WOKÓŁ 17 PROBLEMU HILBERTA

PAWEŁ GŁADKI

Wszystko zaczęło się od Hilberta... Poniższa fotografia przedstawia matematyka z okresu, w którym sformułował listę swoich 23 problemów:

Rysunek 1. Dawid Hilbert około roku 1900

Jak wiadomo, jeżeli wielomian $f \in \mathbb{R}[X_1, \dots, X_n]$ jest sumą kwadratów wielomianów, $f = f_1^2 + \dots + f_k^2$, $f_1, \dots, f_k \in \mathbb{R}[X_1, \dots, X_n]$, to dla wszystkich $(x_1, \dots, x_n) \in \mathbb{R}^n$ $f(x_1, \dots, x_n) \geqslant 0$. Naturalne jest pytanie, czy implikację tę można odwrócić:

Problem **1.** *Czy jeżeli $f(x_1, \dots, x_n) \geqslant 0$ dla wszystkich $(x_1, \dots, x_n) \in \mathbb{R}^n$, $f \in \mathbb{R}[X_1, \dots, X_n]$, to $f = f_1^2 + \dots + f_k^2$, $f_1, \dots, f_k \in \mathbb{R}[X_1, \dots, X_n]$?*

Na pytanie to stosunkowo łatwo odpowiedzieć w przypadku $n = 1$, mianowicie:

Uwaga 1. *Jeżeli $f(x) \geqslant 0$ dla $x \in \mathbb{R}$, $f \in \mathbb{R}[X]$, to $f = g^2 + h^2$, $g, h \in \mathbb{R}[X]$.*

Dowód. Niech

$$f(X) = d \prod_{i=1}^{m} (X - a_i)^{k_i} \prod_{j} = 1^n ((X - b_j)^2 + c_j^2)^{l_j}$$

będzie rozkładem wielomianu f na czynniki nierozkładalne. Wówczas bez trudu stwierdzamy, że $d > 0$ oraz $k_1, \dots, k_m$ są parzyste. Zauważmy ponadto, że dla

$p, q, r, s \in \mathbb{R}$ zachodzi tożsamość:

$$(p^2+q^2)(r^2+s^2) = (pr-qs)^2 + (ps+qr)^2.$$

Korzystając z tej równości przedstawiamy jako sumę kwadratów:

- $((X-b_j)^2+c_j^2)^{l_j}$, $j \in \{1, \ldots, n\}$,
- $(X-a_i)^{\frac{k_i}{2}}\cdot$(to, co otrzymaliśmy), $i \in \{1, \ldots, \min\{m, n\}\}$,
- (to, co otrzymaliśmy) $\cdot$ (to, co zostało).

□

Niestety, ogólnie dla $n \geqslant 2$ odpowiedź jest negatywna, co udowodnił sam Hilbert w roku 1888 (por. [6]). Dowód Hilberta nie był efektywny, pierwszy przykład podał Motzkin w roku 1967 (por. [11]):

Przyk'ad 1. *Niech* $f(X,Y) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2 \in \mathbb{R}[X,Y]$. *Wówczas* $f(x,y) \geqslant 0$ *dla* $(x,y) \in \mathbb{R}^2$*, ale* f *nie jest sumą kwadratów wielomianów.*

Dowód. Pokażemy najpierw, że $f(x,y) \geqslant 0$ dla $(x,y) \in \mathbb{R}^2$. Zauważmy w tym celu, że dla $a, b, c \geqslant 0$:

$$\frac{a+b+c}{3} \geqslant \sqrt[3]{abc}.$$

Kładąc $a = 1$, $b = x^2y^4$, $c = x^4y^2$ otrzymujemy tezę.

