzeci moduł syzygii układu (*) jest niezerowy, to w podobny sposób dochodzimy do następnego (czwartego) układu równań itd.

Twierdzenie Hilberta o syzygiach głosi, że w opisanym procesie konstrukcji układów równań najpóźniej w n-tym kroku, gdy $n > 1$ (n oznacza liczbę zmiennych $x_1, \ldots, x_n$), dojdziemy do układu równań, który nie ma rozwiązań niezerowych (tzn. że n-ty moduł syzygii układu (*) jest zerowy).

W przypadku $n = 1$ moduł syzygii M może być różny od zera. Jeśli jednak elementy $f^{(1)}, \ldots, f^{(p)}$ tworzą minimalny zbiór generatorów modułu, który generują, to pierwszy moduł syzygii układu (*) jest zerowy, tzn. twierdzenie Hilberta jest przy tym założeniu prawdziwe i dla $n = 1$.

Przeformułujemy teraz konstrukcję Hilberta w trochę innym, bardziej współczesnym języku.

Oznaczmy przez R^p moduł wolny z gradacją rzędu p, tzn. moduł z gradacją nad R, którego bazę stanowią elementy $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0), \ldots, e_p = (0, 0, \ldots, 0, 1)$. Moduł rozwiązań $M = M^{(1)}$ jest oczywiście podmodułem modułu R^p generowanym przez elementy $g^{(1)}, g^{(2)}, \ldots, g^{(r)}$. Niech R^r oznacza moduł wolny o r wolnych generatorach $e'_1, e'_2, \ldots, e'_r$. Określamy homomorfizm $\varphi\colon R^r \to M^{(1)}$ przyjmując $\varphi(e'_i) = g^{(i)}$. Odwzorowanie φ jest epimorfizmem (tzn. obrazem φ jest całe $M^{(1)}$); przeanalizujmy jego jądro $M^{(2)}$.

Jeśli element $Y_1e'_1 + Y_2e'_2 + \ldots + Y_re'_r$ należy do jądra φ, to

$$0 = \varphi(Y_1e'_1 + Y_2e'_2 + \ldots + Y_re'_r) = Y_1g^{(1)} + Y_2g^{(2)} + \ldots + Y_rg^{(r)} =$$
$$= (Y_1g_1^{(1)} + Y_2g_1^{(2)} + \ldots + Y_rg_1^{(r)}, Y_1g_2^{(1)} + Y_2g_2^{(2)} + \ldots + Y_rg_2^{(r)}, \ldots$$
$$\ldots, Y_1g_p^{(1)} + Y_2g_p^{(2)} + \ldots + Y_rg_p^{(r)}),$$

a więc ciąg $(Y_1, Y_2, \ldots, Y_r)$ tworzy rozwiązanie układu równań (**). Oczywiście i na odwrót, każde rozwiązanie układu (**) wyznacza element z R^r należący do $M^{(2)}$. Wobec tego mamy ciąg dokładny

$$0 \to M^{(2)} \to R^r \xrightarrow{\varphi} M^{(1)} \to 0 \tag{1}$$

(tzn. obraz każdego homomorfizmu występującego w (1) jest równy jądru homomorfizmu następnego) i jeśli układ (***) nie ma rozwiązań niezerowych, to moduł $M^{(2)}$ jest wolny i na odwrót. Jeśli $M^{(2)}$ nie jest modułem wolnym i $h^{(1)}, \ldots, h^{(s)}$ tworzy minimalny zbiór jednorodnych generatorów $M^{(2)}$, to homomorfizm $\psi\colon R^s = Re''_1 \oplus \ldots \oplus Re''_s \to M^{(2)}$, $\psi(e''_i) = h^{(i)}$ ma jądro niezerowe $M^{(3)}$. Moduł $M^{(3)}$ jest modułem rozwiązań układu (***) i dostajemy ciąg dokładny

$$0 \to M^{(3)} \to R^s \xrightarrow{\psi} M^{(2)} \to 0. \tag{2}$$

Składając oba krótkie ciągi dokładne (1) i (2) otrzymujemy dłuższy ciąg dokładny

$$0 \to M^{(3)} \to R^s \xrightarrow{\psi} R^r \xrightarrow{\varphi} M^{(1)} \to 0.$$

Fakt, że najdalej n-ty układ równań nie ma rozwiązań niezerowych jest równoważny stwierdzeniu, że $M^{(n)}$ jest równe zeru, tzn. (postępując tak jak opisano powyżej) otrzymamy ciąg modułów wolnych i homomorfizmów

$$0 \to M^{(n-1)} \to \ldots \to R^s \xrightarrow{\psi} R^r \xrightarrow{\varphi} M^{(1)} \to 0 \tag{3}$$

długości $n-1$ (występuje $n-1$ modułów wolnych).

