Pokroky matematiky, fyziky a astronomie

Břetislav Novák

O sedmnáctém Hilbertově problému

Pokroky matematiky, fyziky a astronomie, Vol. 20 (1975), No. 3, 154--158

Persistent URL: http://dml.cz/dmlcz/139867

Terms of use:

© Jednota českých matematiků a fyziků, 1975

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

Hilbertovy problémy

O sedmnáctém Hilbertově problému

Břetislav Novák, Praha

Sedmnáctý Hilbertův problém má mezi ostatními jeho problémy zajímavé postavení. Byl rozřešen poměrně brzy, ale v posledních několika letech došlo k rozsáhlé renesanci této problematiky studiem jemnějších otázek, kde se výrazně uplatnily i moderní, nedávno rozvinuté oblasti matematiky. Poznamenejme, že ve sborníku [11] pojednává o tomto problému (možná nezaslouženě stručně) JU. I. MANIN.

Jaká je vlastně formulace tohoto problému ? Z teorie čísel (viz např. [3]) je známa tzv. Bachetova-Lagrangeova věta, která tvrdí, že *každé přirozené číslo lze vyjádřit součtem čtyř čtverců nezáporných celých čísel.* Je také známo, že existují přirozená čísla, která nemůžeme vyjádřit jen součtem tří čtverců nezáporných celých čísel; jsou to ostatně právě všechna čísla tvaru $4^a(8b + 7)$ s nezápornými celými a, b. Hilbert vlastně přenesl tuto problematiku na polynomy a racionální funkce.

Připomeňme nejprve obvyklá označení. Je-li K těleso (jehož nulový prvek značíme 0 a jednotkový 1), potom $K[x_1, x_2, \ldots, x_n]$ buď obor integrity polynomů v n neurčitých $x_1, x_2, \ldots, x_n$ s koeficienty z tělesa K a $K(x_1, x_2, \ldots, x_n)$ příslušné podílové těleso, tj. těleso racionálních funkcí v těchto neurčitých s koeficienty z K. Označme konečně R těleso všech reálných a Q těleso všech racionálních čísel, Z obor integrity celých čísel. Ptejme se nyní, kdy lze polynom $f \in R[x_1, x_2, \ldots, x_n]$ vyjádřit jako součet konečně mnoha čtverců prvků z $R[x_1, x_2, \ldots, x_n]$. Ihned dostaneme nutnou podmínku: polynom f musí být nezáporný, tj. je-li $t_j \in R$, $j = 1, 2, \ldots, n$, musí být $f(t_1, t_2, \ldots, t_n) \geqq 0$. Jak však ukázal Hilbert v [5] vtipným, ale poněkud komplikovaným příkladem, nemusí pro $n = 2$ takové vyjádření obecně vůbec existovat, tj. existují nezáporné polynomy z $R[x_1, x_2, \ldots, x_n]$, které nelze vyjádřit součtem konečně mnoha čtverců polynomů z $R[x_1, x_2, \ldots, x_n]$.

Nedávno (viz [13]) uvedl MOTZKIN příklad polynomu, který jednoduše uvedené tvrzení dokazuje. Buď

$$p(x, y) = 1 + x^2(x^2 - 3)\, y^2 + x^2 y^4 . \tag{1}$$

Snadno zjistíme, že

$$(1 + x^2)^2\, p(x, y) = (1 + x^2 - 2x^2y^2)^2 + x^2y^2(1 - x^2)^2\,(1 + x^2 + x^2y^2),$$

tj. $p(x, y)$ je nezáporný polynom (a uvedené vyjádření udává současně vyjádření $p(x, y)$ součtem čtyř čtverců funkcí z $R(x, y)$). Nechť nyní

$$p(x, y) = \sum_{j=1}^{k} p_j^2(x, y), \tag{2}$$

kde $p_j(x, y) \in R[x, y]$. Protože stupeň polynomu $p(x, y)$ je šest, je stupeň každého polynomu $p_j(x, y)$ nejvýše tři. Protože dále $p(x, 0) = p(0, y) = 1$, musí být $|p_j(x, 0)| \leqq 1$, $|p_j(0, y)| \leqq 1$, $j = 1, 2, \ldots, n$ pro všechna $x, y \in R$, tj. $p_j(x, 0) = p_j(0, y) = a_j$ je konstanta. Je tedy $p_j(x, y) = a_j + xy\, l_j(x, y)$, kde $l_j \in R[x, y]$ jsou polynomy stupně nejvýše jedna. Srovnáme-li pak koeficienty u členu x^2y^2 ve vztahu (2), dostáváme

