Časopis pro pěstování matematiky a fysiky

Vladimír Kořínek
Důkaz jedné věty Einsteinovy

Časopis pro pěstování matematiky a fysiky, Vol. 58 (1929), No. 1-2, 23--29

Persistent URL: http://dml.cz/dmlcz/108936

Důkaz jedné věty Eisensteinovy.

Napsal *Vladimír Kořínek.*

Tento článek jest věnován důkazu této věty pocházející od Eisensteina:

Věta Eisensteinova. *Každá ternární kvadratická forma definitní o reálných a celistvých koeficientech, která má více než dvě automorfie, jest ekvivalentní aspoň jedné z těchto dvou forem:*

$$\begin{aligned} f(x_1, x_2, x_3) &= a_{11} x_1^2 + a_{22} x_2^2 + 2a_{23} x_2 x_3 + a_{33} x_3^2 = \\ &= a_{11} x_1^2 + \varphi(x_2, x_3), \end{aligned} \tag{1}$$

$$\begin{aligned} g(x_1, x_2, x_3) &= 2a_{12} x_1^2 + 2a_{12} x_1 x_2 + a_{22} x_2^2 + 2a_{23} x_2 x_3 + a_{33} x_3^2 = \\ &= 2a_{12} x_1^2 + 2a_{12} x_1 x_2 + \varphi(x_2, x_3). \end{aligned} \tag{2}$$

Při tom v dalším budu rozuměti automorfií ternární kvadratické formy substituci o celistvých reálných koeficientech a determinantu ± 1, která převádí formu samu v sebe. Ternární formy budu uvažovati vždy ve tvaru

$$\begin{aligned} F(x_1, x_2, x_3) &= a_{11} x_1^2 + a_{22} x_2^2 + a_{33} x_3^2 + \\ &+ 2a_{23} x_2 x_3 + 2a_{13} x_1 x_3 + 2a_{12} x_1 x_2, \end{aligned} \tag{3}$$

kdež a_{ik} jsou celá čísla. Formám tvaru (1) resp. (2) budu říkati formy f resp. g.

Hoření větu uveřejnil Eisenstein poprve bez důkazu v Crelleově Journalu v pojednání,[1]) jehož cílem bylo stanovení počtu tříd ternárních kvadratických forem positivních, což se mu pro některé případy podařilo. Ona věta skutečně stačí úplně spolu s výrazem pro váhu forem k stanovení tohoto počtu.[2]) Důkaz věty Eisensteinovy podal P. Bachmann.[3]) Zakládá se na pomocné větě, že každá ternární kvadratická forma definitní, která má více než dvě automorfie, má aspoň jednu automorfii periody 2, a rozdílnou od triviální automorfie

---

[1]) Eisenstein: Tabelle der reduzierten positiven quadratischen Formen. Journal f. r. u. a. Math. 41, 1851, str. 141, 227. Viz str. 168.

[2]) Vl. Kořínek: Rozpravy II. tř. čes. Ak. 35, 1926, č. 14.; 36, 1927, č. 39.

[3]) P. Bachmann: Zahlentheorie IV. Teil II. Abteilung, str. 358—364.

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

která spolu se substitucí identickou jest automorfií každé ternární formy. Důkaz této pomocné věty obsahuje však v Bachmannově knize hrubou chybu[4]) a pokud jest mi známo, lze tuto větu dokázati jen pomocí redukce a její důkaz jest velmi dlouhý. Podávám proto zde důkaz Eisensteinovy věty úplně nezávislý na oné pomocné větě.

Důkaz zakládá se na Sellingově redukci ternárních forem.[5]) Velká výhoda Sellingovy redukce proti redukci Seeberově, pomocí které dospěl asi Eisenstein ke své větě, spočívá v úplné souměrnosti redukčních podmínek. Aby Selling dosáhl této souměrnosti, uvádí ternární formu (3) na trochu jiný tvar tím, že zavede čtvrtou pomocnou proměnnou. Položí totiž

$$x_i = \xi_i - \xi_4, \qquad i = 1, 2, 3.$$

Tím přejde forma F ve tvar

$$\begin{aligned} \Phi(\xi_1, \xi_2, \xi_3, \xi_4) = A_{12}(\xi_1 - \xi_2)^2 + A_{13}(\xi_1 - \xi_3)^2 + A_{14}(\xi_1 - \xi_4)^2 + \\ + A_{23}(\xi_2 - \xi_3)^2 + A_{24}(\xi_2 - \xi_4)^2 + A_{34}(\xi_3 - \xi_4)^2. \end{aligned} \tag{5}$$