Hilbert przeprowadzał swoje rozważania tylko dla pierścienia wielomianów z gradacją $k[x_1, \ldots, x_n]$. Problem rozwiązalności układów równań i konstrukcję Hilberta można jednak sformułować dla dowolnego pierścienia R.

Niech M będzie modułem nad R. Przyjmijmy następującą definicję:

Rezolwentą wolną R-modułu M nazywamy dokładny ciąg modułów i homomorfizmów

$$\ldots \to F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \to \ldots \to F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0,$$

gdzie F_i są modułami wolnymi.

Moduł M może mieć wiele wolnych rezolwent (ma jednak zawsze co najmniej jedną). Oznaczmy przez $d(M)$ minimum długości rezolwent wolnych modułu M, tzn. długość najkrótszej rezolwenty wolnej modułu M.

W tym języku twierdzenie Hilberta można wysłowić następująco: jeśli $M^{(1)}$ oznacza moduł rozwiązań układu (*), to $d(M^{(1)}) \leqslant n-2$.

$M^{(1)}$ jest w tym przypadku bardzo specjalnym modułem. A jaka jest liczba $d(M)$ dla dowolnego modułu skończenie generowanego? Jeśli M jest takim modułem, to istnieje moduł wolny R^m i epimorfizm $R^m \to M \to 0$. Oznaczmy przez $M^{(0)}$ jądro tego homomorfizmu. $M^{(0)}$ jako podmoduł modułu wolnego jest skończenie generowany: niech $f^{(1)}, f^{(2)}, \ldots, f^{(p)}$ będzie minimalnym zbiorem generatorów modułu $M^{(0)}$. Budując homomorfizm modułu wolnego $R^p = Re_1 \oplus \ldots \oplus Re_p$ na $M^{(0)}$ tak, by $e_i \mapsto f^{(i)}$, otrzymujemy ciąg dokładny $0 \to M^{(1)} \to R^p \to M^{(0)} \to 0$, gdzie $M^{(1)}$ jest modułem wszystkich rozwiązań układu (*). Wobec tego dostaliśmy ciąg dokładny

$$0 \to M^{(1)} \to R^p \to R^m \to M \to 0,$$

co w połączeniu z ciągiem (3) daje wolną rezolwentę modułu M długości $\leqslant n$

$$0 \to \underbrace{M^{(n-1)} \to \ldots \to R^s \to R^r}_{n-1} \to \underbrace{R^p \to R^m}_{2} \to M \to 0.$$

Twierdzenie Hilberta mówi zatem, że dla dowolnego modułu skończenie generowanego M nad $k[x_1, \ldots, x_n]$ mamy $d(M) \leqslant n$.

Przyjmijmy następującą definicję: *Wymiarem globalnym pierścienia* R (gl.dim R) nazywamy kres górny wymiarów $d(M)$ R-modułów M skończenie generowanych:

$$\text{gl.dim}\, R = \sup d(M).$$

Widzimy więc, że twierdzenie Hilberta jest równoważne stwierdzeniu, że

$$\text{gl.dim}\, k[x_1, \ldots, x_n] \leqslant n. \tag{4}$$

W pracy Hilberta z 1890 roku jest nawet udowodniona równość $\mathrm{gl.dim}\, k[x_1, \ldots, x_n] = n$, ale nim do tego przejdziemy — kilka ogólnych uwag dotyczących metod dowodu powyższego twierdzenia.

Oryginalny dowód Hilberta twierdzenia o syzygiach jest długi i skomplikowany. Dowód ten jest szczególnie dopasowany do pierścienia z gradacją i chociaż wymiar globalny pierścienia wielomianów bez gradacji również jest równy liczbie zmiennych, to twierdzenie to nie było wówczas znane. Rozwój topologii algebraicznej i wyabstrahowanie czysto algebraicznych metod tam występujących doprowadziło na przełomie lat czterdziestych i pięćdziesiątych do powstania algebry homologicznej. Przez zastosowanie tych metod problem postawiony i rozwiązany przez Hilberta dla pierścienia z gradacją $k[x_1, \ldots, x_n]$ został uogólniony, stał się bardziej naturalny, a twierdzenie o syzygiach stanowi obecnie jedno z prostszych twierdzeń algebry homologicznej. Innymi słowy praca Hilberta znacznie wyprzedziła powstanie metod pozwalających skutecznie atakować postawiony problem.

