7. přednáška, 14. 11. 2023

5.4. Podgrupy aditivní grupy $\mathbb{Z}$

Najdeme všechny podgrupy aditivní grupy $\mathbb{Z} = (\mathbb{Z}, +, 0, -)$. Pro celé nezáporné číslo $m \in \mathbb{N}_0$ označme

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}.$$

Tvrzení 5.4.1. *Množiny $m\mathbb{Z}$, $m \in \mathbb{N}_0$, jsou podgrupy aditivní grupy $\mathbb{Z}$ a jiné podgrupy v $\mathbb{Z}$ nejsou.*

Důkaz. Buď $m \in \mathbb{N}_0$ libovolné. Ukážeme, že $m\mathbb{Z}$ je podgrupa. Pro libovolné $mk, ml \in m\mathbb{Z}$ platí $mk+ml = m(k+l) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem ke sčítání. Množina $m\mathbb{Z}$ obsahuje neutrální prvek 0 grupy $\mathbb{Z}$. Nakonec, pro libovolné $mk \in m\mathbb{Z}$ platí $-(mk) = m(-k) \in m\mathbb{Z}$, čímž je dokázána uzavřenost množiny $m\mathbb{Z}$ vzhledem k inverzi (opačným prvkům).

Buď $B \subseteq \mathbb{Z}$ libovolná podgrupa grupy $\mathbb{Z}$. Ukážeme, že B je rovna některé podgrupě $m\mathbb{Z}$. Jelikož B je podgrupa, obsahuje neutrální prvek 0. Pokud $B = \{0\}$, pak $B = 0\mathbb{Z}$ ($m = 0$). Předpokládejme, že $B \neq \{0\}$, tedy existuje nenulové číslo $b \in B$. Navíc existuje *kladné* číslo $b_+ \in B$, buď $b_+ = b$, nebo $b_+ = -b$ ($-b \in B$, protože B je podgrupa). Označme m *nejmenší kladné číslo* v B (v každé neprázdné množině kladných celých čísel existuje nejmenší číslo).

Dokážeme, že toto číslo m je hledané číslo, pro něž $B = m\mathbb{Z}$. Nejdříve ukážeme, že $m\mathbb{Z} \subseteq B$. Již víme, že $0 \in B$ a $m \in B$. Předpokládejme, že $mk \in B$. Potom i $m(k+1) = mk+m \in B$ a díky matematické indukci dostáváme, že $mk \in B$ pro každé $k \in \mathbb{N}$. A potom i inverzní prvky $-mk$ leží v B, a tím je ukázáno, že všechny prvky množiny $m\mathbb{Z}$ leží v B.

Zbývá dokázat, že $B \subseteq m\mathbb{Z}$. Buď $b \in B$ libovolné a předpokládejme, že $b \notin m\mathbb{Z}$. Pak existují $q, r \in \mathbb{Z}$ taková, že

$$b = mq + r \quad \text{a} \quad 0 < r < m.$$

Potom $r = b - mq = b + m(-q)$ je kladný prvek B, menší než m, což je v rozporu s definicí prvku m. Proto $b \in m\mathbb{Z}$. □

5.5. Faktorové grupy

Definice 5.5.1. *Relace* na množině X je podmnožina kartézského součinu $X \times X$.

Je-li ρ relace, místo „(x, y) je v relaci ρ“ se obvykle říká „x je v relaci ρ s y“ a místo $(x, y) \in \rho$ se obvykle píše $x \,\rho\, y$.

Definice 5.5.2. Relace ρ na množině X je *relace ekvivalence*, jestliže je

(1) reflexivní, tj. $x \,\rho\, x$ pro každé $x \in X$,
(2) symetrická, tj. $x \,\rho\, y$ implikuje $y \,\rho\, x$,
(3) tranzitivní, tj. $x \,\rho\, y$, $y \,\rho\, z$ implikuje $x \,\rho\, z$.

Definice 5.5.3. Buďte $\equiv$ relace ekvivalence na množině X a $x, y \in X$. Jestliže $x \equiv y$, potom x je *ekvivalentní* y vzhledem k $\equiv$. Množina

$$\{y \in X \mid x \equiv y\}$$

všech prvků ekvivalentních prvku x je *třída ekvivalence* příslušná x vzhledem k $\equiv$, označujeme ji $[x]_\equiv$ nebo jen $[x]$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$[x]_\equiv = \{y \in X \mid x \equiv y\}.$$

Definice 5.5.4. Buď $\equiv$ relace ekvivalence na množině X. Množina

$$\{[x]_\equiv \mid x \in X\}$$

všech příslušných tříd ekvivalence je *faktorová množina* vzhledem k $\equiv$, označujeme ji $\tilde{X}_\equiv$ nebo jen $\tilde{X}$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$\tilde{X}_\equiv = \{[x]_\equiv \mid x \in X\}.$$

Poznamenejme, že $\tilde{X}$ je *rozklad množiny* X, to znamená, že množiny $[x]$ jsou neprázdné, po dvou disjunktní a jejich sjednocení je X.