Aby zobaczyć, że f nie jest sumą kwadratów wielomianów przypuśćmy, że jest na odwrót, czyli że $f = \sum f_i^2$, $f_i \in \mathbb{R}[X,Y]$. Oczywiście $\deg f_i \leqslant 3$, tak więc każdy f_i jest kombinacją liniową wielomianów:

$$1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, Y^3.$$

Zauważmy, że X^3 nie występuje w żadnym z f_i (bo wówczas w f występowałoby X^6). Podobnie zauważamy, że Y^3, X^2, Y^2, X, Y nie występują w żadnym z f_i. Wobec tego:

$$f_i = a_i + b_iXY + c_iX^2Y + d_iXY^2.$$

Ale w takim razie $\sum b_i^2 = -3$, co daje sprzeczność. □

Wobec powyższego, Minkowski zaproponował Hilbertowi następującą modyfikację zagadnienia:

Problem **2.** *Czy jeżeli* $f(x_1, \ldots, x_n) \geqslant 0$ *dla wszystkich* $(x_1, \ldots, x_n) \in \mathbb{R}^n$*,* $f \in \mathbb{R}[X_1, \ldots, X_n]$*, to* $f = f_1^2 + \ldots + f_k^2$*,* $f_1, \ldots, f_k \in \mathbb{R}(X_1, \ldots, X_n)$*?*

Hilbert przedstawił ten problem na słynnym zjeździe matematyków w Paryżu w 1900 roku i odtąd zagadnienie to znane jest jako 17ty problem Hilberta. Oto, co o zagadnieniu mówił sam Hilbert:[1)]

> Rzeczywista funkcja całkowita [2)] lub forma dowolnej liczby zmiennych o współczynnikach rzeczywistych taka, która nie przyjmuje wartości ujemnych zwana jest dodatnio określoną. Zbiór form dodatnio określonych jest zamknięty ze względu na operacje dodawania i mnożenia, ale również iloraz dwóch form dodatnio określonych – rozważany jako funkcja całkowita tych samych zmiennych – jest

[1)] Cytat za [9].

[2)] To znaczy funkcja analityczna na całej płaszczyźnie zespolonej o współczynnikach rzeczywistych.

dodatnio określona. Kwadrat dowolnej formy jest niewątpliwie formą dodatnio określoną. Ale odkąd, jak pokazałem,[3)] okazało się, że nie każda forma dodatnio określona może być otrzymana przez dodawanie kwadratów form, pojawia się pytanie – na które twierdząco odpowiedziałem w przypadku form trzech zmiennych[4)] – czy każda forma dodatnio określona może być przedstawiona jako iloraz sum kwadratów form. Odtąd wydaje się również pożądane, na przykład przy próbach odpowiedzi na pewne pytania dotyczące wykonywalności wybranych konstrukcji geometrycznych, aby wiedzieć, czy współczynniki form użytych w szukanym przedstawieniu mogą zawsze być wzięte z ciała, z którego pochodzą współczynniki danej formy.[5)]

Problem ten został rozwiązany pozytywnie przez Emila Artina w roku 1925 (por. [1]). Był to jeden z najbardziej spektakularnych sukcesów współczesnej algebry, która w owym czasie właśnie zaczynała się formować. Rozumowanie Artina można streścić następująco:

- Niech P będzie wielomianem, który nie jest sumą kwadratów funkcji wymiernych o współczynnikach rzeczywistych.
- Przez **pre-uporządkowanie** ciała rozumiemy zbiór:
  (1) zamknięty na dodawanie,
  (2) zamknięty na mnożenie,
  (3) zawierający wszystkie kwadraty.
  Jasne jest, że pre-uporządkowanie jest właściwe (tj. różne od całego ciała), gdy nie zawiera -1.
- Skoro P nie jest sumą kwadratów, istnieje pre-uporządkowanie ciała rzeczywistych funkcji wymiernych, które nie zawiera P.
- Wobec lematu Kuratowskiego - Zorna istnieje maksymalne pre-uporządkowanie o powyższej własności.
- Za pomocą takiego pre-uporządkowania wprowadzamy w ciele funkcji wymiernych porządek, w którym P jest ujemny.
- Ciało nazwiemy **formalnie rzeczywistym**, gdy -1 nie jest sumą kwadratów. Ciało nazwiemy **rzeczywiście domkniętym** , gdy jest równe każdemu swemu rzeczywistemu rozszerzeniu algebraicznemu.
- Konstruujemy ciało rzeczywiście domknięte i uporządkowane, zawierające ciało funkcji wymiernych ze zdefiniowanym przez nas porządkiem i takie, że jego porządek „indukuje” nasz porządek. W ciele tym P przyjmuje wartości ujemne.
- Pozostaje sprawdzić, że jeśli P przyjmuje wartości ujemne w skonstruowanym powyżej ciele rzeczywiście domkniętym, które zawiera ciało $\mathbb{R}$, to przyjmuje również wartości ujemne w ciele $\mathbb{R}$.