$$-3 = \sum_{j=1}^{k} l_j^2(0, 0),$$

což zřejmě není možné. Proto Hilbert formuloval svůj problém takto ([11], str. 49): *Buď* $f \in R[x_1, x_2, \ldots, x_n]$ *nezáporný polynom. Lze nalézt racionální funkce* $g_j \in R(x_1, x_2, \ldots, x_n)$, $j = 1, 2, \ldots, k$ *tak, že* $f = g_1^2 + g_2^2 + \ldots + g_k^2$? Ihned vidíme, že náš problém se nezmění, jestliže místo nezáporného polynomu $f \in R[x_1, x_2, \ldots, x_n]$ připustíme obecněji nezápornou racionální funkci $f \in R(x_1, x_2, \ldots, x_n)$ (tj. takovou racionální funkci f, která má tu vlastnost, že pro každou volbu, $t_j \in R$, $j = 1, 2, \ldots, n$, pro něž je definována hodnota $f(t_1, t_2, \ldots, t_n)$, je tato hodnota nezáporná). Konečně dostaneme zřejmě rovnocenný problém, požadujeme-li vyjádření takové racionální funkce f ve tvaru podílu dvou součtů polynomů z $R[x_1, x_2, \ldots, x_n]$.

Některé částečné výsledky byly známy ještě před r. 1900, kdy Hilbert své problémy formuloval. Tak např. sám Hilbert vyřešil případ $n = 2$ (viz [5]), E. Landau ukázal (viz [8]), že pro $n = 2$ lze každý nezáporný polynom vyjádřit ve tvaru součtu ne více než čtyř čtverců. Poznamenejme, že Hilbert formuloval dokonce ostřejší otázku, jak se situace změní, nahradíme-li těleso R reálných čísel jiným číselným tělesem, např. Q. Pro srovnání rozdílnosti obou problémů uvažujeme případ $n = 1$. Je-li f nezáporný polynom s reálnými koeficienty, vidíme ihned z rozkladu na kořenové činitele, že

$$f(x) = f_1^2(x)\,(f_2(x) + if_3(x))\,(f_2(x) - if_3(x)) = (f_1(x)f_2(x))^2 + (f_1(x)f_3(x))^2,$$

kde f_1, f_2, f_3 jsou polynomy s reálnými koeficienty. V oboru integrity $R[x]$ lze tedy každý nezáporný polynom vyjádřit jako součet dvou čtverců. Na druhé straně je zřejmé, že polynomy f_1f_2, f_1f_3 z předchozí formule nemusí mít racionální koeficienty, i když $f \in Q[x]$. E. Landau však ukázal (viz [8]), že v oboru integrity $Z[x]$ stačí k vyjádření každého nezáporného polynomu osm čtverců. (Poznamenejme, že z citované Lagrangeovy věty plyne, že potřebujeme alespoň čtyři čtverce pro konstatní polynomy a alespoň pět čtverců pro polynomy stupně alespoň prvého.)

Úplné řešení sedmnáctého Hilbertova problému podal E. Artin (viz [1]). Abychom naznačili hlavní myšlenky jeho postupu, zobecníme nejprve celý problém. Buď K libovolné těleso a označme $S_j(K)$ množinu všech $a \in K$, k nimž existují $a_1, a_2, \ldots, a_j \in K$, ne všechny nulové, tak, že $a = a_1^2 + a_2^2 + \ldots + a_j^2$; označme ještě $S(K)$ sjednocení všech $S_j(K)$, $j = 1, 2, \ldots$. Je zřejmé, že množina $S(K)$ je uzavřená vzhledem k sčítání a násobení; je-li $0 \neq a = a_1^2 + a_2^2 + \ldots + a_m^2 \in S(K)$, je $a^{-1} = (a_1/a)^2 + (a_2/a)^2 + \ldots + (a_m/a)^2$, tj. $a^{-1} \in S(K)$.

