4. cvičení - řešení příkladů:

1) Hledáme podgrupy:
   a) $(\mathbf{Z}, +)$: triviální podgrupy $\{0\}$, $\mathbf{Z}$
      - hledáme další podgrupy: předpokládáme, že existuje nějaké číslo $k \in \mathbf{Z}$, $k \neq 1$ (jinak by generovalo $\mathbf{Z}$), $k \neq 0$ (jinak by generovalo $\{0\}$), $\{k\}$ generuje podgrupu H, přitom $H \neq \{0\}$, $H \neq \mathbf{Z}$
      - tedy $\mathbf{H}$ je obecně vždy **podgrupa násobků nějakého čísla $k \in \mathbf{Z}$**, např. pro $k = 2$ máme $\{2, 4, 6, 8, -2, -4, -6, \ldots\}$
      - pokud $k = 0$, pak jeho násobky generují $\{0\}$
      - pokud $k = 1$, pak jeho násobky generují $\mathbf{Z}$
      - důkaz si můžete prohlédnout zde:

Zřejmě $\{0\}$ a $\mathbb{Z}$ jsou podgrupy grupy $(\mathbb{Z},+)$. Nechť $\{0\}\neq H\neq\mathbb{Z}$ je podgrupa grupy $(\mathbb{Z},+)$. Pak $1\notin H$ (jinak by $H=\mathbb{Z}$), a protože $H\neq\{0\}$, existuje $h\in H$ takové, že $1\neq h>0$. Zvolme za k nejmenší přirozené číslo různé od 1, které patří do H. Ukážeme, že H je generovaná množinou $\{k\}$. Jestliže $m\in H$, pak $m=q\cdot k+r$ kde $q,r\in\mathbb{Z}$ a platí $0\leq r<k$. Jelikož $m\in H$, $k\in H$, pak také $q\cdot k=k+k+\ldots+k$ (q-krát) patří do H, a tedy také $r=m-q\cdot k\in H$. Avšak $r<k$. Jelikož k je nejmenší přirozené číslo z H, je tedy $r=0$. Neboli $m=q\cdot k$, t.j. $m=k+\ldots+k$ (q-krát). Tedy každé $m\in H$ lze vygenerovat pomocí k, t.j. $\{k\}$ generuje H. Tedy každá podgrupa grupy $(\mathbb{Z},+)$ je množinou všech násobků některého čísla $k\in\mathbb{Z}$ (pro $\{0\}$ je $k=0$, pro $\mathbb{Z}$ je $k=1$).

   b) $(\mathbf{Z}_6, +)$: triviální podgrupy $\{0\}$, $\mathbf{Z}_6$
      - další podgrupy vygenerujeme pomocí dělitelů čísla 6:
      - 2 generuje podgrupu $\{0, 2, 4\}$
      - 3 generuje podgrupu $\{0, 3\}$
   c) $(\mathbf{Z}_7, +)$ má pouze triviální podgrupy $\{0\}$ a $\mathbf{Z}_7$, – jedná se totiž o grupu prvočíselného řádu.
2) Minule jsme nalezli těchto šest podgrup:
   $\{id\}, \{id, o_1\}, \{id, o_2\}, \{id, o_3\}, \{id, r_1, r_2\}, \{id, o_1, o_2, o_3, r_1, r_2\}$
      - pro všechny prvky a z G chceme ověřit, že $a \circ H = H \circ a$:

   {id}:
   jelikož id je jednotkou grupy, pro každý prvek $a \in G$ platí $a \circ id = id \circ a = a$.
   Tedy nutně $H_l = \{id, o_1, o_2, o_3, r_1, r_2\} = H_p$, tzn. $\{id\}$ je normální podgrupa.

$\{id, o_1\}$:
$o_2 \circ \{id, o_1\} = \{o_2, r_2\} = H_l$
$\{id, o_1\} \circ o_2 = \{o_2, r_1\} = H_p$
⇨ $H_l \neq H_p$, tedy $\{o_1, id\}$ není normální podgrupa.

$\{id, o_2\}$:
$o_1 \circ \{id, o_2\} = \{o_1, r_1\} = H_l$
$\{id, o_2\} \circ o_1 = \{o_1, r_2\} = H_p$
⇨ $H_l \neq H_p$, tedy $\{id, o_2\}$ není normální podgrupa

$\{id, o_3\}$:
$o_1 \circ \{id, o_3\} = \{o_1, r_2\} = H_l$
$\{id, o_3\} \circ o_1 = \{o_1, r_1\} = H_p$
⇨ $H_l \neq H_p$, tedy $\{id, o_3\}$ není normální podgrupa

$\{id, o_1, o_2, o_3, r_1, r_2\}$:

- jelikož skládáním jakéhokoliv prvku s množinou $\{id, o_1, o_2, o_3, r_1, r_2\}$ získáme opět tuto množinu (nutná podmínka grupy – pamatujeme si, že v Cayleyho tabulce se musí každý prvek vyskytnout v každém sloupci či řádku právě jednou), musí pro všechny prvky platit $H_l = H_p$ a tedy se jedná o normální podgrupu.