Definice 5.5.5. Buďte X množina s binární operací $*$ a $\equiv$ relace ekvivalence na množině X. Relace $\equiv$ je *kongruence* na X s $*$, jestliže platí *podmínka kompatibility*, čili implikace

$$\text{jestliže } x_1 \equiv x_2 \text{ a } y_1 \equiv y_2, \text{ pak } x_1 * y_1 \equiv x_2 * y_2,$$

nebo ekvivalentně

$$\text{jestliže } [x_1] = [x_2] \text{ a } [y_1] = [y_2], \text{ pak } [x_1 * y_1] = [x_2 * y_2].$$

Tvrzení 5.5.1. *Buďte $\equiv$ kongruence na množině s asociativní binární operací a x, y invertibilní prvky. Pak platí implikace*

$$\textit{jestliže } x \equiv y, \textit{ pak } x^{-1} \equiv y^{-1}$$

nebo ekvivalentně zapsáno

$$\textit{jestliže } [x] = [y], \textit{ pak } [x^{-1}] = [y^{-1}].$$

Důkaz. Nechť $x \equiv y$. Jelikož $x^{-1} \equiv x^{-1}$ a $y^{-1} \equiv y^{-1}$, z podmínky kompatibility dostaneme $x * x^{-1} \equiv y * x^{-1}$, tedy $e \equiv y * x^{-1}$, a $y^{-1} * e \equiv y^{-1} * y * x^{-1}$, tedy $y^{-1} \equiv x^{-1}$. □

Příklad. (1) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$. Potom $\equiv$ je kongruence, protože součet jakýchkoliv sudých čísel je sudé číslo, součet jakýchkoliv dvou lichých čísel je sudé číslo a součet jakéhokoliv sudého čísla a jakéhokoliv lichého čísla je liché číslo.
(2) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě kladná nebo obě nulová, tedy $\tilde{\mathbb{Z}} = \{[-1], [0], [1]\}$. Potom $\equiv$ je relace ekvivalence, platí implikace

$$\text{jestliže } x \equiv y, \text{ pak } -x \equiv -y,$$

ale existují $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ taková, že $x_1 \equiv x_2$ a $y_1 \equiv y_2$, ale $x_1 + y_1 \not\equiv x_2 + y_2$. Čili $\equiv$ nesplňuje podmínku kompatibility a není to tedy kongruence na $\mathbb{Z}$.

(3) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě nezáporná, tedy $\tilde{\mathbb{Z}} = \{[-1], [0]\}$. Potom $\equiv$ je relace ekvivalence, ale existují $x, y \in \mathbb{Z}$ taková, že $x \equiv y$, ale $-x \not\equiv -y$. Podle Tvrzení 5.5.1 $\equiv$ není kongruence na $\mathbb{Z}$, a nesplňuje tedy podmínku kompatibility. □

Máme-li kongruenci a třídy $[x], [y]$, pak díky podmínce kompatibility třída $[x * y]$ je jednoznačně určena třídami $[x], [y]$, čili nezávisí na konkrétním výběru jejich prvků x, y (*reprezentantů*). Na množině $\tilde{X}$ tedy můžeme zavést binární operaci $\tilde{*}$ předpisem

$$[x]\tilde{*}[y] = [x * y]. \tag{9}$$

Příklad. Mějme grupu $(\mathbb{Z}, +, 0, -)$ a kongruenci $\equiv$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$.

Na $\tilde{\mathbb{Z}}$ máme binární operaci $\tilde{+}$ definovanou předpisem (9), tedy $[x]\tilde{+}[y] = [x + y]$. Takže

$$\begin{aligned}
&[0]\tilde{+}[0] = [0 + 0] = [2 + 6] = [8 + (-14)] = [0],\\
&[0]\tilde{+}[1] = [0 + 1] = [2 + 7] = [(-6) + 11] = [1],\\
&[1]\tilde{+}[0] = [1 + 0] = [7 + 6] = [17 + (-2)] = [1],\\
&[1]\tilde{+}[1] = [1 + 1] = [3 + 13] = [(-7) + 5] = [0].
\end{aligned}$$ □

Tvrzení 5.5.2. *Mějme kongruenci na množině X s binární operací $*$. Buď $\tilde{*}$ binární operace na $\tilde{X}$ definovaná předpisem (9). Potom*

(i) je-li $*$ asociativní, pak $\tilde{*}$ je asociativní;
(ii) je-li e neutrální prvek $*$, pak $[e]$ je neutrální prvek $\tilde{*}$;
(iii) je-li x^{-1} inverze k x vzhledem k $*$, pak $[x^{-1}]$ je inverze k $[x]$ vzhledem k $\tilde{*}$;
(iv) je-li $*$ komutativní, pak $\tilde{*}$ je komutativní.