Zajímavá je otázka, tvoří-li množina všech nenulových prvků z $S_j(K)$ vzhledem k násobení grupu. To platí zřejmě pro $j = 1$; z identity

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

a podobných identit pro $j = 4,8$ plyne kladná odpověď na naši otázku pro tato j. HURWITZ (viz [7]) však ukázal, že podobné identity existují právě pro uvedená j. Přesto se však A. PFISTEROVI (viz [9]) podařilo ukázat, že odpověď je kladná pro všechna j, která jsou mocninou dvojky. Tyto výsledky byly v souvislosti s Hilbertovým problémem podstatně využity.

Ptejme se nyní, jaký je vztah mezi K a $S(K)$. Jednoduchá je odpověď, je-li charakteristika tělesa K rovna dvěma. Potom je totiž $(a_1 + a_2 + \ldots + a_m)^2 = a_1^2 + a_2^2 + \ldots + a_m^2$, a tedy $S(K)$ obsahuje právě všechny čtverce prvků tělesa K a je to (vzhledem ke vztahu $-a = a$) dokonce těleso. Je-li K konečné těleso nebo prvotěleso, je zřejmě $S(K) = K$.

V dalším nechť je K těleso charakteristiky $p \neq 2$. Nechť nejprve $0 \in S(K)$, tj. existují $b_1, b_2, \ldots, b_j \in K$, ne všechny nulové, tak, že $b_1^2 + b_2^2 + \ldots + b_j^2 = 0$. Odtud plyne, že existují prvky $a_1, a_2, \ldots a_{j-1} \in K$ tak, že $a_1^2 + a_2^2 + \ldots + a_{j-1}^2 = -1$. Pro libovolné $a \in K$ potom platí

$$a = (1 + a)^2/4 - (1 - a)^2/4 = ((1 + a)/2)^2 + (a_1(1 - a)/2)^2 + \\ + (a_2(1 - a)/2)^2 + \ldots + (a_{j-1}(1 - a)/2)^2 \in S(K),$$

tj. v tomto případě máme $S(K) = K$. Poznamenejme, že poslední vztah platí speciálně pro libovolné těleso, jehož charakteristika p je větší než dvě – stačí položit $a_1 = a_2 = \ldots = a_{j-1} = 1, j = p$.

Poslední – a nejobtížnější – případ tedy je, když $0 \notin S(K)$. Charakteristika těchto těles je nutně nula a nazýváme je *tělesa formálně reálná.* Teorii těles tohoto typu založili E. ARTIN a J. SCHREIER (viz např. [1]). Formálně reálná tělesa lze velmi jednoduše charakterizovat jako tělesa, která lze uspořádat, tj. můžeme určit množinu P „kladných" prvků tělesa která neobsahuje nulu, je uzavřená vzhledem k násobení a sečítání a navíc, je-li c nenulový prvek tohoto tělesa je buď $c \in P$, nebo $-c \in P$. (V obvyklém zápisu znamená pak $a < b$ přesně totéž, co $b - a \in P$; tyto „nerovnosti" lze sečítat, násobit „kladným" prvkem atp.) Povšimněme si, že každý nenulový čtverec, a tedy i každý prvek množiny $S(K)$ je při každém uspořádání tělesa K kladný. Důležité je, že platí i obrácené tvrzení: *Jestliže prvek $a \in K$ je kladný při každém uspořádání tělesa K (tzv. totálně pozitivní prvek), potom $a \in S(K)$.*

Poznamenejme, že tělesa Q, R připouštějí jen jediné (přirozené) uspořádání. Existují však tělesa, která mají i nespočetně mnoho různých uspořádání. Např. těleso $Q[\sqrt{(2)}]$ má právě dvě uspořádání: jedno přirozené a druhé určené tím, že jeho kladné prvky mají tvar $a - b\sqrt{(2)}$, $a, b \in Q$, kde – v přirozeném uspořádání – je $a + b\sqrt{(2)} > 0$. Těleso $Q(x)$ můžeme uspořádat třeba takto: řekneme, že $f(x) \in Q(x)$ je kladný prvek, je-li $f(\pi) > 0$ (roli čísla π může také převzít libovolné transcendentní číslo) atp.