Mezi koeficienty formy F a Φ platí tyto vztahy:

$$a_{12} = -A_{12}, \qquad a_{13} = -A_{13}, \qquad a_{23} = -A_{23}$$

$$\begin{aligned} a_{11} - A_{12} - A_{13} &= A_{14} \\ -A_{12} + a_{22} - A_{23} &= A_{24} \\ -A_{13} - A_{23} + a_{33} &= A_{34} \\ -A_{14} - A_{24} - A_{34} &= -a_{44}, \end{aligned} \tag{6}$$

kdež $a_{44} = F(1, 1, 1) > 0$. Formou F jest jednoznačně určena forma Φ a naopak. Přejde-li forma F v F' substitucí o determinantu ± 1

$$x_i = \alpha_{i1} x'_1 + \alpha_{i2} x'_2 + \alpha_{i3} x'_3 \qquad i = 1, 2, 3, \tag{7}$$

pak přejde příslušná forma Φ v Φ' substitucí

---

[4]) Viz [3]). Na str. 359 jest první výraz pro S' chybný. Z něho jest odvozena a tudíž i nesprávná rovnice (36) na str. 360, na níž se celý důkaz zakládá.

[5]) Selling: Über die binären und ternären quadratischen Formen. Journal f. r. u. a. Math. 77, 1874, 143.

Selling: Des formes quadratiques binaires et ternaires. Journal pour les math. p. et app. 3, 1877, 21, 153.

Velmi pěkně jest vyložena tato redukce v práci Charve: De la réduction des formes quadratiques ternaires positives. Annales de l'Ec. N. S. 2. sér., 9, 1880, sup.

Shrnuji zde výsledky Sellingovy, protože zavádím pro další výklady poněkud jiné označení než Selling a Charve.

$$\xi_i - \xi_4 = \bar{a}_{i1}\,\xi'_1 + \bar{a}_{i2}\,\xi'_2 + \bar{a}_{i3}\,\xi'_3 + \bar{a}_{i4}\,\xi'_4 \qquad i = 1, 2, 3, \quad (8)$$

kdež

$$\bar{a}_{i1} + \bar{a}_{i2} + \bar{a}_{i3} + \bar{a}_{i4} = 0 \qquad i = 1, 2, 3. \quad (9)$$

Protože ve formě Φ i Φ' záleží jen na rozdílech proměnných, lze odečísti od každého koeficientu v témže i-tém sloupci substituce (8) jedno a totéž číslo a_{4i}, a substituci (8) psáti ve tvaru souměrnějším

$$\xi_i = a_{i1}\,\xi'_1 + a_{i2}\,\xi'_2 + a_{i3}\,\xi'_3 + a_{i4}\,\xi'_4 \qquad i = 1, 2, 3, 4, \quad (10)$$

kdež místo vztahů (9) platí vztahy

$$\sum_{i=1}^{4} a_{1i} = \sum_{i=1}^{4} a_{2i} = \sum_{i=1}^{4} a_{3i} = \sum_{i=1}^{4} a_{4i}, \quad i = 1, 2, 3, 4. \quad (11)$$

Sellingovy podmínky redukční lze shrnouti ve větu:[6])

1. věta. *Ternární kvadratická forma positivní F jest redukovaná, když v příslušné formě Φ součet koeficientů*

$$A_{12} + A_{13} + A_{14} + A_{23} + A_{24} + A_{34} \quad (12)$$

jest minimem. V tomto případě platí pro koeficienty tyto nerovnosti

$$A_{12} \geqq 0, \quad A_{13} \geqq 0, \quad A_{14} \geqq 0, \quad A_{23} \geqq 0, \quad A_{24} \geqq 0, \quad A_{34} \geqq 0.$$

V každé třídě ternárních kvadratických forem positivních jsou 24 formy redukované, které dostaneme z jedné z nich všemi permutacemi proměnných $\xi_1, \xi_2, \xi_3, \xi_4$, a není-li žádný z koeficientů formy Φ roven nule, existují ve třídě jen tyto formy redukované.

