Posudek oponenta bakalářské práce

Název: Eliptické křivky nad konečnými tělesy
Autor: Adam Beran

Shrnutí obsahu práce

Práce Adama Berana je věnována důkazu asociativity grupové operace a odhadu počtu bodů na nesingulární eliptické křivce nad konečným tělesem charakteristiky různé od dvou a tří. Text práce se skládá vedle motivačního úvodu a závěru ze tří kapitol, které obsahují geometrické zavedení grupové operace na nesingulární eliptické křivce a podrobné důkazy asociativity a Hasseovy věty. Součástí práce je zdrojový kód spolu s výpočtem porovnání racionálních výrazů v programu Mathematica, který tvoří jádro matematicky elementárního, ovšem výpočetně náročného ověření asociativního zákona.

Celkové hodnocení práce

Téma práce. Téma bylo sice poměrně obtížné avšak velmi zajímavé a svým charakterem vhodné pro zpracování v bakalářské práci. Zadání bylo studentem podle mého mínění bezezbytku naplněno.

Vlastní příspěvek. Práce je kompilací několika zdrojů doplněná o netriviální detaily a především o kód programu a jím provedený výpočet ověřující platnost Lemmat 3, 4 a 5, jež tvoří základ důkazu asociativity grupové operace na eliptické křivce.

Matematická úroveň. Matematická úroveň práce je vysoká, formulace jsou korektní a důkazy velmi pečlivě sepsané.

Práce se zdroji. Text práce zpracovává a doplňuje teorii převzatou několik zdrojů a bezpochyby na nich není formulačně závislý.

Formální úprava. Po formální stránce nezasluhuje práce žádnou výtku. Jazykových nepřesností je v textu velmi málo a výsledný text je velmi čtivý.

Připomínky a otázky

1. s.3, Definice 1 - Formulace „L je těleso splňující $K \subseteq L$ není příliš přesná, raději bychom měli říci, že L je nadtěleso tělesa K.
2. s.7 - Korektnost pojmu tečna v bodě a její nalezení pomocí implicitní derivace by nad obecným tělesem myslím stálo za obsáhlejší diskusi.

Závěr Práce podle mého názoru splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
4.9.2018