Trudno w tym artykule omówić wszystkie aspekty i metody algebry homologicznej. Wydaje się jednak, że najważniejsza w obliczaniu wymiarów modułów i pierścieni jest metoda funktorów pochodnych. Istnieje ciąg funktorów dwóch argumentów Ext^n, $n = 0, 1, 2, \ldots$ o tej własności, że dla pierścieni i modułów z gradacją mamy

$$d(M) = n \Leftrightarrow \mathrm{Ext}^k(M, X) = 0 \text{ dla dowolnego modułu } X \text{ i } k > n \text{ oraz istnieje taki moduł } N, \text{ że } \mathrm{Ext}^n(M, N) \neq 0.$$

Rozwinięcie teorii funktorów Ext (i ogólnej teorii funktorów pochodnych) pozwala skutecznie badać problem rozpatrywany 80 lat temu przez Hilberta.

Czytelników pragnących zapoznać się bliżej z metodami algebry homologicznej odsyłam do książki Balcerzyka [2] — jedynego w języku polskim podręcznika w tej dziedzinie. Tam też (str. 265) można znaleźć dowód twierdzenia o syzygiach (dla pierścienia wielomianów bez gradacji).

Istotną cechą rozważań Hilberta jest korzystanie na każdym kroku z gradacji. Moduły z gradacją nad pierścieniem z gradacją mają jednak pewne dodatkowe zalety i własności, które zostały odkryte już w późniejszym okresie. W dalszym ciągu ograniczę się do pierścieni z gradacją, ilustrując na tym przykładzie rozwój metod stosowanych do dokładniejszej analizy pierwotnego problemu Hilberta.

Niech $A = \bigoplus_{i=0}^{\infty} A_i$ będzie algebrą z gradacją nad ciałem k taką, że $A_0 = k$. Przykładami takich algebr są: algebra wielomianów $k[x_1, \ldots, x_n]$, algebra zewnętrzna $\Lambda(kx_1 \oplus \ldots \oplus kx_n)$. W konstrukcji układów równań liniowych Hilbert za każdym razem wybierał minimalny zbiór generatorów, tzn. taki zbiór, że żaden jego podzbiór już nie jest zbiorem genera-

torów. Istnieją takie pierścienie i takie moduły nad nimi, które mają minimalne zbiory generatorów różnej mocy. Inaczej jest dla pierścieni z gradacją. Jeśli przez I oznaczyć ideał $I = \bigoplus_{i=1}^{\infty} A_i$, to mamy następujące kryterium:

Zbiór jednorodnych elementów $\{x_\alpha\}_{\alpha\in\Lambda}$ jest minimalnym zbiorem generatorów modułu M wtedy i tylko wtedy, gdy elementy $\{\overline{x}_\alpha = x_\alpha + IM\}_{\alpha\in\Lambda}$ tworzą bazę przestrzeni liniowej M/IM nad ciałem k.

Korzystając z tej własności można dla każdego A-modułu z gradacją M zbudować rezolwentę wolną w następujący sposób: jeśli $\{m_\alpha\}_{\alpha\in\Lambda_0}$ tworzy minimalny zbiór generatorów modułu M (m_α — elementy jednorodne), to przyjmijmy $F_0 = \bigoplus_{\alpha\in\Lambda_0} Ax_\alpha$ (gdzie F_0 oznacza moduł wolny nad A o bazie x_α, $\alpha\in\Lambda_0$) i określmy d_0: $F_0 \to M$, gdzie $d_0(x_\alpha) = m_\alpha$. Jeśli N_0 jest jądrem d_0, to ciąg $0 \to N_0 \to F_0 \xrightarrow{d_0} M \to 0$ jest dokładny. Gdy $\{n_\alpha\}_{\alpha\in\Lambda_1}$ jest minimalnym zbiorem generatorów modułu N_0, to przyjmując $F_1 = \bigoplus_{\alpha\in\Lambda_1} Ay_\alpha$, $d_1(y_\alpha) = n_\alpha$ otrzymujemy ciąg dokładny $0 \to N_1 \to F_1 \xrightarrow{d_1} N_0 \to 0$, gdzie N_1 jest równe jądru d_1. O ile $N_1 \neq 0$, to postępujemy podobnie jak poprzednio. W ten sposób otrzymujemy rezolwentę wolną