Důkaz. (i) Jestliže $*$ je asociativní, potom pro libovolné třídy $[x], [y], [z] \in \tilde{X}$ platí

$$\begin{aligned}
[x]\tilde{*}([y]\tilde{*}[z]) &= [x]\tilde{*}[y * z] =\\
&= [x * (y * z)] =\\
&= [(x * y) * z] =\\
&= [x * y]\tilde{*}[z] =\\
&= ([x]\tilde{*}[y])\tilde{*}[z],
\end{aligned}$$

takže $\tilde{*}$ je asociativní.

(ii) Jestliže e je neutrální prvek oparace $*$, potom pro libovolnou třídu $[x] \in \tilde{X}$ platí

$$\begin{aligned}
&[x]\tilde{*}[e] = [x * e] = [x],\\
&[e]\tilde{*}[x] = [e * x] = [x],
\end{aligned}$$

takže $[e]$ je neutrální prvek operace $\tilde{*}$.

(iii) Jestliže x^{-1} je inverzní prvek k x vzhledem k $*$, pak

$$\begin{aligned}
&[x]\tilde{*}[x^{-1}] = [x * x^{-1}] = [e],\\
&[x^{-1}]\tilde{*}[x] = [x^{-1} * x] = [e],
\end{aligned}$$

takže $[x^{-1}]$ je inverzní prvek k $[x]$ vzhledem k operaci $\tilde{*}$.

(iv) Z (9) je zřejmé, že je-li $*$ komutativní, pak i $\tilde{*}$ je komutativní. □

Důsledek. *Pro každou (komutativní) grupu a každou kongruenci na této grupě příslušná faktorová množina s operací definovanou předpisem (9) je (komutativní) grupa.*

Důkaz. Tvrzení je jednoduchým důsledkem předchozího tvrzení. □

Jelikož každý prvek množiny s asociativní operací má nejvýše jeden inverzní prvek, viz Tvrzení 5.1.2 nebo Tvrzení 5.5.1, třída $[x^{-1}]$ je v takovém případě jednoznačně určena třídou $[x]$, čili nezávisí na konkrétním výběru jejího prvku x, a proto je korektní ji označovat $[x]^{-1}$.

Definice 5.5.6. Faktorová množina s operací definovanou předpisem (9) z předchozího Důsledku je *faktorová grupa*.

Příklad. Mějme grupu $(\mathbb{Z}, +, 0, -)$ a kongruenci danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$.

Na $\tilde{\mathbb{Z}}$ máme asociativní binární operaci $\tilde{+}$: $[x]\tilde{+}[y] = [x + y]$, neutrální prvek operace $\tilde{+}$ je $[0]$ a opačný prvek $-[x]$ k prvku $[x]$ je $[-x]$, čili $-[0] = [0]$, $-[1] = [-1] = [1]$. □

5.6. Zbytkové třídy

Mějme aditivní grupu $(\mathbb{Z}, +, 0, -)$ a buď m libovolné přirozené (kladné celé) číslo. Definujme relaci $\equiv_m$ na $\mathbb{Z}$ předpisem:

$$x \equiv_m y \text{ právě tehdy, když } x - y \text{ je celočíselný násobek čísla } m$$

(čili $m \mid (x - y)$ a existuje tedy $k \in \mathbb{Z}$ takové, že $x - y = km$ a $x = y + km$).

Potom $\equiv_m$ je relace ekvivalence (cvičení), příslušné třídy ekvivalence $[i]_{\equiv_m}$ se značí $[i]_m$ a

$$\begin{aligned}
&\vdots\\
[-2]_m &= \{-2 + km \mid k \in \mathbb{Z}\} = \{\ldots, -2 - 2m, -2 - m, -2, -2 + m, -2 + 2m, \ldots\},\\
[-1]_m &= \{-1 + km \mid k \in \mathbb{Z}\} = \{\ldots, -1 - 2m, -1 - m, -1, -1 + m, -1 + 2m, \ldots\},\\
[0]_m &= \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\},\\
[1]_m &= \{1 + km \mid k \in \mathbb{Z}\} = \{\ldots, 1 - 2m, 1 - m, 1, 1 + m, 1 + 2m, \ldots\},\\
[2]_m &= \{2 + km \mid k \in \mathbb{Z}\} = \{\ldots, 2 - 2m, 2 - m, 2, 2 + m, 2 + 2m, \ldots\},\\
&\vdots\\
[i]_m &= \{i + km \mid k \in \mathbb{Z}\} = \{\ldots, i - 2m, i - m, i, i + m, i + 2m, \ldots\},\\
&\vdots
\end{aligned}$$