Důkaz této věty provedl Selling na základě věty:[7])

2. věta. *Ve formě Φ o koeficientech jen kladných neb rovných nule zvětší se výraz (12) každou substitucí mimo ty substituce, které převádějí každý rozdíl $\xi_i - \xi_k$ ve Φ se vyskytující opět v takový rozdíl $\xi'_e - \xi'_m$.*

Protože automorfie formy nechává výraz (12) beze změny a převádí formu Φ samu v sebe, dostáváme z této věty ihned tuto:

3. věta. *Automorfie (7) redukované formy F provedená ve tvaru (10) na příslušnou formu Φ permutuje jen s případnou změnou znaménka rozdíly $\xi_i - \xi_k$ ve formě Φ se vyskytující.*

V dalším pro jednoduchost označíme $\iota, \varkappa, \lambda, \mu$ jistou libovolnou permutaci čísel 1, 2, 3, 4, a zavedeme označení $a_{\iota\varkappa} = a_{\varkappa\iota}$ a $A_{\iota\varkappa} = A_{\varkappa\iota}$ pro $\iota > \varkappa$. Důkaz věty Eisensteinovy provedeme nyní na základě této věty:

4. věta. *Formě g jsou ekvivalentní tyto formy:*

1. forma, pro niž platí

$$a_{\iota\lambda} = a_{\varkappa\lambda}, \quad a_{\iota\iota} = a_{\varkappa\varkappa},$$

t. j. podle rov. (6)

$$A_{\iota\lambda} = A_{\varkappa\lambda}, \quad A_{\iota\mu} = A_{\varkappa\mu};$$

---

[6]) Viz [5]): Charve str. 12, Selling str. 167.

[7]) Viz [5]): Charve str. 15 a násl.

2. *forma, pro niž platí*

$$a_{\iota\iota} = a_{\varkappa\varkappa}, \quad a_{\lambda\lambda} = a_{\mu\mu},$$

t. j. podle rov. (6)

$$A_{\iota\mu} = A_{\varkappa\lambda}, \quad A_{\iota\lambda} = A_{\varkappa\mu}.$$

Podle 1. věty libovolná permutace indexů u proměnných značí jen přechod k ekvivalentní formě redukované. Možno tudíž položiti bez újmy všeobecnosti $\iota = 1$, $\varkappa = 2$, $\lambda = 3$, $\mu = 4$. Pak přejde forma pod 1. neb forma pod 2. ve formu g substitucí

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ neb } \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Budeme nyní vyšetřovati zvláště formy Φ, v nichž žádný koeficient A_{ik} nerovná se nule, dále ty formy Φ, v nichž jeden, dva neb tři koeficienty A_{ik} se rovnají nule.

I. Vyšetřujme nejdříve formy Φ, v nichž žádný koeficient nerovná se nule. O těchto formách platí:

Není-li žádný koeficient A_{ik} v Φ roven nule, dává nám každá substituce (8), která permutuje až snad na změnu znaménka rozdíly $\xi_i - \xi_k$ z Φ mezi sebou, jednu a jen jednu substituci tvaru (10) takovou, že permutuje jen mezi sebou proměnné $\xi_1, \xi_2, \xi_3, \xi_4$, při čemž buď u všech proměnných změní znaménko neb u žádné. Naopak každá substituce (10) těchto vlastností dává nám jednu a jen jednu substituci tvaru (8), která permutuje až snad na změnu znaménka rozdíly $\xi_i - \xi_k$ z Φ.

Snadno nalezneme, že substituce (8) hořeních vlastností má tento tvar, je-li $\varepsilon = \pm 1$:

$$\begin{aligned} \xi_1 - \xi_4 &= \varepsilon\xi_\iota && - \varepsilon\xi_\mu \\ \xi_2 - \xi_4 &= \varepsilon\xi_\varkappa && - \varepsilon\xi_\mu \\ \xi_3 - \xi_4 &= \varepsilon\xi_\lambda && - \varepsilon\xi_\mu. \end{aligned} \tag{13}$$

Substituci (10) dostaneme pomocí (11), položíme-li

$$\alpha_{4\iota} = 0, \quad \alpha_{4\varkappa} = 0, \quad \alpha_{4\lambda} = 0, \quad \alpha_{4\mu} = \varepsilon.$$

Jest ihned viděti, že permutuje jen proměnné ξ_i a to beze změny znaménka neb se změnou znaménka u všech proměnných podle toho, je-li $\varepsilon = +1$ neb -1. Naopak má-li substituce (10) tento tvar, dostaneme z ní ihned jednu a jen jednu substituci (8) ve tvaru (13).