$$\ldots \to F_n \xrightarrow{d_n} F_{n-1} \to \ldots \to F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0,$$

która ma tę dodatkową własność, że dla każdego i jądro d_i jest zawarte w podmodule IF_i modułu F_i. Rezolwentę taką nazywamy *rezolwentą minimalną*. Można wykazać, że każde dwie rezolwenty minimalne modułu M są izomorficzne, a więc istnieją izomorfizmy φ_i: $F_i \to P_i$ takie, że diagram

$$\begin{array}{ccccccccccc}
\ldots \to & F_n & \xrightarrow{d_n} & F_{n-1} & \to \ldots \to & F_1 & \xrightarrow{d_1} & F_0 & \xrightarrow{d_0} & M & \to 0 \\
& \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \| & \\
\ldots \to & P_n & \xrightarrow{\partial_n} & P_{n-1} & \to \ldots \to & P_1 & \xrightarrow{\partial_1} & P_0 & \xrightarrow{\partial_0} & M & \to 0
\end{array}$$

jest przemienny, tzn. $\varphi_{i-1}d_i = \partial_i\varphi_i$ dla $i = 0, 1, \ldots$ Jeśli M jest modułem skończenie generowanym, a algebra A jest skończenie generowaną algebrą przemienną (np. algebrą ilorazową algebry wielomianów) i F, P są dwiema rezolwentami minimalnymi modułu M, to rząd F_i = rząd $P_i < \infty$ i wobec tego liczby $b_i(M)$ = rząd F_i nie zależą od wyboru rezolwenty, a tylko od samego modułu M. Ciąg $\{b_i(M)\}$, $i = 0, 1, \ldots$, tworzy nowy ciąg niezmienników modułu M. W języku Hilberta $b_{i-1}(M^{(1)})$ jest liczbą elementów minimalnego zbioru generatorów modułu $M^{(i)}$ — i-tego modułu syzygii układu (*). Liczby $b_i(M)$ wyrażają się również w terminach wspomnianych już funktorów Ext: A-moduły $\mathrm{Ext}^i(M, k)$ są przestrzeniami liniowymi nad ciałem k i mamy $b_i(M) = \dim_k \mathrm{Ext}^i(M, k)$.

Jak opisać i wyznaczyć niezmienniki $b_i(M)$? Pewna metoda pozwalająca zbliżyć się do odpowiedzi na to pytanie podana będzie nieco później. A na razie wróćmy do udowodnionej przez Hilberta nierówności (4). W omawianej pracy Hilberta każde twierdzenie jest ilustrowane przykładami. Po dowodzie twierdzenia o syzygiach podany jest przykład ciągu syzygii ideału $(x_1, x_2, \ldots, x_n)$ nad pierścieniem $k[x_1, \ldots, x_n]$ w następującym sformułowaniu:

„Jeśli utworzyć łańcuch pochodnych układów równań równania

$$x_1X_1+x_2X_2+\ldots+x_nX_n=0,$$

to s-ty układ równań tego łańcucha składa się z $\binom{n}{s-1}$ równań o $\binom{n}{s}$ niewiadomych i liczba elementów minimalnego zbioru rozwiązań tego układu wynosi $\binom{n}{s+1}$. Współczynniki wszystkich układów równań są formami liniowymi".

Przed dowodem tego stwierdzenia dla dowolnego n Hilbert szczegółowo analizuje przykład dla $n = 4$. Jednakże już przykład $n = 3$ dobrze ilustruje ogólną metodę postępowania Hilberta. Mamy równanie

$$x_1X_1+x_2X_2+x_3X_3=0. \tag{5}$$

Nietrudno pokazać, że rozwiązania $\xi_1 = (0, -x_3, x_2)$, $\xi_2 = (-x_3, 0, x_1)$, $\xi_3 = (-x_2, x_1, 0)$ tworzą minimalny zbiór generatorów zbioru rozwiązań równania (5). Układ pochodny układu (5) jest postaci

$$\begin{aligned} -x_3U_2-x_2U_3&=0,\\ -x_3U_1+x_1U_3&=0,\\ x_2U_1+x_1U_2&=0 \end{aligned} \tag{6}$$

i ma tylko jedno rozwiązanie niezależne $(x_1, -x_2, x_3)$, a więc zbiór rozwiązań jest modułem wolnym o jednym generatorze $(x_1, -x_2, x_3)$. W ten sposób budowa rezolwenty wolnej została zakończona, tzn. otrzymaliśmy rezolwentę długości 3

$$0\to R\to R^3\to R^3\to R\to k\to 0.$$

Podobnie Hilbert znajduje dla pierścienia $k[x_1, x_2, \ldots, x_n]$ rezolwentę wolną długości n ciała k i dowodzi jednocześnie, że $d(k) = n$.

