Posudek vedoucího na bakalářskou práci

Adam Beran: Eliptické křivky nad konečnými tělesy

Práce se zabývá základními vlastnostmi eliptických křivek nad konečnými tělesy charakteristiky různé od 2 a 3. Zaměřuje se především na podrobné důkazy následujících faktů:

1. důkaz asociativity grupové operace na eliptické křivce,
2. Hasseho věta (odhad na počet bodů na křivce).

I když je práce kompilační a jde o známé výsledky, jejich důkazy jsou značně netriviální a jdou nad rámec bakalářského studia. Autor navíc pracoval velice samostatně a potřebné doplňující zdroje si z velké části dohledal sám.

V případě důkazu asociativity zvolil autor ne příliš obvyklou cestu spočívající v tom, že jde vlastně o to porovnat dva polynomy v celkem konkrétním faktorokruhu okruhu polynomů. I když jde o důkaz z povahy věci velice přirozený (grupová operace je racionální zobrazení) a vlastně přímočarý, dotčené polynomy mají tolik členů, že bylo nutné několik výpočtů provést na počítači. Dalším problémem, který autor pečlivě ošetřil, je nepříjemné rozebírání speciálních případů, kdy se někde ve výrazech $(P_1 + P_2) + P_3$ a $P_1 + (P_2 + P_3)$ vyskytne součet dvou stejných prvků, protože v tomto případě je nutné použít pro sčítání jiný vzorec.

V případě Hasseho věty autor podal takřka úplný důkaz, kde z prostorových důvodů bez důkazu citoval jen tvrzení o stupni lineární kombinace automorfismů eliptické křivky (tvrzení 23). Důkaz je veden pečlivě a je z něj dobře vidět hlavní myšlenka.

Práci považuji za velice zdařilou, **doporučuji ji k obhajobě** a návrh hodnocení přikládám zvlášť.

V Praze dne 28. 8. 2018 doc. RNDr. Jan Šťovíček, Ph.D.