Buď nyní K nějaké těleso reálných čísel. K i $K(x_1, x_2, \ldots, x_n) = K(x)$ jsou zřejmě formálně reálná tělesa. Poznamenejme, že každé uspořádání tělesa $K(x)$ indukuje některé uspořádání tělesa K. Nyní platí toto důležité tvrzení: *Je-li v tělese $K(x)$ dáno uspořádání a jsou-li $f_j(x) \in K(x)$, $j = 1, 2, \ldots, m$, potom existují prvky $a_1, a_2, \ldots, a_n \in K$ (dokonce $a_1, a_2, \ldots, a_n \in Q$) takové, že polynom $f_j(x)$ při uspořádání tělesa $K(x)$ a prvek $f_j(a_1,$*

$a_2, \ldots, a_n) \in K$ *při indukovaném uspořádání tělesa* K *mají „stejná znaménka“,* $j = 1, 2, \ldots, m$.

Odtud již lze odvodit řešení Hilbertova problému v tomto tvaru:

Věta. *Buď* K *těleso reálných čísel (tj. máme* $Q \subset K \subset R$*), v němž existuje jediné (tj. pouze přirozené) uspořádání. Potom* $S(K(x_1, x_2, \ldots, x_n))$ *obsahuje právě všechny nezáporné racionální funkce* $f \in K(x_1, x_2, \ldots, x_n)$.

Důkaz. Nechť $f \in K(x)$ je nezáporná racionální funkce, která neleží v $S(K(x))$. Potom f musí být záporným prvkem v některém uspořádání $<$ tělesa $K(x)$, a proto pro vhodnou n-tici $a_1, a_2, \ldots, a_n$ prvků z K je $f(a_1, a_2, \ldots, a_n) < 0$. Protože však $f(a_1, a_2, \ldots, a_n) \in K$ a těleso K připouští jen přirozené uspořádání, je $f(a_1, a_2, \ldots, a_n)$ záporné reálné číslo a máme spor s předpokladem, že f je nezáporná racionální funkce, cbd.

Poznamenejme, že podstatným bodem důkazu věty je výše uvedené tvrzení, které je nejsložitější částí důkazu (i když se zdá být přirozené a jednoduché). Jeho důkaz probíhá indukcí podle počtu proměnných a využívá v podstatě rozkladu polynomů z $K[x]$ na ireducibilní faktory a jednoduchého faktu, že polynom „v okolí jednoduchého nulového bodu mění znaménko“.

Tím byl Hilbertův sedmnáctý problém vyřešen, ale vlastně jen ve své původní formulaci. Landauův výsledek dává vznik řadě otázek, na něž Artinova věta nemůže vzhledem k patrné neefektivnosti svého důkazu dát odpověď. Omezíme se na speciální případ. Ptejme se, zdali existuje přirozené číslo $m = m(n)$ tak, že každá nezáporná racionální funkce z $R(x_1, x_2, \ldots, x_n)$ je součtem nejvýše m čtverců prvků z $R(x_1, x_2, \ldots, x_n)$. (Upozorněme opět výslovně, že z Artinovy věty neplyne ani existence tohoto čísla, natož jeho numerická hodnota.) Existuje-li takovéto m, označme $N = N(n)$ minimální m uvedené vlastnosti.

Ukázali jsme, že $N(1) = 2$ a uvedli jsme Landauův výsledek $N(2) \leqq 4$ (viz [8]). Uvažujme polynom

$$p(x_1, x_2) = 1 + x_1^2 + x_2^2 .$$

Tento polynom je zřejmě ireducibilní v $Q[x_1, x_2]$ a ze vztahu

$$p = (f_1/f_0)^2 + (f_2/f_0)^2, \text{ tj. } pf_0^2 = (f_1 + \mathrm{i}f_2)(f_1 - \mathrm{i}f_2),$$

kde $0 \neq f_0, f_1, f_2 \in Z[x_1, x_2]$ a f_0, f_1 jsou nesoudělné polynomy, by plynulo, že p dělí $f_1 \mathrm{i} f_2$, a tedy i f_0, což je spor. Je tedy $N(2) > 2$. Více než šedesát let zůstal však problém přesné hodnoty $N(2)$ nerozřešen. Konečně pomohl Motzkinův polynom (1). V roce 1971 (viz [12]) bylo dokázáno, že vztah

$$1 + x_1^2(x_1^2 - 3)\, x_2^2 + x_1^2 x_2^4 = g_1^2 + g_2^2 + g_3^2 , \quad g_1, g_2, g_3 \in R(x_1, x_2) \tag{3}$$