$\{id, r_1, r_2\}$:

$id \circ \{id, r_1, r_2\} = \{id, r_1, r_2\}$	$\{id, r_1, r_2\} \circ id = \{id, r_1, r_2\}$
$o_1 \circ \{id, r_1, r_2\} = \{o_1, o_2, o_3\}$	$\{id, r_1, r_2\} \circ o_1 = \{o_1, o_2, o_3\}$
$o_2 \circ \{id, r_1, r_2\} = \{o_1, o_2, o_3\}$	$\{id, r_1, r_2\} \circ o_2 = \{o_1, o_2, o_3\}$
$o_3 \circ \{id, r_1, r_2\} = \{o_1, o_2, o_3\}$	$\{id, r_1, r_2\} \circ o_3 = \{o_1, o_2, o_3\}$
$r_1 \circ \{id, r_1, r_2\} = \{r_1, r_2, id\}$	$\{id, r_1, r_2\} \circ r_1 = \{r_1, r_2, id\}$
$r_2 \circ \{id, r_1, r_2\} = \{r_1, r_2, id\}$	$\{id, r_1, r_2\} \circ r_1 = \{r_1, r_2, id\}$

⇨ pro všechny prvky platí $H_l = H_p$, tedy se jedná o normální podgrupu

3) Více než jeden generátor má např. grupa $(\mathbf{Z}_4, \oplus)$ s generátory 1 a 3:
$1 \oplus 1 = 2, (1 \oplus 1) \oplus 1 = 3, (1 \oplus 1) \oplus (1 \oplus 1) = 0, 1 = 1 => 1$ je generátor
$3 \oplus 3 = 2, (3 \oplus 3) \oplus 3 = 1, (3 \oplus 3) \oplus (3 \oplus 3) = 0, 3 = 3 => 3$ je generátor

Dalším příkladem je např. grupa $(\mathbf{Z}_5, \oplus)$ s generátory 1, 2, 3, 4 (ověřte).

4) $(\mathbf{Z}, +)$ – v případě, že nemáme dodefinovanou operaci – (odečítání, chápáno jako inverzní operace k operaci +), neexistuje jednoprvkový generátor.
V případě, že operaci – dodefinovanou máme, existují právě dva jednoprvkové generátory: 1 a -1.

5) a_1: řád 1, generuje podgrupu $\{a_1\}$
a_2: řád 2, generuje podgrupu $\{a_1, a_2\}$
a_3: řád 2, generuje podgrupu $\{a_1, a_3\}$
a_4: řád 2, generuje podgrupu $\{a_1, a_4\}$
a_5: řád 3, generuje podgrupu $\{a_1, a_5, a_6\}$
a_6: řád 3, generuje podgrupu $\{a_1, a_5, a_6\}$

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_5	a_6	a_3	a_4
a_3	a_3	a_6	a_1	a_5	a_4	a_2
a_4	a_4	a_5	a_6	a_1	a_2	a_3
a_5	a_5	a_4	a_2	a_3	a_6	a_1
a_6	a_6	a_3	a_4	a_2	a_1	a_5

6) Výčtem několika prvních prvků zapíšeme podgrupy H_1 a H_2:
$H_1 = \langle 4 \rangle = \{4, 8, 12, 16, 20, 24, 28, \ldots\}$
$H_2 = \langle 6 \rangle = \{6, 12, 18, 24, 30, 36, \ldots\}$

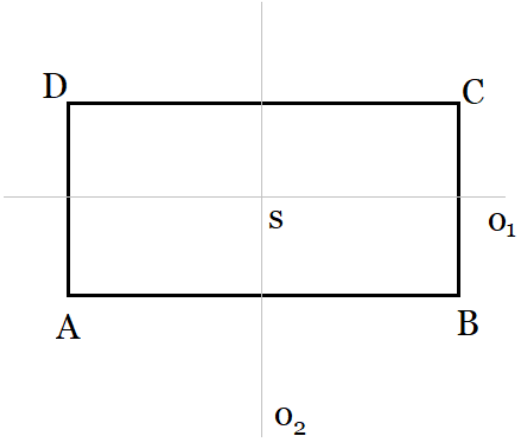
Vidíme, že průnik H_1 a H_2 je generovaný nejmenším společným násobkem generátorů, tzn. $H_1 \cap H_2 = \langle 12 \rangle = \{12, 24, 36, 48, \ldots\}$.

