10. přednáška, 30. 11. 2021

6.5. Faktorové grupy

Definice 6.5.1. *Relace* na množině X je podmnožina kartézského součinu $X \times X$. Je-li ρ relace, místo $(x, y) \in \rho$ často píšeme $x \,\rho\, y$.

Definice 6.5.2. 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 $x \,\rho\, z$.

Buď $(X, *, e, {}^{-1})$ grupa. Buď $\equiv$ relace ekvivalence na množině X. Třídu ekvivalence příslušnou prvku x označme $[x]_\equiv$ (nebo jen $[x]$, je-li zřejmé, o jakou relaci ekvivalence se jedná) a množinu všech tříd ekvivalence (*faktorovou množinu*) označme $\tilde{X}$, tedy

$$[x]_\equiv = \{y \in X \mid x \equiv y\} \quad \text{a} \quad \tilde{X} = \{[x]_\equiv \mid x \in X\}.$$

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

Definice 6.5.3. Relace ekvivalence $\equiv$ je *kongruence*, jestliže platí implikace (*podmínka kompatibility*)

$$\text{jestliže } x_1 \equiv x_2, y_1 \equiv y_2, \text{ pak } x_1 * y_1 \equiv x_2 * y_2, \tag{1}$$

$$\text{jestliže } x \equiv y, \text{ pak } x^{-1} \equiv y^{-1} \tag{2}$$

nebo ekvivalentně zapsáno

$$\text{jestliže } [x] = [x'], [y] = [y'], \text{ pak } [x * y] = [x' * y'], \tag{3}$$

$$\text{jestliže } [x] = [y], \text{ pak } [x^{-1}] = [y^{-1}]. \tag{4}$$

Je-li $\cong$ kongruence, pak třída $[x * y]$ závisí jen a jen na třídách $[x], [y]$ a ne na konkrétním výběru prvků x, y, které v nich leží (reprezentantů). Na množině $\tilde{X}$ tedy můžeme zavést binární operaci $\tilde{*}$ pravidlem

$$[x] \,\tilde{*}\, [y] = [x * y]. \tag{5}$$

Tvrzení 6.5.1. *Pro každou kongruenci na (komutativní) grupě i příslušná faktorová množina s operací definovanou pravidlem (5) je (komutativní) grupa.*

Důkaz. Buďte $(X, *, e, {}^{-1})$ grupa s kongruencí a $\tilde{X}$ příslušná faktorová množina s operací $\tilde{*}$. 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.

Pro libovolnou třídu $[x] \in \tilde{X}$ platí

$$[x] \,\tilde{*}\, [e] = [x * e] = [x],$$
$$[e] \,\tilde{*}\, [x] = [e * x] = [x],$$

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

Pro libovolnou třídu $[x] \in \tilde{X}$ platí

$$[x] \mathbin{\tilde{*}} [x^{-1}] = [x * x^{-1}] = [e],$$
$$[x^{-1}] \mathbin{\tilde{*}} [x] = [x^{-1} * x] = [e],$$

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

Z (5) je zřejmé, že je-li $*$ komutativní, pak i $\tilde{*}$ je komutativní. □

Z jednoznačnosti inverzních prvků plyne, že třída $[x^{-1}]$ je jednoznačně určena třídou $[x]$, a proto je korektní ji označovat $[x]^{-1}$.

Definice 6.5.4. Faktorová množina s operací definovanou pravidlem (5) je *faktorová grupa*.

6.6. Zbytkové třídy

Pro libovolné přirozené číslo $m > 1$ zkonstruujeme faktorovou grupu $\mathbb{Z}_m$ aditivní grupy $\mathbb{Z}$. Grupa $\mathbb{Z}_m$ bude mít m prvků.

Zaveďme podmnožiny $[i]_m \subset \mathbb{Z}$:

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

Zřejmě $j \in [i]_m$ právě tehdy, když existuje číslo $k \in \mathbb{Z}$ takové, že $j = i + km$.

Všimněme si, že pro $i = 0, \ldots, m-1$ množina $[i]_m$ obsahuje právě ta celá čísla z, pro něž i je zbytkem při celočíselném dělení čísla z přirozeným číslem m, říká se jim proto *zbytkové třídy*. Ale všechny možné zbytky při dělení číslem m jsou právě $0, 1, \ldots, m-1$, takže každé číslo $z \in \mathbb{Z}$ leží v právě jedné ze zbytkových tříd $[0]_m, [1]_m, \ldots, [m-1]_m$. Tudíž, zbytkové třídy $[0]_m, [1]_m, \ldots, [m-1]_m$ tvoří rozklad množiny $\mathbb{Z}$ a existuje relace ekvivalence na množině $\mathbb{Z}$, jejíž třídy ekvivalence jsou právě $[0]_m, [1]_m, \ldots, [m-1]_m$. Příslušnou faktorovou množinu označujeme

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

Ověříme podmínku kompatibility (1). Předpokládejme, že $[x]_m = [x']_m$ a $[y]_m = [y']_m$. Pak $x' \in [x]_m$ a $y' \in [y]_m$, a tedy $x' = x + km$, $y' = y + lm$ pro vhodná $k, l \in \mathbb{Z}$, načež $x' + y' = x + km + y + lm = x + y + (k + l)m \in [x + y]_m$. Tudíž, $[x + y]_m = [x' + y']_m$.