W związku z pozytywną odpowiedzią Artina pojawiły się nowe pytania. Można pogrupować je następująco:

- Jak można oszacować liczbę kwadratów w otrzymanej sumie?
- Jak efektywnie wyznaczyć dany rozkład? (Dowód Artina korzysta z pewnika wyboru)

[3)] Por. [6].
[4)] Por. [7].
[5)] Por. [8], zwłaszcza rozdział 7, ustęp 38.

- Jakie są możliwie najlepsze oszacowania stopni wielomianów wchodzących w skład sumy?

Jeżeli chodzi o oszacowanie liczby kwadratów, najważniejszymi dotąd poznanymi twierdzeniami są następujące dwa: Cassels w 1964 roku udowodnił, że dla wielomianów z $\mathbb{R}[X_1, \dots, X_n]$ liczba kwadratów w sumie jest nie mniejsza od $n+1$ (por. [2]), zaś w 1967 Pfifster, że nie większa od 2^n por. [12]. Istnieje hipoteza, że liczba ta jest równa 2^n, ale jedyny postęp w jej zweryfikowaniu został poczyniony dla $n = 1$ (por. powyższy przykład) i dla $n = 2$ - bardzo trudny dowód tego faktu opublikowali w 1971 Cassels, Ellison i Pfifster (por. [3]).

Problem znalezienia algorytmu rozkładu wielomianu na sumę kwadratów funkcji wymiernych jest również niezmiernie skomplikowany. Pierwsze dowody konstruktywne podali Habich i Kreisel, przegląd obecnej wiedzy na ten temat znaleźć można w [4] i [5].

17 problem Hilberta może być rozpatrywany też jako fragment o wiele wiekszej i ogólniejszej teorii, jaką jest skonstruowanie „słownika” pomiędzy geometrią i algebrą w przypadku rzeczywistym. Jak wiadomo, w przypadku geometrii zespolonej (lub, ogólnie, uprawianej nad dowolnym ciałem algebraicznie domkniętym) istnieje bardzo czytelny słownik pomiędzy pojęciami geometrycznymi - tj. zbiorami algebraicznymi - a pojęciami algebraicznymi - tj. ideałami radykalnymi. Klasyczne twierdzenie geometrii algebraicznej - twierdzenie Hilberta o zerach, zwane Nullstellensatz - w jednej z licznych wersji, w których bywa formułowane, brzmi:

Twierdzenie 1. *Niech $S = \{f_1, \dots, f_s\}$ będzie skończonym podzbiorem $\mathbb{C}[X_1, \dots, X_n]$, a A* **zbiorem algebraicznym** *związanym ze zbiorem S:*

$$A = \{(a_1, \dots, a_n) \in \mathbb{C}^n : f(a_1, \dots, a_n) = 0, f \in S\}.$$

Niech $f \in \mathbb{C}[X_1, \dots, X_n]$. Wówczas:

$$\bigwedge_{(a_1,\dots,a_n)\in A} f(a_1, \dots, a_n) = 0 \Longrightarrow \bigvee_{m\in\mathbb{N}} \bigvee_{h_1,\dots,h_s\in\mathbb{C}[X_1,\dots,X_n]} f^m = f_1h_1 + \dots + f_sh_s.$$

