

# NI-MPI cvičení 8

## Algebra III

FIT ČVUT

Autoři: Karel Klouda, Tomáš Kalvoda, Jan Spěvák, Štěpán Starosta  
Problémy, návrhy apod. hlaste v [GitLabu](#).

Verze souboru: 2023-09-25 12:03.

### Obsah

20. Homomorfismus a izomorfismus

21. Diskrétní logaritmus

## Poznámka

Co byste si měli z tohoto cvičení odnést:

- ▶ Jak poznat homomorfismus a najít izomorfismus grup.

A co byste se měli doučit, pokud to ještě/už neumíte:

- ▶ stačí znát z přednášky definice a základní vlastnosti výše zmíněných pojmů.

## 20. Homomorfismus a izomorfismus

### Cvičení 20.1

Zjistěte, která z následujících zobrazení jsou homomorfismem a která z nich jsou izomorfismy (pro dané grupoidy).

- (a) Zobrazení  $f(n) = 3n + 2$  z grupy  $(\mathbb{Z}, +)$  do  $(\mathbb{R}, +)$ .
- (b) Zobrazení  $f(x) = 2^x$  z grupy  $(\mathbb{R}, +)$  do  $(\mathbb{R}^+, \cdot)$ .
- (c) Zobrazení  $f(A) = A_{1,1}$  z grupy reálných matic dimenze  $n \times n$  se sčítáním po prvcích  $(\mathbb{R}^{n \times n}, +)$  do  $(\mathbb{R}, +)$ .
- (d) Zobrazení  $f(A) = A_{1,1}$  z grupy regulárních reálných matic dimenze  $n \times n$  s maticovým násobením  $(\mathbb{R}_{reg}^{n \times n}, \cdot)$  do  $(\mathbb{R}, \cdot)$ .

### Cvičení 20.2

Najděte nějaký homomorfismus grupy regulárních reálných matic s maticovým násobením  $(\mathbb{R}_{reg}^{n \times n}, \cdot)$  do  $(\mathbb{R}, \cdot)$ .

### Cvičení 20.3

Je  $\mathbb{Z}_{10}^\times$  izomorfní s  $\mathbb{Z}_5^\times$ ? Pokud ano, najděte nějaký izomorfismus.

## Základní cvičení 20.4

*Pro prvočíslo  $p$  popište, jak byste našli izomorfismus grupy  $\mathbb{Z}_p^\times$  s grupou  $\mathbb{Z}_{p-1}^+$ . Kolik různých izomorfismů existuje?*

## Cvičení 20.5

*Mějme grupy  $G$  a  $H$ , kde  $G := \mathbb{Z}_5^+$  a  $H := \mathbb{Z}_{13}^\times$ . Nalezněte všechny homomorfismy z  $G$  do  $H$  a zdůvodněte, že jsou všechny.*

## Cvičení 20.6

*Bud'  $\varphi : G \rightarrow H$  nějaký homomorfismus grup  $G = \mathbb{Z}_{12}^+$  a  $H = \mathbb{Z}_6^+$ . Ukažte, že  $\varphi(4) \neq 5$ .*

## 21. Diskrétní logaritmus

### Cvičení 21.1

Vyřešte rovnici

$$5^x \equiv 12 \pmod{23}.$$

### Cvičení 21.2

*Anastázie chce předat Bořivojovi tajnou zprávu během hodiny dějepisu a tak Bořivojovi naprosto veřejně pošle papírek říkající: „Bořivoji, něco Ti pošlu a použiji Diffie-Hellmana. Můj veřejný klíč je prvočíslo 29, generátor 8 a vypočítané číslo 24“. Bořivoj na to: „Jasně, Anastázie, moje je 15“. Anastázie: „Super, je-li  $n$  naše sdílené tajemství, tak se sejdemé  $(n - 2 \pmod{7})$ -tý den příštího týdne v  $n - 7$  hodin na hřbitově u hrobu číslo  $5n + 6$ . Tož zatím!“ Kdy a kde se Anastázie a Bořivoj setkají?*