Informacja ta w połączeniu z wcześniejszą nierównością (4) daje równość

$$\mathrm{gl.dim}\, k[x_1, \ldots, x_n] = n = d(k).$$

Powyższy przykład daje nam jednak precyzyjniejsze wiadomości o minimalnej rezolwencie wolnej ciała k. Dowiadujemy się z niego nie tylko o długości rezolwenty, ale również o wartościach niezmienników $b_i(k)$.

Mamy mianowicie

$$b_i(k) = \binom{n}{i} \quad \text{dla} \quad 0 \leqslant i \leqslant n,$$

$$b_i(k) = 0 \quad \text{dla} \quad i > n.$$

Okazuje się, że dla dowolnej algebry z gradacją A nad ciałem k mamy równość $\mathrm{gl.dim}\, A = d(k)$, tzn. globalny wymiar k-algebry A realizuje się jako wymiar $d(k)$ A-modułu k. Pozwala to ograniczyć się tylko do szukania rezolwenty wolnej ciała k. Wróćmy jeszcze do przykładu rezolwenty ciała k nad pierścieniem $A = k[x_1, x_2, x_3]$. Rozpatrzmy algebrę zewnętrzną $\boldsymbol{X}$ na module wolnym o trzech generatorach wolnych u_1, u_2, u_3:

$$\boldsymbol{X} = \Lambda(Au_1 \oplus Au_2 \oplus Au_3).$$

Jest to algebra z gradacją $\boldsymbol{X} = \boldsymbol{X}_0 \oplus \boldsymbol{X}_1 \oplus \boldsymbol{X}_2 \oplus \boldsymbol{X}_3$ ($\boldsymbol{X}_i = 0$ dla $i > 3$), gdzie $\boldsymbol{X}_i = \Lambda^i(Au_1 \oplus Au_2 \oplus Au_3)$ są modułami wolnymi nad A, a mianowicie

$$\boldsymbol{X}_0 = A,$$

$$\boldsymbol{X}_1 = Au_1 \oplus Au_2 \oplus Au_3,$$

$$\boldsymbol{X}_2 = Au_1 \wedge u_2 \oplus Au_1 \wedge u_3 \oplus Au_2 \wedge u_3,$$

$$\boldsymbol{X}_3 = Au_1 \wedge u_2 \wedge u_3.$$

Określamy homomorfizmy d_1, d_2, d_3 następująco:

$$d_1\colon \boldsymbol{X}_1 \to \boldsymbol{X}_0, \quad d_1(u_i) = x_i,$$

$$d_2\colon \boldsymbol{X}_2 \to \boldsymbol{X}_1, \quad d_2(u_i \wedge u_j) = x_i u_j - x_j u_i,$$

$$d_3\colon \boldsymbol{X}_3 \to \boldsymbol{X}_2, \quad d_3(u_1 \wedge u_2 \wedge u_3) = x_1 u_2 \wedge u_3 - x_2 u_1 \wedge u_3 + x_3 u_1 \wedge u_2.$$

Można łatwo przeliczyć, że w taki sposób otrzymujemy ciąg dokładny

$$0 \to \boldsymbol{X}_3 \xrightarrow{d_3} \boldsymbol{X}_2 \xrightarrow{d_2} \boldsymbol{X}_1 \xrightarrow{d_1} \boldsymbol{X}_0 \to k \to 0, \tag{7}$$

który jest rezolwentą wolną ciała k nad A i który jest izomorficzny z rezolwentą skonstruowaną poprzednio. Dla przykładu obliczmy jądro homomorfizmu d_2: jeśli $U_3 u_1 \wedge u_2 + U_2 u_1 \wedge u_3 + U_1 u_2 \wedge u_3$ należy do jądra d_2, to

$$U_3(x_1 u_2 - x_2 u_1) + U_2(x_1 u_3 - x_3 u_1) + U_1(x_2 u_3 - x_3 u_2) = 0,$$

czyli

$$(-x_2 U_3 - x_3 U_2) u_1 + (-x_3 U_1 + x_1 U_3) u_2 + (x_2 U_1 + x_1 U_2) u_3 = 0,$$

