Posudek oponenta k diplomové práci
Tateova-Šafarevičova grupa a eliptické křivky
Adama Zvěřiny

Struktura grupy bodů na eliptické křivce patří k hlavním tématům v teorii čísel i algebraické geometrii. Pro eliptické křivky nad tělesem racionálních čísel je známo, že je tato komutativní grupa konečně generovaná (Mordellova-Weilova věta). Zatímco torzní podgrupa této grupy je až na izomorfismus značně omezena Mazurovou větou a lze ji algoritmicky spočítat (viz příklady na str. 11 a 12) otázky ohledně ranku této grupy (včetně algoritmu pro jeho výpočet) jsou z velké části otevřené problémy.

Hlavním cílem práce bylo zavedení Tateovy-Šafarevičovy grupy racionální eliptické křivky. Tato grupa do určité míry vyjadřuje neplatnost Hasseho-Minkowského principu (který platí na kvadrikách) pro danou eliptickou křivku.

Tateova-Šafarevičova grupa je definována přes grupovou kohomologii profinitní grupy $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$. Základní poznatky z teorie profinitních grup jsou součástí druhé kapitoly práce.

Závěrečná kapitola je pak věnována verzím Birchovy-Swinnerton-Dyerovy hypotézy dávající mimo jiné do souvislosti rank grupy bodů eliptické křivky a chování analytického prodloužení L-funkce eliptické křivky v okolí jedničky.

Studované téma je velmi náročné a tomu odpovídá i způsob zpracování. S výjimkou druhé kapitoly autor neuvádí žádné důkazy a práce tak místy připomíná spíše přehledový článek k danému tématu. Z předloženého textu nelze příliš posoudit, jak hluboko do dané problematiky autor vlastně pronikl.

Po formální stránce je práce napsaná pečlivě, množství překlepů je zanedbatelné. Některé konkrétní připomínky uvádím v seznamu níže.

V zásadě lze říct, že autor splnil zadání práce, ačkoliv některá témata ze zadání práce (např. kohomologie profinitních grup) nebyla zpracována. Práci doporučuji uznat jako práci diplomovou.

V Praze 2. 2. 2023

Pavel Příhoda

Konkrétní připomínky

- Definice 2: Pokud předpokládáme, že eliptická křivka je nesingulární, měla by být podmínka $4a^3 + 27b^2 \neq 0$ v definici.
- str. 5: Úvahy ohledně Hilbertovy věty o nulách: Nepotřebujeme algebraicky uzavřené těleso?
- Definice 4: Vzhledem k Definici 6 bych očekával f_1, f_2 racionální.
- str. 11, dole: Každá šestiprvková komutativní grupa je isomorfní $\mathbb{Z}/6\mathbb{Z}$.

- str. 14: V definici T_k jsou prohozeny U a V.
- Věta 13, implikace (1) $\rightarrow$ (3) předpoklad nesouvislosti dvouprvkové množiny mi přijde málo - je splněn v každém Hausdorffově prostoru.
- str. 16: Proč jsou množiny Y^i otevřené?
- Definice 26: Pojem hladké křivky není zaveden. Přijde mi, že práce používá jiné značení než citovaná Silvermanova kniha, což je přinejmenším matoucí.
- Definice 27: Apriori není jasné, že jsou všechny akce E na E isomorfní. Bylo by na místě říct, že triviální je třída, která obsahuje akci E na E translací.
- Přijde mi, že kapitola 3.2 je zcela klíčová. Uvedený příklad s křivkou $y^2 = (x - e_1)(x - e_2)(x - e_3)$ je nepochybně zajímavý, ale je to už trochu nadstavba. Elementárnější příklad (pokud existuje), případně podrobnější komentáře k definicím by jistě přispěly ke srozumitelnosti textu.
- str. 32: Třetí a čtvrtý odstavec jsou stejné.