Podle (5) potom na m-prvkové množině $\mathbb{Z}_m$ vzniká binární operace, kterou pro jednoduchost označíme zase $+$, zadaná předpisem

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

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

Podobně ověříme podmínku kompatibility (1) pro operaci $\cdot$. Předpokládejme, že $[x]_m = [x']_m$ a $[y]_m = [y']_m$, tj. $x' = x + km$, $y' = y + lm$ pro vhodná $k, l \in \mathbb{Z}$, načež $x' \cdot y' = (x + km) \cdot (y + lm) = xy + (ky + lx + klm)m \in [xy]_m$. Tudíž, $[xy]_m = [x'y']_m$.

Na $\mathbb{Z}_m$ tedy můžeme zavést i binární operaci násobení předpisem

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

Stejně jako v důkazu Tvrzení 6.5.1 lze dokázat, že 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 6.6.1. *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 $D(x,m) = yx + km$. V našem případě $1 = xy + km$, 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.

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

■

7. Okruhy a pole

Definice 7.0.1. Množina P se dvěmi binárními operacemi + a · je *okruh*, jestliže

(1) + a · jsou asociativní a komutativní operace,
(2) + má neutrální prvek, značíme ho 0,
(3) · má neutrální prvek různý od 0, značíme ho 1,
(4) ke každému prvku x existuje inverzní prvek vzhledem k +, značíme ho $-x$,
(5) pro libovolné $x, y, z \in P$ platí $x \cdot (y + z) = x \cdot y + x \cdot z$ (*distributivní zákon*).

Pokud navíc ke každému prvku $x \neq 0$ existuje inverzní prvek vzhledem k operaci · (značíme ho x^{-1}), množina P s operacemi + a · je *pole*.

Příklad. (1) Množiny $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ s operacemi sčítání a násobení jsou pole.

(2) Množina $\mathbb{Z}$ s operacemi sčítání a násobení je okruh, ale není pole.

(3) Množina $\mathbb{N}_0$ s operacemi sčítání a násobení není okruh.

(4) Množina $P[x]$ s operacemi sčítání a násobení polynomů je okruh, ale není pole.

(5) Množina $\mathcal{M}_n(P)$ s operacemi sčítání a násobení matic není okruh.

(6) Nechť $P = \{0, 1\}$ a binární operace + a · na P jsou takové, že

+	0	1
0	0	1
1	1	0

a

·	0	1
0	0	0
1	0	1

Neutrální prvek operace + je 0 a inverzní (opačné) prvky jsou $-0 = 0$ a $-1 = 1$. Neutrální prvek operace · je 1 a inverzní prvek k 1 je 1 ($1^{-1} = 1$), inverzní prvek k 0 neexistuje. Množina $\{0, 1\}$ s těmito operacemi je pole.

(7) Nechť $P = \{0, 1, 2, 3\}$ a binární operace + a · na P jsou takové, že

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

a

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Potom neutrální prvek operace + je 0, neutrální prvek operace · je 1 a

$$\begin{array}{ll} -0 = 0 & 0^{-1} \text{ neexistuje} \\ -1 = 3 & 1^{-1} = 1 \\ -2 = 2 & 2^{-1} \text{ neexistuje} \\ -3 = 1 & 3^{-1} = 3 \end{array}$$

a

Množina $\{0, 1, 2, 3\}$ s těmito operacemi je okruh, ale není pole. ■

Tvrzení 7.0.1. *Buď P okruh. Pak pro libovolné prvky $x, y, z \in P$ platí*

(i) $x \cdot 0 = 0$;
(ii) $x \cdot (-1) = -x$;
(iii) $x \cdot (y - z) = x \cdot y - x \cdot z$.

Důkaz. (i) Máme

$$\begin{aligned} x \cdot 0 &= x \cdot (0 + 0) = \\ &= x \cdot 0 + x \cdot 0 \end{aligned}$$

a přičteme-li k oběma stranám rovnosti prvek $-(x \cdot 0)$, obdržíme požadovaný výsledek.

