## 8. Cyklické grupy

**1.** Dokažte, že každá grupa prvočíselného řádu $p$ je izomorfní Abelově grupě $\mathbb{Z}_p$.

**2.** Buďte $0 < m < n$ celá čísla a uvažte endomorfismus $\psi : a \to ma$ grupy $\mathbb{Z}_n(+,-,0)$. Popište $\operatorname{Ker}\psi$ a $\ker\psi$. Jaký je řád $\operatorname{Ker}\psi$? Charakterizujte $\operatorname{Im}\psi$.

**3.** Označme $I_n$ množinu všech invertibilních prvků $\mathbb{Z}_n$. Pak na $I_n$ můžeme hledět jako na multiplikativní grupu. Ukažte, že $I_n \simeq \operatorname{Aut}(\mathbb{Z}_n)$ a $\mathbb{Z}_n(\cdot,1) \simeq \operatorname{End}(\mathbb{Z}_n)$.

**4.** Nalezněte $n$ takové, že $I_n$ je izomorfní Kleinově grupě.

**5.** Nalezněte $n, m \in \mathbb{N}$ taková, že $I_n \simeq I_m$ a $n > m > 2$.

**6.** Dokažte, že grupa, která obsahuje podgrupu izomorfní Kleinově grupě, není cyklická.

**7.** Dokažte, že není $I_{32} \simeq I_{17}$, ačkoliv $|I_{32}| = |I_{17}|$.

**8.** Dokažte, že pro každé $n \geq 3$ obsahuje $I_{2^n}$ podgrupu izomorfní Kleinově grupě.

**9.** Pro $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$ zkoumejte množinu $M$ řešení kongruenční rovnice

$$ax \equiv b \bmod n.$$

Dokažte:

(i) Je-li $c \in M$, je $[c]_n \subseteq M$.
(ii) Je-li $NSD(a,n) = 1$, tak $M \in \mathbb{Z}/n\mathbb{Z}$.
(iii) Jestliže $NSD(a,n)$ nedělí $b$, tak $M = \emptyset$.
(iv) Jestliže $k \in \mathbb{N}$ dělí $a$, $b$ i $n$, tak $M$ se shoduje s množinou řešení kongruenční rovnice $a'x \equiv b' \bmod n'$, kde $a = a'k$, $b = b'k$ a $n = n'k$.
(v) Je-li $NSD(a,n) = 1$, tak $M = [a^{\varphi(n)-1}b]_n$

**10.** V $\mathbb{Z}_{21}$ vyřešte rovnice $6x = 9$ a $5y = 8$.

**11.** Buď $1 \leq r \leq s \leq n$ celá čísla, jež dělí $n \in \mathbb{N}$. Dokažte, že $(r\mathbb{Z}_n) \cup (s\mathbb{Z}_n) \subseteq NSD_{\mathbb{N}}(r,s)\mathbb{Z}_n$ a $(r\mathbb{Z}_n) \cap (s\mathbb{Z}_n) = NSN_{\mathbb{N}}(r,s)\mathbb{Z}_n$.

**12.** Dokažte, že v $\mathbb{Z}_n$, $n \in \mathbb{N}$, je každé $a \in \mathbb{Z}_n$ asociované právě s jedním dělitelem $n$. Jsou-li $r, s \in \mathbb{Z}_n$ dva nenulové dělitele $n$, dokažte, že $NSD_{\mathbb{Z}_n}(r,s) = NSD_{\mathbb{N}}(r,s)$ a $NSN_{\mathbb{Z}_n}(r,s) = NSN_{\mathbb{N}}(r,s)$ (aby poslední vztah platil formálně přesně, je někdy nutné ztotožnit $n$ a 0).

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

## Řešení

**1.** Ať $|G| = p$ a $a \in G$, $a \neq \mathbf{1}$. Pak $a$ generuje cyklickou grupu, jejíž řád dělí $|G| = p$. Tudíž $a$ generuje $G$.

**2.** Ať $k = NSD_{\mathbb{N}_0}(m, n)$. Pak $\operatorname{Im}\psi = k\mathbb{Z}_n$, $|\operatorname{Ker}\psi| = k$, $\operatorname{Ker}\psi = r\mathbb{Z}_n$, kde $n = kr$, a $\psi(a) = \psi(b)$ právě když $r$ dělí $a - b$.

**3.** Ať $\psi_a \in \operatorname{End}(\mathbb{Z}_n)$ označuje endomorfismus $i \to ai$. Pak hledané izomorfismy jsou dány přiřazením $a \to \psi_a$.

**4.** $n = 8$.

**5.** Například $n = 6$ a $m = 3$.

**6.** Cyklická grupa obsahuje jediný prvek řádu 2.

**7.** $I_{17}$ je cyklická (3 je jeden z generátorů). Na druhé straně $\{1, 15, 17, 31\}$ je podgrupa grupy $I_{32}$, která je izomorfní Kleinově grupě.

**8.** $\{1, 2^{n-1} - 1, 2^{n-1} + 1, 2^n - 1\}$.

**10.** $x \in \{5, 12, 19\}$, $y = 10$.

**11.** Obě situace lze pomocí $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(a) = a \bmod n$, převést do $\mathbb{Z}$.

**12.** Invertibilní prvky $\mathbb{Z}_n$ jsou nenulové prvky, které jsou s $n$ nesoudělné. Každý prvek $\mathbb{Z}_n$ lze napsat jako součin invertibilních prvků a dělitele $n$. Proto je každé $a \in \mathbb{Z}_n$ asociováno s jediným dělitelem $n$. Při úvahách o $NSD$ a $NSN$ v $\mathbb{Z}_n$ se tedy lze omezit na dělitele $n$.