7) a) Tušíme, že levé a pravé třídy rozkladu se rovnají pro všechny prvky, jelikož operace + je komutativní na $\mathbf{Z}$.
Máme podgrupu $H = \{5, -5, 10, -10, 15, -15, \ldots\}$.
$a + H = \{1, 6, -4, 11, -9, 16, -14, \ldots\}$ pro $a = 1, 6, 11, 16, -4, -9, \ldots$
$a + H = \{2, 7, -3, 12, -8, 17, -13, \ldots\}$ pro $a = 2, 7, -3, 12, -8, -13, \ldots$
$a + H = \{0, 5, -5, 10, -10, 15, -15, \ldots\}$ pro $a = 0, 5, 10, 15, -5, -10, \ldots$
Celkem takto vznikne 5 tříd rozkladu daných výsledkem operace a modulo 5 (vyzkoušejte).

b) Máme čtyři zákrytové pohyby:

id – identita, o1, o2 – otočení kolem os souměrnosti, s – otočení kolem středu o 180°

- je dána podgrupa $H = \{id, o_1\}$



Jsou dány čtyři třídy rozkladu:
$id \circ \{id, o_1\} = \{id, o_1\} = \{id, o_1\} \circ id$
$s \circ \{id, o_1\} = \{s, o_2\} = \{id, o_1\} \circ s$
$o_1 \circ \{id, o_1\} = \{o_1, id\} = \{id, o_1\} \circ o_1$
$o_2 \circ \{id, o_1\} = \{id, s\} = \{id, o_1\} \circ o_2$

Vidíme, že levé a pravé třídy rozkladu se rovnají, zřejmě je tedy operace skládání zobrazení obdélníka komutativní (na rozdíl např. od skládání zobrazení rovnostranného trojúhelníka).

8) Při důkazu vycházíme z definic:
Pro cyklickou grupu $(G, \cdot)$ platí, že je generována nějakým svým prvkem (můžeme jej označit a), tedy všechny prvky G lze vyjádřit jako a^n pro nějaké $n \in \mathbf{N}$.
Pro všechny prvky $x, y \in G$ abelovské grupy musí platit rovnost $x \cdot y = y \cdot x$.
Jelikož $x = a^m$ a $y = a^n$ pro nějaké $m, n \in \mathbf{N}$, pak $x \cdot y = a^m \cdot a^n = a^{(m+n)}$.
Zároveň pak $y \cdot x = a^n \cdot a^m = a^{(n+m)} = a^{(m+n)}$. Tímto jsme dokázali, že $x \cdot y = y \cdot x$ pro všechna $x, y \in G$ a každá cyklická grupa musí být nutně abelovská.

9) Řádem $k \in \mathbf{N}$ prvku a rozumíme nejmenší mocninu takovou, že $a^k = e$.
Řádem n grupy $(G, \cdot)$ rozumíme počet jejích prvků, tedy $|G|$.
Cyklická grupa je grupa generovaná jedním svým prvkem, označme jej a.
Provedeme důkaz pomocí dvou směrů implikace:
<=

Víme, že prvek a řádu n generuje n-prvkovou podgrupu grupy $(G, \cdot)$. Jelikož ale $|G| = n$, prvek a musí nutně generovat celou grupu a $(G, \cdot)$ je tedy cyklická.
=>
Jestliže $(G, \cdot)$ je cyklická a má řád n, znamená to, že musí být celá generovaná nějakým prvkem (označíme jej a). Aby prvek a generoval celou grupu, musí být také řádu n. Důkaz je hotový.

10) Zobrazení f z $(G, \circ)$ do $(H, *)$ je homomorfismem právě tehdy, když pro všechny prvky $a, b \in G$ platí, že $f(a) * f(b) = f(a \circ b)$:

a) je homomorfismus, jelikož $3a + 3b = 3(a+b)$
b) není homomorfismus, jelikož $5(a+1) + 5(b+1) = 5(a+b+2) \neq 5(a+b+1)$
c) není homomorfismus, jelikož rovnice $a^2 + b^2 = (a+b)^2$ obecně neplatí
d) není homomorfismus, jelikož $f(a) + f(b) = 1 + 1 \neq 1 = f(a+b)$
e) je homomorfismus, jelikož $f(a) + f(b) = 0 + 0 = 0 = f(a+b)$