W podobny sposób wynik Artina wiąże nieujemność, która jest własnością geometryczną, z sumami kwadratów, co jest własnością algebraiczną. O wiele głębszym i ogólniejszym faktem jest twierdzenie Stengle'a z roku 1974 (por. [13]), które pokrótce omówimy. Rozważmy mianowicie przestrzeń $\mathbb{R}^n$ i pierścień $\mathbb{R}[X_1, \dots, X_n]$. Dla danego skończonego podzbioru S zbioru $\mathbb{R}[X_1, \dots, X_n]$ **pre-uporządkowaniem generowanym przez** S nazywamy najmniejsze pre-uporządkowanie zawierające zbiór S, tj. najmniejszy zbiór zawierający zbiór S, zbiór wszystkich kwadratów oraz zamknięty ze względu na sumę i iloczyn. Przyjmujemy oznaczenie $\sum \mathbb{R}[X_1, \dots, X_n]^2[S]$. Twierdzenie Stengle'a, zwane Positivenstellensatz, orzeka co następuje:

Twierdzenie 2. *Niech $S = \{f_1, \dots, f_s\}$ będzie skończonym podzbiorem $\mathbb{R}[X_1, \dots, X_n]$, a W* **zbiorem semialgebraicznym** *związanym ze zbiorem S:*

$$W = \{(a_1, \dots, a_n) \in \mathbb{R}^n : f(a_1, \dots, a_n) \geqslant 0, f \in S\}.$$

Niech $\sum \mathbb{R}[X_1, \dots, X_n]^2[S]$ będzie pre-uporządkowaniem generowanym przez zbiór S, niech $f \in \mathbb{R}[X_1, \dots, X_n]$. Wówczas:

$$\bigwedge_{(a_1,\dots,a_n)\in W} f(a_1, \dots, a_n) \geqslant 0 \Longrightarrow \bigvee_{m\in\mathbb{N}} \bigvee_{g,h\in\sum\mathbb{R}[X_1,\dots,X_n]^2[S]} fg = f^{2m} + h$$

Dowód Stengle'a wykorzystuje pewnik wyboru. Naturalne pytanie, które się pojawia, to kwestia efektywnego sprawdzania, czy dany wielomian spełnia wymienione zależności. Na tym polu osiągnięto dotychczas niewielki postęp - przykładowy efektywny algorytm podany jest w pracy Lombardiego z roku 1990 (por. [10]), tym nie mniej daleo mu do doskonałości.

Bibliografia

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Hamb. Abh. 5 (1927), 110 - 115.

[2] J. W. S. Cassels, *On the representation of rational functions as sums of squares*, Acta Arith. 9 (1964), 79 - 82.

[3] J. W. S. Cassels, K. Ellison, A. Pfifster, *On sums of squares and on elliptic curves over function fields*, J. Number Theory 3 (1971), 125 - 149.

[4] C. N. Delzell, *Kreisel's unwinding of Artin's proof*, w: Kreiseliana: about and around Georg Kreisel, A K Peters, 1996, 113 - 246.

[5] C. N. Delzell, L. Gonzales - Vega, H. Lombardi, *A continuous and rational solution to Hilbert's 17th problem and several cases of the Positivstellensatz*, Computational Algebraic Geometry, materiały z konferencji w Nicei, 21 - 25 kwiecień 1992, Progr. Math. 109, Birkhauser, Boston, 1993.

[6] D. Hilbert, *Über die Darstellung definiter Formen als Summe von Formenquadraten*, Math. Ann. 32 (1888), 342 - 350.

[7] D. Hilbert, *Über ternäre definite Formen*, Acta Mathematica 17 (1893), 169 - 198.

[8] D. Hilbert, *Grundlagen der Geometrie*, Leipzig, 1899.

[9] D. Hilbert, *Mathematische Probleme*, Arch. Math. Physik 1 (1901), no. 44 - 63, 213 - 277.

[10] H. Lombardi, *Nullstellensatz reel effectif et variantes*, C. R. Acad. Sci. Paris Ser. I Math. 310 (1990), no. 8, 635 - 640.

[11] T. S. Motzkin, *The arithmetic - geometric inequality*, Inequalities (Proc. Sympos. Wright - Patterson Ait Force Base, Ohio, 1965), Academic Press, New York, 1967, 205 - 224.

[12] A. Pfifster, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Invent. Math. 4 (1967), 229 - 237.

[13] G. Stengle, *A nullstellensatz and a positivenstellensatz in semialgebraic geometry*, Math. Ann. 207 (1974), 87 - 97.