Posudek školitele na diplomovou práci

Adam Zvěřina: Tateova-Šafarevičova grupa eliptické křivky

Cílem práce práce bylo představit Tateovu–Šafarevičovu grupu racionální eliptické křivky, která měří, nakolik pro eliptickou křivku selže lokální–globální princip (analogie Hasseho–Minkowského věty pro kvadratické formy). Řád Tateovy–Šafarevičovy grupy (o kterém se stále v obecnosti neví, jestli je konečný) vystupuje též v Birchově–Swinnerton-Dyerově domněnce, což je jeden z Millennium Problems, na jejichž vyřešení je vypsána odměna ve výši milion dolarů, a kterou chtěl autor práce též lépe pochopit. Je zřejmé, že téma je hodně náročné, proto práce byla od začátku plánována jako převážně kompilační s tím, že budou doplněny detaily a rozpracovány příklady.

Autor však práci pojal trochu více přehledově, než jsem očekával. Z tohoto pohledu je sepsaná velice pěkně a orientaci ohledně stavu kolem Tateovy-Šafarevičovy grupy a Birchovy–Swinnerton-Dyerovy domněnky autor studiem různých zdrojů získal dobrou, ale do detailu jde práce i v případech, kdy by to stále bylo technicky únosné, poměrně zřídka. Nad rámec kompilace tak jde především o rozpracování příkladů a důkazů základních faktů v úvodních dvou kapitolách.

Zde je několik nedotažených míst a faktických nepřesností, které přes všechnu péči v práci zůstaly:

1. Definice 4 úplně neodpovídá pozdějšímu použití, kde jsou zobrazení mezi křivkami často zadána pomocí racionálních funkcí. U těch pak není úplně triviální záležitost dodefinovat takové zobrazení v pólech některé z funkcí, byť to jde: je známo, že každé racionální zobrazení mezi projektivními nesingulárními křivkami jde v těchto bodech přirozeně dodefinovat.

2. Kapitola 1.3 vůbec neřeší nesingularitu (nebo též hladkost) křivky C, která je potřeba, už kvůli předchozí poznámce (když chceme pomocí racionálních funkcí definovat isomorfismus) a také proto, že kdyby C měla singularity, těžko bude isomorfní nesingulární eliptické křivce ve Weierstrassově normálním tvaru. Tady bych podotknul, že v definici 22 na straně 25 je hladkost výslovně požadována, ale zase tam není vysvětleno, co ten pojem přesně znamená.

3. Důkaz na str. 15 implikace $1 \implies 3$ věty 13 je špatně. Singletony $\{x\}$ a $\{y\}$ jsou sice obojetné množiny v dvouprvkovém podprostoru $\{x, y\}$, ale už ne nutně v celém prostoru X, jak se v podmínce 3 požaduje. Ona totiž tato implikace za uvedených předpokladů ani dokázat nejde,

protože neplatí. Platila by např., pokud bychom předpokládali, že X je kompaktní (nebo obecněji lokálně kompaktní) prostor.

4. Uprostřed strany 23 se tvrdí bez dalšího komentáře, že křivky $C_{a,b,c}$ a E jsou isomorfní. To vůbec není zjevné a například na str. 27 je později naznačeno, jak by mohl takový isomorfismus vypadat. To by bývalo stálo za zmínku.

5. Na str. 25 by v definici homogenního prostoru mělo být všude $E(\overline{K})$ (nebo prostě jenom E) místo $E(K)$. Stejně tak na str. 26 ve znění věty 29 má být $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))$.

Na závěr ještě uvádím několik nalezených překlepů:

- str. 6, řádek -9: pod složenou závorkou má být m místo n,
- str. 6, řádek -4: definiční obor zobrazení $[\cdot]$ by asi měl být $\mathbb{Z} \setminus \{0\}$, abychom byli konzistentní s def. 6,
- str. 7, řádek 7: fráze „obecně platí“ naznačuje, že průnik každé dvojice kvadrik je eliptická křivka, což není pravda (musí být v obecné poloze, což znamená, že nesmí být shodné a průnik musí být nesingulární),
- str. 7, řádek -3: špatná rovnice plochy, se kterou C pronikáme,
- str. 8, poslední dva řádky: žádná křivka E tady nebyla zmíněna, ta se objevuje až na str. 23,
- str. 11, první příklad: ve výpočtu se používá nejen, že $y|108$, ale dokonce, že $y^2|108$,
- str. 14, definice T_k v důkazu věty 10: jsou prohozeny U a V,
- str. 17, druhá polovina důkazy věty 18: místo H' by mělo být N',
- str. 32: duplikovaný odstavec.

Práci **doporučuji k obhajobě** a návrh hodnocení sdělím přímo komisi.

V Praze dne 2. 2. 2023 doc. RNDr. Jan Šťovíček, Ph.D.