a więc wektor (U_1, U_2, U_3) jest rozwiązaniem układu równań (6). W zupełnie podobny sposób można otrzymać rezolwentę ciała k nad algebrą $A = k[x_1, \ldots, x_n]$. W tym przypadku określamy

$$\boldsymbol{X} = \Lambda(Au_1 \oplus \ldots\ldots \oplus Au_n) = \bigoplus_{i=0}^{\infty} \boldsymbol{X}_i, \quad \boldsymbol{X}_i = \Lambda^i(Au_1 \oplus \ldots \oplus Au_n)$$

oraz $d_p\colon X_p \to X_{p-1}$ przyjmując

$$d_p(u_{i_1} \wedge \ldots \wedge u_{i_p}) = \sum_{j=1}^{p} (-1)^{j+1} x_{i_j} u_{i_1} \wedge \ldots \wedge u_{i_{j-1}} \wedge u_{i_{j+1}} \wedge \ldots \wedge u_{i_p}.$$

Ciąg dokładny

$$0 \to X_n \to \ldots \to X_p \xrightarrow{d_p} X_{p-1} \to \ldots \to X_1 \xrightarrow{d_1} X_0 \to k \to 0 \tag{8}$$

jest rezolwentą izomorficzną z tą, którą skonstruował Hilbert. Ale rezolwenta (8) ma tę zaletę, że jest wyposażona dodatkowo w strukturę algebry. Dokładniej, rezolwenta (8) ma następujące własności:

1) X jest algebrą z gradacją, $X = \bigoplus_{p=0}^{\infty} X_p$, $X_0 = A$,

2) każde X_p jest modułem wolnym z gradacją nad A, $X_p = \bigoplus_{q=0}^{\infty} X_{p,q}$,

3) X jest algebrą przemienną, tzn. dla elementów jednorodnych $x \in X_{p,q}$, $y \in X_{i,j}$ mamy

$$x \cdot y = (-1)^{ip+qi} y \cdot x,$$

4) określony jest A-homomorfizm (różniczka) $d = \oplus d_p\colon X \to X$ stopnia -1, tzn. $d_p\colon X_p \to X_{p-1}$ i $d^2 = 0$, czyli $d_{p-1} d_p = 0$,

5) struktury różniczki i algebry są zgodne, tzn. dla jednorodnych elementów $x \in X_{p,q}$, $y \in X_{i,j}$

$$d(xy) = dx \cdot y + (-1)^p x \cdot dy,$$

6) ciąg

$$\ldots \to X_p \xrightarrow{d_p} X_{p-1} \to \ldots \to X_1 \xrightarrow{d_1} X_0 \to k \to 0$$

jest minimalną rezolwentą wolną A-modułu k.

Można udowodnić, że dla dowolnej przemiennej (tzn. spełniającej warunek $ab = (-1)^{ij} ba$, $a \in A_i$, $b \in A_j$) algebry z gradacją A nad ciałem k istnieje rezolwenta mająca własności 1)-6).

Powróćmy teraz do niezmienników $b_i(k)$, $i = 0, 1, 2, \ldots$ Za ich pomocą można utworzyć szereg Poincarégo algebry A definiując $\mathscr{P}(A) = \sum_{i=0}^{\infty} b_i(k) t^i$. Wykorzystując sposób konstrukcji rezolwenty algebrowej dowodzi się (patrz [3]), że szereg $\mathscr{P}(A)$ ma postać ilorazu dwóch iloczynów

$$\mathscr{P}(A) = \frac{(1+t)^{n_1}(1+t^2)^{n_2}(1+t^3)^{n_3}\ldots}{(1-t)^{m_1}(1-t^2)^{m_2}(1-t^3)^{m_3}\ldots}.$$

Najprostszą postać $\mathscr{P}(A) = (1+t)^n$ przyjmuje ten wzór, gdy A jest algebrą wielomianów $k[x_1, \ldots, x_n]$ (wynik Hilberta). Można też udowodnić, że jest to charakteryzacja algebry $k[x_1, \ldots, x_n]$.

W ten sposób stare twierdzenie Hilberta o syzygiach stało się początkiem obecnych badań i odkryć w teorii homologii pierścieni.

Bibliografia

[1] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. 36 (1890), str. 473–534.

[2] S. Balcerzyk, *Wstęp do algebry homologicznej*, Biblioteka Matematyczna, t. 34, Warszawa 1970.

[3] T. Józefiak, *Tate resolutions for commutative graded algebras*, Bull. Acad. Polon. Sci., Ser. sci. math., astr. et phys. 17, nr 10 (1969), str. 617–621.