nemůže platit, tj. máme $N(2) = 4$. Tento příklad je patrně nejjednodušší, neboť pro polynomy z $R(x_1, x_2)$ stupně menšího než šest nebo stupně menšího než čtyři vzhledem k jedné z proměnných vyjádření součtem tří čtverců nalezneme. K obtížnému (více než dvacetistránkovému) důkazu uveďme jen, že z platnosti vztahu (3) plyne, že existují $\xi, \eta \in R(x_1)$, $\eta \neq 0$ a ξ nezáporné tak, že

$$-\eta^2 = \xi(\xi - x_1^2(x_1^2 - 3) - 2x_1)(\xi - x_1^2(x_1^2 - 3) + 2x_1), \tag{4}$$

tj. máme ukázánu existenci „racionálního bodu" na eliptické křivce (4), který má jisté speciální vlastnosti (ξ nezáporné). Vyšetřením grupy všech racionálních bodů na křivce (2) lze pak ukázat, že to není možné.

Do dnešního dne není hodnota $N(n)$ pro $n \geqq 3$ známa. Je pouze ukázáno, že $N(n) \leqq 2^n$ (Ax [2] pro $n = 3$, obecně PFISTER [9]). Na druhé straně ukázal CASSELS (viz [4]), že polynom $1 + x_1^2 + x_2^2 + \ldots + x_n^2$ nemůže být součtem n čtverců z $R(x_1, x_2, \ldots, x_n)$, tj. $N(n) \geqq n + 1$. Vysoce pravděpodobná domněnka je $N(n) = 2^n$, ale dnešního dne jsme asi jejímu důkazu ještě hodně vzdáleni.

Uveďme ještě závěrem, že tento Hilbertův problém je v zajímavém vztahu ke geometrii, přesněji ve vztahu ke konstrukcím kružítkem a pravítkem na jedné straně a konstrukcím pravítkem (a pevnou jednotkou délky) na straně druhé (blíže viz [6]). Konečně nezůstal Hilbertův problém ušetřen vlivu současných proudů v matematice a v letech 1955—7 publikoval A. ROBINSON (viz [10], kap. VIII) důkaz jistého zobecnění Artinovy věty pomocí teorie modelů. V každém případě tedy sedmnáctý Hilbertův problém dal a dává podnět k vypracování nových teorií, jejichž problematika je stále živá.

Literatura

[1] E. ARTIN, *Über die Zerlegung definiter Funktionen in Quadrate*, Abh. Math. Sem. Hamburg *5* (1927), 100—115.

[2] J. AX, *On ternary definite rational functions*, Proc. London Math. Soc. (v tisku).

[3] Z. I. BOREVIČ, I. P. ŠAFAREVIČ, *Těorija čiseł*, Moskva 1964.

[4] J. W. S. CASSELS, *On the representation of rational functions as sums of squares*, Acta Arithmetica *IX* (1964), 79—82.

[5] D. HILBERT, *Über die Darstellung definiter Formen als Summe von Formen quadraten*, Math. Ann. *32* (1888), 342—350.

[6] D. HILBERT, *Grundlagen der Geometrie*, B. G. Teubner 1930.

[7] A. HURWITZ, *Über die Komposition der quadratischen Formen von beliebig vielen Variablen*, Nachrichten der Königlichen Gesellschaft der Wisschenschaften zu Göttingen 1898, 309—316.

[8] E. LANDAU, *Über die Darstellung definiter Funktionen durch Quadrate*, Math. Ann. *62* (1906), 272—285.

[9] A. PFISTER, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Invent. Math. *4* (1967), 229—237

[10] A. ROBINSON, *Introduction to model theory and to the mathematics of algebra*, North-Holland Publ. Comp. 1963.

[11] *Problemy Gil'berta* (sborník), Moskva 1969.

[12] J. W. S. CASSELS, W. J. ELLISON, A. PFISTER, *On Sums of Squares and on Elliptic Curves over Function Fields*, Journal of Number Theory *3* (1971), 125—149.

[13] T. S. MOTZKIN, *The arithmetic-geometric inequality*, Proc. Sympos. on Inequalities, Academic Press, New York, 1967, 205—224.

I dobrá logika uvedená ve špatném čase a na špatném místě může být nejhorší nepřítel dobrého učení.

G. PÓLYA
