POSUDEK OPONENTA

Název práce: Elementární důkaz věty o primitivním prvku
Autor: Miroslav Majerčík

Zadáním bylo zpracovat důkaz věty o primitivním prvku využívající pouze elementární teorii čísel. První kapitola obsahuje (nad rámec zadání) důkaz Gaussova kvadratického zákona reciprocity, také pomocí elementárních metod. Věta o primitivním prvku je dokázána v kapitole druhé. Při zpracování student čerpal z knihy

[1] Milan Paštéka, Renata Smolíková, *Úlohy z teorie čísel*, Ostravská univerzita, Ostrava, 1996,

ve které jsou důkazy obou vět předvedeny ve formě většího množství úloh z elementární teorie čísel.

Předložená práce má 23 stran. Obsahuje 63 lemmat, z nichž převážná většina doslovně odpovídá úlohám ze sbírky [1], student doplnil důkazy (řešení úloh). (Znění některých lemmat dokonce začíná slovy *„Dokažte, že...“*) Struktura obou důkazů je tak z velké části převzatá z knihy [1].

Kromě lemmat jsou na několika místech z knihy [1] doslovně převzaty i texty definic a komentářů, například definice Legendreova symbolu (str. 2 ř. -3 až str. 3 ř. 6). Hodnota Legendreova symbolu pro násobky a je oproti [1] předefinována, čímž se ovšem definice stává nejednoznačnou.

Vlastním příspěvkem studenta je kromě vyřešení úloh z knihy [1] využití Schématu rozdílu mocnin (Věta 1) k doplnění mezery v důkazu Lemmatu 37 c) (Úloha 241 c) v [1]). Je škoda, že to nebylo v závěru vyzdvihnuto.

V předložené podobě jsou oba důkazy těžko čitelné. Dle mého názoru se měl student pokusit je lépe strukturovat, vydestilovat klíčové kroky a oddělit a seskupit kroky jednoduché až triviální.

Například znění Gaussova kvadratického zákona reciprocity, které je uvedeno na začátku první kapitoly, je po důkazu několika pomocných lemmat zopakováno v Lemmatu 15. Lemma 15 je pak dokázáno pomocí lemmat 16 až 20. Důkaz Lemmatu 16 je pouhé vynásobení dvou čísel, Lemma 17 je také triviální, lemmata 18 a 19 říkají prakticky totéž a Lemma 20 zní *„Platí lemma 15“*. Několik jednoduchých úprav vzorečků je tak rozvedeno do 6 lemmat, jejichž důkazy mají dohromady pouhých 8 řádků.

Definice nových pojmů jsou uvedeny v rámci běžného textu a nejsou nikterak zvýrazněny. Výjimkou je Definícia 1 na straně 15 (symbol pro

rozdíl mocnin). Čím si právě tento jeden pomocný symbol zasloužil vlastní definici?

Za jeden z největších nedostatků práce považuji skutečnost, že většina důkazů není psána ve formě vět, ale zkratkovitě pomocí kombinace spojek a symbolu „⇒“ (místy „→“). V některých částech práce (např. v části o Schématu rozdílu mocnin) se tento nedostatek nevyskytuje a text důkazů je podrobnější a jazykově v pořádku. Proč?

Vážným nedostatkem je také nesoulad abstraktu s textem práce. Abstrakt slibuje historické přiblížení v úvodu a také důkaz Malé Fermatovy věty. Historické přiblížení neexistuje, a místo důkazu Malé Fermatovy věty nacházíme pouze informaci, že důkazů existuje mnoho, že jsou triviální a založené teorii grup. Tím rezignujeme na „self-containedness“ důkazu Gaussova zákona, navíc Malá Fermatova věta je téměř dokázána ve druhé kapitole, při důkazu cykličnosti násobení modulo p.

Překlad abstraktu do anglického jazyka je špatný, věta *„K dôkazu týchto viet...“* je přeložena jako *„To proof this two sentences...“*

Seznam literatury obsahuje kromě knihy [1] čtyři další zdroje, vesměs starší učební texty k přednáškám na MFF UK. Tyto zdroje nejsou nikde v práci citovány a není jasné, k čemu byly použity. Naopak z práce není zřejmé, odkud student čerpal část zabývající se Schématem rozdílu mocnin.

Poněkud nešťastné je, že z práce vypadlo znění samotné Věty o primitivním prvku, druhá kapitola začíná slovem „**Znenie:**“ a vynechaným místem. Celkově práce působí dojmem, že byla psána ve spěchu a po dokončení vůbec neprošla kontrolou. Mnoho nedostatků, z nichž některé uvádím níže, mohlo být odhaleno už při zběžném pročtení. V práci také chybí velké množství teček na konci vět, zejména ve zněních lemmat a v důkazech.

Závěr: Student odvedl při řešení úloh poměrně velké množství práce, místy i matematicky netriviální. Vzhledem k závažným nedostatkům převážně formálního charakteru, k velkému množství drobných chyb a celkově nízké kvalitě zpracování je však úroveň práce nedostatečná. Proto předloženou práci **nedoporučuji uznat jako práci bakalářskou**.

V Praze dne 15. ledna 2013 Jakub Bulín

Posudek doplňuji o soupis několika drobnějších chyb:

- Text Lemmatu 51 není matematickým tvrzením, jde pouze o komentář k Lemmatu 52.
- U celkem sedmi lemmat začíná důkaz „*Dôkaz.* Dôkaz:“, podobně „**Definícia 1.** Definícia:“
- Poslední věta z důkazu Lemmatu 23 do něj již nepatří, poslední věta z Definice 1 také nemá být součástí definice.

- Lemma 29 má začínat *„Nechť platí předpoklady Lemmatu 27“*.
- V důkazu Lemmatu 37 a) má být *„Pre* $r \in \{1, \ldots, k\}$*“* místo *„Pre* $k \in \{1 \ldots k\}$*“*
- Předpoklad $\alpha \geq 1$ z komentáře na konci strany 17 je nadbytečný.