Podle 3. věty automorfie formy F musí míti tvar právě uvažovaný a musí převáděti příslušnou formu Φ v sebe. Identická permutace proměnných ξ_i dává nám pro $\varepsilon = 1$ substituci identickou, pro $\varepsilon = -1$ druhou automorfii (4) každé ternární formy. Má-li tudíž forma F více než dvě automorfie, pak grupa permutací proměnných ξ_i, spojených s případnou změnou znaménka, která odpovídá grupě automorfií formy F, obsahuje aspoň jednu z těchto permutací psaných v cyklech, nebereme-li ohled na případnou změnu znaménka:

$$(\xi_\iota, \xi_\varkappa), \quad (\xi_\iota, \xi_\varkappa)(\xi_\lambda, \xi_\mu), \quad (\xi_\iota, \xi_\varkappa, \xi_\lambda), \quad (\xi_\iota, \xi_\lambda, \xi_\varkappa, \xi_\mu).$$

Obsahuje-li grupa čtvrtou permutaci, obsahuje i druhou. Podle 1. věty možno bez újmy všeobecnosti zvoliti $\iota = 1$, $\varkappa = 2$, $\lambda = 3$, $\mu = 4$.

1. Aby forma Φ přecházela v sebe permutací (ξ_1, ξ_2) jest nutno, aby

$$A_{13} = A_{23}, \quad A_{14} = A_{24},$$

což jest 1. případ 4. věty.

2. Má-li forma Φ přecházeti v sebe permutací $(\xi_1, \xi_2) \cdot (\xi_3, \xi_4)$, jest nutno, aby

$$A_{13} = A_{24}, \quad A_{14} = A_{23},$$

což jest 2. případ 4. věty.

3. Má-li forma Φ přecházeti v sebe permutací (ξ_1, ξ_2, ξ_3), jest nutno, aby

$$A_{12} = A_{23} = A_{13}, \quad A_{14} = A_{24} = A_{34},$$

což jest 1. případ 4. věty.

V dalším budeme psáti formu Φ ve tvaru

$$\Phi = A_{12} X_1^2 + A_{13} X_2^2 + A_{14} X_3^2 + A_{23} X_4^2 + A_{24} X_5^2 + A_{34} X_6^2,$$

kdež význam veličin X_i plyne ihned srovnáním s výrazem (5) pro Φ.

II. Nechť ve Φ jeden koeficient rovná se nule. Bez ujmy všeobecnosti možno podle 1. věty položiti $A_{13} = 0$. Veličiny X_1 až X_6 nejsou na sobě nezávislé, nýbrž v tomto případě platí mezi nimi tyto vztahy:

$$\begin{aligned} X_1 - X_3 + X_5 &= 0 \\ X_4 - X_5 + X_6 &= 0. \end{aligned} \tag{14}$$

Snadno se najde, že každá substituce (7) o determinantu ± 1 taková, že příslušná substituce (8) ve formě Φ s $A_{13} = 0$ permutuje až na případnou změnu znaménka rozdíly $\xi_i - \xi_k$ ve Φ se vyskytující, t. j. proměnné X_1, X_3, X_4, X_5, X_6, převádí v sebe systém rovnic (14). Naopak každá permutace proměnných X_1, X_3, X_4, X_5, X_6 spojená s případnými změnami znamének, která převádí rovnice (14) v sebe, dává nám substituci (7) o determinantu ± 1 a takovou, že příslušná substituce (8) převádí formu Φ v ekvivalentní formu Φ', v níž opět $A'_{13} = 0$. Při tom možno zvoliti u jedné z proměnných X_1, X_3, X_4, X_5, X_6 znaménko libovolně a u ostatních jest již určeno požadavkem, že rovnice (14) přecházejí v sebe.

Podle 3. věty každá automorfie formy F vede k určité hoření permutaci proměnných X_1, X_3, X_4, X_5, X_6 s případnými změnami znamének. Z rovnic (14) plyne, že X_5 vždy přechází jen v sebe, neboť se vyskytuje v obou rovnicích. Zbývá tedy uvažovati permutace proměnných X_1, X_3, X_4, X_6. Identická permutace dává opět identickou automorfii, se změnou znaménka u proměnných pak automorfii (4). Neidentická permutace, která převádí rov. (14) v sebe, převádí aspoň X_1 neb X_4 v jinou proměnnou. Protože permutace

$$(X_1, X_4, X_3, X_6), \tag{15}$$

která převádí s příslušnými změnami znamének rovnice (14) v sebe, značí jen přechod k ekvivalentní formě, stačí uvažovati jen proměnnou X_1.

1. Nechť X_1 přejde danou permutací v X_3, pak jest nutno, aby

$$A_{12} = A_{14},$$

a stačí změniti znaménko u x_1 a x_3, abychom dostali formu g.

