

Posudek

na diplomovou práci

Polotělesa a planární funkce

Bc. Terezy Hrubéšové

Matematicko-fyzikální fakulta Univerzity Karlovy, Praha, 2018

Výzkumná témata práce představují 1) polotělesa spolu s jejich izotopismy, 2) planární funkce a speciálně tzv. Dembowského—Ostromovy polynomy (DO polynomy), zavedené v [Dembowski, P., Ostrom, T., Math. Z., 103 (1968)], a 3) vztahy mezi předchozími dvěma tématy.

Zaměřením práce náleží do moderní projektivní geometrie a matematické kryptografie.

Obsah práce a některé výsledky

Autorka shrnuje jak známé poznatky o vztazích rovin a okruhů, zkoumané již Davidem Hilbertem a jeho studenty Maxem Dehmem a Ruth Moufangovou při analýze nedesarguesovských rovin, tak se zabývá současnými výzkumnými tématy jakými jsou izotopie kvazigrup a polotěles a tzv. Dembowského—Ostromovými polynomy. DO polynomy zkoumané v práci jsou definovány na konečných tělesech. Takto se do práce dostávají kombinatorické úvahy, které lze provádět s příslušnými konečnými incidenčními strukturami. Vlastnosti DO polynomů umožněné konečností tělesa na druhou stranu umožňuje lineárně geometrickou formulaci. Práce je tak co do metod povahy geometrické, kombinatorické a algebraické.

Pro projektivní rovinu autorka v kapitolách 1 a 2 uvádí standardní konstrukci souřadnicového ternárního okruhu a známé podmínky, za nichž je tento okruh kvazitělesem, nebo dokonce polotělesem. Tyto kapitoly lze považovat za motivující k představení algebraických struktur a jejich výzkumu, kterým se Bc. Hrubéšová zabývá v kapitolách 3 a 4. V kapitole 3 jsou podrobně zkoumána (před)polotělesa a jejich izotopismy. V kapitole 4 jsou zkoumány planární funkce a jimi generované incidenční struktury, zejména pak polotělesové roviny, a Dembowského—Ostromovy polynomy včetně jejich souvislosti s kvadratickými zobrazeními. Roviny zadané planární funkcí takové, že jejichž souřadnicové okruhy tvoří polotělesa, jsou izomorfní rovinám „generovaným“ DO polynomy (s. 56 a Věta 4.32). V páté kapitole lze nalézt pro práci klíčové informace o planárních DO polynomech, jimiž „indukovaná“ polotělesa jsou izotopní konečným popř. komutativním smyknutým tělesům (Důsledky 5.7 a 5.8).

Charakter, původnost výsledků a přínos

Práce má v převažující míře **kompilační charakter**, ale mnohé výsledky (zejm. Kap 4 a 5) jsou **původní** (viz *Otázky*). Kompaktní důkaz výsledků pokročilých částí práce, jako jsou Věta 4.32 a Důsledky 5.7 a 5.8 považuji za přínos práce. Práce čítá přes 60 stran.

Autorka **usouvztažňuje** důkaz [Coulter, R., Henderson, M., Commutative presemifields and semifields, *Advances of Math.*, Vol. 217 (2008)] o souvislosti planárních DO polynomů a komutativních polotěles lichého řádu k poznatkům o izotopii polotěles, podávajíc tak **zpřesnění a doplnění** zmíněného důkazu. Originální je také výzkum **souvislosti DO polynomů a kvadratických zobrazení**.

Přínos vidím také v **shrnutí** zmíněných témat v jednu práci a zvláště zařazení systematického pojednání o izotopii kvazigrup a polotěles v kapitole 3. Výsledky práce se jeví jako aktuální vzhledem k použití DO polynomů v kryptografii a jejímu současnému rozvoji.

Sloh práce

Práce je přehledně a z jazykového hlediska velmi pěkně napsána. Formulace vět jsou přesné a členění činí text srozumitelný.

Drobný nedostatek vidím 1) v nepoměru mezi počtem stran (cca 20) části, v níž je formulován výsledek, kterého autorka dosáhla, a relativně dlouhého úvodu (cca 40 stran). Tomu se možná dalo předejít formulováním úvodních partií stručněji, např. pro ternární okruhy, jež jsou polotělesy. 2) **Větší míra upozorňování na to, co je vlastním výsledkem a co je již známé**, by bylo pro vědeckou úroveň, ale i pro čtivost, práci přínosné.

Překlepy či typografické chyby se v práci téměř nevyskytují.

Nesrovnalosti

1) Slosloví “ternární systém” není v práci definováno, s. 16; jde zřejmě o množinu s operacemi splňující (T1) – (T4) [popř. (T1) – (T5) nebo (T1) – (T4) s modifikací (T2), jenž je v práci uváděna]

2) Ve větě 2.2 se tvrdí, že dvojice (P, L) je projektivní rovina, přičemž P je definováno za užití symbolu l_∞ , jehož definice (těsně nad větou) je podána pro souřadnicový ternární okruh pocházející z projektivní roviny. Autorka však to, že ternární okruh pochází z projektivní roviny (je souřadnicový ternární okruh) v důkazu nepředpokládá. Na druhou stranu („přímku v nekonečnu”) l_∞ lze definovat i bez toho, že T je souřadnicový ternární okruh.

Otázky

Mohla by autorka uvést **některé** z vět, které jsou dokázány v kapitolách 4 a 5 a které nejsou uvedeny v preprintech [Drápal, A., Attempting to solve a problem in commutative fields, 2017] a [Drápal, A., Few facts about isotopy, 2017], na něž je odkazováno – zejména ty, které považuje za podstatné. Preprinty nejsou zatím veřejně dostupné.

Zdroj ke kapitole 1 není uveden explicitně (u ostatních kapitol řešeršní povahy uveden je). Jde o původní práci předkladatelky?

Závěr

Obor práce je tzv. klasický, a tak jakékoliv nové výsledky v něm, zvláště jsou-li navázány na přitažlivé aplikace, jsou závažné a výjimečné, byť zde se jedná třeba jen o opravu a doplnění důkazu.

Autorka prokázala dobrou schopnost pracovat v syntetickém matematickém oboru, schopnost přesné formulace tvrzení a definic a dosáhnout nových výsledků.

Hodnocení

Práce splňuje požadavky kladené na Univerzitě Karlově na diplomovou práci.

V Praze 25. 1. 2018

Doc. Mgr. Svatopluk Krýsl, Ph.D.

Matematický ústav Univerzity Karlovy (Matematicko-fyzikální fakulta UK)