

**Oponentský posudek
na doktorskou disertační práci Mgr. Václava Flašky
„Congruence-simple semirings and semimodules“**

Předložená doktorská disertační práce Mgr. Václava Flašky „Kongruenčně jednoduché polookruhy a polomoduly“ je věnována problematice, která je v současné době vysoce aktuální zejména vzhledem k potenciálním aplikacím v kryptografii, jak ukazují některé nedávné práce C. Monica, J. Zumbärgela a dalších. V článkách R. El Bashira a T. Kepky bylo ukázáno, že každý kongruenčně jednoduchý polokruh (tj. polokruh, který má právě dvě kongruence) patří do jedné z pěti tříd. Otevřeným problémem však zůstávala otázka existence polokruhů v jedné z těchto tříd, totiž kongruenčně jednoduchých aditivně zeropotentních polokruhů, v nichž lze každý prvek vyjádřit jako součet dvou prvků.

Autor ve své disertační práci dokázal tento problém pozitivně vyřešit. Hlavním nástrojem je komplikovaná kombinatorika slov ve volném monoidu. Po krátkém úvodu je ve druhé, poměrně rozsáhlé kapitole práce vybudována teorie speciálních prepisovacích systémů, které vycházejí ze slov, která se vzájemně nepřekrývají. Ve třetí části práce je vybudovaná teorie použita ke studiu konečných maximálních oddělujících množin slov se dvěma generátory. Ve čtvrté, závěrečné části práce autor podává jistou metodu konstrukce aditivně zeropotentních polokruhů, která umožňuje vyřešit výše zmíněný zásadní problém.

Práce je pěkně a přehledně sepsána standardním matematickým způsobem, dobře se čte. Důkazy jsou jasně formulovány, rovněž jazyková úroveň práce je slušná. Práce také obsahuje jen velmi málo překlepů, kuriózní je však překlep přímo na českém titulním listě, kde je uvedeno „Kongruenčně jednoduché polookruhy a polomoduly“. Zdá se mi rovněž poněkud neobvyklé, že důkaz neprázdnosti výše zmíněné třídy kongruenčně jednoduchých polokruhů, což je vlastně hlavní výsledek práce, je formulován pouze v poznámkovém textu za Propozicí 4.2.10. Celkově práci hodnotím jako velmi kvalitní.

Na závěr mohu konstatovat, že disertační práce Mgr. Václava Flašky „Congruence-simple semirings and semimodules“ jednoznačně prokazuje předpoklady autora k samostatné tvořivé práci a doporučuji proto, aby po úspěšné obhajobě byl panu Mgr. Václavu Flaškovi udělen titul Ph.D.

V Praze dne 24. července 2008



Prof. RNDr. Ing. Petr Němec, DrSc.

katedra matematiky TF ČZU
Kamýcká 129
165 21 Praha 6 - Suchbátka