2. Nechť X_1 přejde v X_4, pak z (14) plyne, že X_3 přechází v X_6, a jest nutno, aby

$$A_{12} = A_{23}, \quad A_{14} = A_{34},$$

což jest 1. případ 4. věty.

3. Nechť přejde X_1 v X_6, pak plyne z (14), že současně přechází X_3 v X_4. Provedeme-li zde však permutaci (15), dostaneme přechody X_4 v X_1 a X_6 v X_3, což dává stejný výsledek jako předchozí případ.

III. Nechť ve formě Φ jsou dva koeficienty rovny nule. Protože podle 1. věty lze provésti napřed libovolnou permutaci indexů u koeficientů, mohou nastati jen tyto dva podstatně různé případy: 1. $A_{12} = 0$; $A_{13} = 0$; 2. $A_{12} = 0$, $A_{34} = 0$. V případě prvém jest již forma F ve tvaru f. Zbývá tedy uvažovati jen případ druhý. Zde platí mezi proměnnými X_2, X_3, X_4, X_5 tento vztah

$$X_2 - X_3 - X_4 + X_5 = 0. \tag{16}$$

Lehko se opět nalezne, že každá substituce (7) o determinantu $+1$ taková, že příslušná substituce (8) permutuje ve formě Φ mezi sebou s případnou změnou znaménka jen rozdíly $\xi_i - \xi_k$ ve Φ se vyskytující, t. j. proměnné X_2, X_3, X_4, X_5 převádí rovnici (16) samu v sebe. Naopak každá permutace proměnných X_2, X_3, X_4, X_5 spojená s takovými změnami znamének, aby rovnice (16) přecházela v sebe, dává nám substituci (7) o determinantu $+1$, a takovou, že příslušná substituce (8) převádí formu Φ ve Φ', v níž opět $A'_{12} = 0$, $A'_{34} = 0$. Při tom lze určiti u jedné proměnné X_i znaménko a při dané permutaci jsou ostatní znaménka určena již rovnicí (16). Značí tedy permutace proměnných X_2, X_3, X_4, X_5 přechod k ekvivalentní formě. Identická permutace dává nám identickou substituci, spojená se změnou znaménka substituci (4). Podle 3. věty každá automorfie permutuje proměnné X_2, X_3, X_4, X_5. Má-li tedy forma více automorfií než dvě, pak jistě jedna z těchto proměnných přechází v jinou. Bez ujmy všeobecnosti lze předpokládat podle předchozího, že X_2 přechází v X_5, čímž dostáváme 2. případ 4. věty.

IV. Jsou-li konečně tři koeficienty v Φ rovny nule, jest forma F vždy ve tvaru f. Více než tři koeficienty A_{ik} nemohou býti v positivní formě rovny nule. Tím jest Eisensteinova věta dokázána.

*

Démonstration d'un théorème d'Eisenstein.

(Extrait de l'article précédent.)

L'article précédent contient une démonstration du théorème, dû à Eisenstein, (Pour la bibliographie, voir les notes 1) 3) 5) suivant:

Une forme quadratique ternaire positive à coefficients réels et entiers qui possède plus de deux transformations en elle-même à coefficients entiers, est équivalente au moins à une de ces deux formes:

$$f(x_1, x_2, x_3) = a_{11} x_1^2 + a_{22} x_2^2 + 2a_{23} x_2 x_3 + a_{33} x_3^2,$$
$$g(x_1, x_2, x_3) = 2a_{12} x_1^2 + 2a_{12} x_1 x_2 + a_{22} x_2^2 + 2a_{23} x_2 x_3 + a_{33} x_3^2.$$

Ce théorème servait à Eisenstein pour point de départ pour le calcul du nombre de classes des formes quadratiques ternaires positives. Il a été démontré pour la première fois par P. Bachmann. (Voir la note 3) a 4). Dans sa démonstration Bachmann se servait du lemme suivant: Chaque forme quadratique ternaire positive ayant plus que deux transformations en elle-même en possède une avec la période 2, différente de la transformation triviale (4). Mais la démonstration de ce lemme donnée dans le livre de Bachmann n'est pas exacte (p. 359). On ne peut le démontrer qu' au moyen de la réduction des formes ternaires et positives. Cette démonstration est très longue. Dès lors, il serait interessant de donner une autre démonstration du théorème d'Einsenstein, indépendante du lemme mentionné. Dans ce qui précède, je donne une telle démonstration qui est relativement très courte, en me servant de la réduction de Selling comme base.