Teorie čísel: Cvičení 10

25. dubna 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@gmail.com

Definice: Grupa $(G, \cdot, ^{-1}, 1)$ se nazývá *cyklická*, pokud existuje prvek $g \in G$ takový, že $\langle g \rangle = G$, čili g generuje celou grupu G (tedy pro každé $h \in G$ existuje $n \in \mathbb{Z}$ splňující $g^n = h$). (Upozornění: Ve sčítacích grupách píšeme přirozeně $ng = h$ místo $g^n = h$.)
Poznámka: Množina $\mathbb{Z}_n = \{0, \ldots, n-1\}$ zbytků po dělení n přirozeně tvoří grupu $(\mathbb{Z}_n, +, -, 0)$. Když píšeme grupa $\mathbb{Z}_n$, myslí se tím vždy sčítací grupa (pokud není řečeno jinak).

Pokud nás zajímá grupa zbytků modulo n s násobením (značíme ji $\mathbb{Z}_n^*$), pak její nosná množina obsahuje právě ty prvky, které mají inverzní prvek (z Algebry byste měli vědět, že jsou to právě prvky $a \in \mathbb{Z}_n$, pro které $NSD(a, n) = 1$).
Definice: Nechť $n \geq 2$. Pokud je $\mathbb{Z}_n^*$ cyklická, tak se její libovolný generátor nazývá primitivní prvek modulo n. (Na přednášce se brzo dokáže, že primitivní prvek existuje právě když $n = p^k$ nebo $n = 2p^k$ pro liché prvočíslo p, nebo $n = 2, 4$.)
Definice: Nechť $(G, \cdot, ^{-1}, 1)$ a $(H, *, ', e)$ jsou grupy. Zobrazení $\varphi : G \to H$ je *homomorfismus grup* G a H, pokud pro všechny $a, b \in G$ platí $\varphi(g \cdot h) = \varphi(g) * \varphi(h)$. (Z Algebry víme, že pak $\varphi(1) = e$ a $\varphi(a^{-1}) = \varphi(a)'$.) Zobrazení definované $\varphi(g) = e$ pro všechny $g \in G$ je vždy homomorfismus, nazývá se *triviální homomorfismus*. Bijektivní homomorfismus se nazývá *izomorfismus*.

-2. Najděte všechny generátory grupy $\mathbb{Z}_{12}$.

-1. Najděte všechny homomorfismy následujících grup:
   (a) Ze $\mathbb{Z}_3$ do $\mathbb{Z}_6$.
   (b) Ze $\mathbb{Z}_5$ do $\mathbb{Z}_6$.

0. Rozhodněte, zda jsou grupy $\mathbb{Z}_{11}^*$ a $\mathbb{Z}_8^*$ cyklické a pokud ano, najděte v nich nějaký primitivní prvek.

1. Rozmyslete si následující fakty o generátorech grup $\mathbb{Z}_n$:

! (a) Najděte všechny generátory grupy $\mathbb{Z}_{18}$.
   (b) Které prvky $\mathbb{Z}_n$ nemohou generovat celou grupu $\mathbb{Z}_n$?
   (c) Popište všechny generátory grupy $\mathbb{Z}_n$. (Nápověda: Bézoutovy koeficienty)

! 2. Rozhodněte, zda jsou následující zobrazení homomorfismy grup:
   (a) $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_3$, $\varphi(a) = a \bmod 3$
   (b) $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_3$, $\varphi(a) = a \bmod 3$

! 3. Najděte všechny homomorfismy následujících grup:
   (a) Ze $\mathbb{Z}_4$ do $\mathbb{Z}_8$.
   (b) Ze $\mathbb{Z}_4$ do $\mathbb{Z}_6$.
   (c) Ze $\mathbb{Z}_4$ do $\mathbb{Z}_7$.

! 4. Určete řády všech prvků v grupách $\mathbb{Z}_7$ a $\mathbb{Z}_7^*$.

! 5. Rozhodněte, které z grup $\mathbb{Z}_5^*$, $\mathbb{Z}_6^*$, $\mathbb{Z}_9^*$, $\mathbb{Z}_{12}^*$ jsou cyklické.

! 6. Víme, že pro každé prvočíslo p existuje primitivní prvek modulo p.
   (a) Najděte nějaký primitivní prvek modulo 3, 5 a 7.
   (b) Pomocí části a) sestrojte izomorfizmus grup $\mathbb{Z}_7^*$ a $\mathbb{Z}_6$.

7. Uvažujme grupu $\mathbb{Z}_p^*$, kde p je prvočíslo.
   (a) Najděte všechny prvky této grupy. Kolik jich je?
   (b) Víme, že tato grupa je cyklická, označme nějaký její generátor a. Jaký řád má a v grupě $\mathbb{Z}_p^*$?
   (c) Najděte izomorfizmus grupy $\mathbb{Z}_p^*$ a grupy $\mathbb{Z}_{p-1}$. (Nápověda: Generátor a grupy $\mathbb{Z}_p^*$ se musí zobrazit na nějaký generátor grupy $\mathbb{Z}_{p-1}$.)

8. Najděte všechny primitivní prvky modulo 7.

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.
Úlohy s ! je doporučeno řešit přednostně.
Úlohy s $*$ jsou náročnější.