Pro $i \in \{0, \ldots, m-1\}$ třída ekvivalence $[i]_m$ obsahuje právě ta celá čísla z, po jejichž celočíselném dělení číslem m číslo i je zbytek. Třídám $[i]_m$, kde $i \in \{0, \ldots, m-1\}$, se proto říká *zbytkové třídy*. Při dělení číslem m všechny možné zbytky jsou právě $0, 1, \ldots, m-1$, takže každé celé číslo leží v právě jedné ze zbytkových tříd $[0]_m, [1]_m, \ldots, [m-1]_m$. Příslušná faktorová množina $\tilde{\mathbb{Z}}_{\equiv_m}$ se značí $\mathbb{Z}_m$, tedy

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Ověříme, zda $\equiv_m$ je kongruence na $\mathbb{Z}$, čili podmínku kompatibility. Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 \in [x_1]_m$ a $y_2 \in [y_1]_m$, čili $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 + y_2 = x_1 + km + y_1 + lm = x_1 + y_1 + (k + l)m \in [x_1 + y_1]_m$, a tedy $[x_1 + y_1]_m = [x_2 + y_2]_m$.

Na množině $\mathbb{Z}_m$ tedy máme binární operaci $+$ (značí se obvykle stejně jako původní operace) podle (9)

$$[x]_m + [y]_m = [x + y]_m$$

a příslušná faktorová grupa $(\mathbb{Z}_m, +, [0]_m, -)$ je komutativní *aditivní grupa zbytkových tříd modulo* m.

Na množině $\mathbb{Z}$ uvažujme operaci $\cdot$, která je asociativní a má neutrální prvek 1. Ověříme podmínku kompatibility pro operaci $\cdot$.

Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 \cdot y_2 = (x_1 + km) \cdot (y_1 + lm) = x_1 y_1 + (ky_1 + lx_1 + klm)m \in [x_1 y_1]_m$, a tedy $[x_1 y_1]_m = [x_2 y_2]_m$.

Na $\mathbb{Z}_m$ tedy máme i binární operaci $\cdot$ podle (9)

$$[x]_m \cdot [y]_m = [x \cdot y]_m.$$

Podle Tvrzení 5.5.2 operace $\cdot$ na množině $\mathbb{Z}_m$ je komutativní, asociativní a má neutrální prvek $[1]_m$. Faktorová množina $\mathbb{Z}_m$ s operací $\cdot$ a neutrálním prvkem $[1]_m$ je komutativní *multiplikativní monoid zbytkových tříd modulo* m (*monoid* je množina s asociativní binární operací a neutrálním prvkem). Otázka existence inverzí vzhledem k operaci $\cdot$ není tak jednoduchá jako v případě operace $+$.

Tvrzení 5.6.1. *Prvek $[x]_m \in \mathbb{Z}_m$ má inverzi vzhledem k operaci $\cdot$ právě tehdy, když x a m jsou nesoudělná, tedy jejich největší společný dělitel $D(x, m)$ je* 1.

Důkaz. Předpokládejme, že $[y]_m$ je inverze k $[x]_m$, tedy $[x]_m \cdot [y]_m = [xy]_m = [1]_m$. Takže $xy + km = 1$ pro vhodné $k \in \mathbb{Z}$ a každý společný dělitel čísel x a m je dělitel i čísla 1. Proto $D(x, m) = 1$.

Předpokládejme, že $D(x, m) = 1$. Podle Bézoutovy věty existují čísla $y, k \in \mathbb{Z}$ taková, že $D(x, m) = xy + km$, tedy $1 = xy + km$, takže $[1]_m = [xy]_m = [x]_m \cdot [y]_m$ a $[y]_m$ je inverze k $[x]_m$. □

Příklad. Nechť $m = 5$. Následující tabulka naznačuje rozložení množiny všech celých čísel do pěti tříd:

$[0]_5$				-5						0					5							
$[1]_5$						-4					1					6						
$[2]_5$	$\cdots$						-3					2						7				$\cdots$
$[3]_5$								-2					3						8			
$[4]_5$										-1					4						9	

Aditivní grupa $\mathbb{Z}_5$ resp. multiplikativní monoid $\mathbb{Z}_5$ mají tabulky

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

resp.

$\cdot$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

□