(ii) Máme

$$0 = x \cdot 0 = x \cdot (1 + (-1)) = x \cdot 1 + x \cdot (-1) = \\ = x + x \cdot (-1)$$

a přičteme-li k oběma stranám rovnosti prvek $-x$, obdržíme požadovaný výsledek.
(iii) Cvičení. □

Cvičení. Dokažte, že v každém okruhu platí:
(1) $(-1) \cdot (-1) = 1$,
(2) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$. ▷

Tvrzení 7.0.2. *Buď P pole a buďte $x, y \in P$. Jestliže $x \cdot y = 0$, pak $x = 0$ nebo $y = 0$.*

Důkaz. Nechť $x \cdot y = 0$. Předpokládejme, že jeden z prvků x, y je nenulový, například $x \neq 0$. Potom s využitím bodu (i) v předchozím tvrzení dostaneme $y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0$. □

Příklad. (1) V příkladu (7) máme okruh, v němž $2 \cdot 2 = 0$. To ukazuje, že předchozí tvrzení neplatí pro okruhy.
(2) Pro okruh $P[x]$ ale předchozí tvrzení platí, viz kapitolu o polynomech. ■

Důsledek. *Buď P pole a buďte $x, y \in P$. Potom $x \cdot y \neq 0$ právě tehdy, když $x \neq 0$ a $y \neq 0$.*

Důkaz. Tvrzení je důsledkem předchozích dvou tvrzení. □

Obdobně jako v kapitole 6 P^* označuje množinu $P \setminus \{0\}$.

Je-li P okruh, pak P s operací $+$ je komutativní grupa. Pro pole máme navíc následující tvrzení.

Tvrzení 7.0.3. *Je-li P pole, pak P^* s operací $\cdot$ je komutativní grupa.*

Důkaz. Buďte $x, y \in P^*$, tedy $x \neq 0$ a $y \neq 0$. Podle předchozího Důsledku $x \cdot y \neq 0$, tedy $x \cdot y \in P^*$, a množina P^* je uzavřená vzhledem k operaci $\cdot$. Zbytek tvrzení plyne z toho, že operace $\cdot$ je asociativní a komutativní, $1 \in P^*$ je neutrální prvek, každý nenulový prvek je invertibilní a příslušné inverze jsou nenulové. □

Tvrzení 7.0.4. *Množina $\mathbb{Z}_m$, $m > 1$, zbytkových tříd je pole právě tehdy, když m je prvočíslo.*

Důkaz. Buď $m > 1$. Podle kapitoly 6.6 $\mathbb{Z}_m$ splňuje podmínky (1)–(4) z definice okruhu a pole. Ověření, že platí distributivní zákon (5), ponecháme jako cvičení. Zbývá ukázat, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverzní prvek vzhledem k operaci $\cdot$ právě tehdy, když m je prvočíslo.

Předpokládejme, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverze. Podle Tvrzení 6.6.1 každé takové x je nesoudělné s m, tedy m je prvočíslo.

Na druhou stranu, je-li m prvočíslo, pak každé $x \in \mathbb{Z}$ takové, že $[x]_m \neq [0]_m$, je nesoudělné s m. Opět podle Tvrzení 6.6.1 $[x]_m$ má inverzi.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 3. Pole]. □

Stejně jako máme podgrupy grup (a podstruktury dalších algebraických struktur), existují podokruhy okruhů a podpole polí. Zmíníme jen podpole.

Definice 7.0.2. Buď P pole. Buď $Q \subset P$ podmnožina taková, že
(1) $0, 1 \in Q$;
(2) je-li $x, y \in Q$, pak $x + y \in Q$ a $xy \in Q$;
(3) je-li $x \in Q$, pak $-x \in Q$;

(4) je-li $x \in Q$, $x \neq 0$, pak $x^{-1} \in Q$.

Potom Q je *podpole* pole P.

Aby podmnožina pole byla podpole, musí obsahovat neutrální prvky obou binárních operací, musí být uzavřená vzledem k oběma binárním operacím a musí být uzavřená vzhledem k inverzím vzhledem k oběma binárním operacím.

Každé podpole je pole.

Příklad. (1) Pole $\mathbb{Q}$ je podpole polí $\mathbb{R}$ a $\mathbb{C}$. Pole $\mathbb{R}$ je podpole pole $\mathbb{C}$.

(2) Množina $\mathbb{Z}$ není podpole pole $\mathbb{Q}$, protože neobsahuje inverzi k 2 vzhledem k operaci $\cdot$.

(3) Množina $\{0, 1\}$ není podpole pole $\mathbb{Q}$ (a samozřejmě ani $\mathbb{R}$ a $\mathbb{C}$), protože $1 + 1 = 2 \notin \{0, 1\}$. Ačkoliv, jak už víme, na množině $\{0, 1\}$ lze definovat operace sčítání a násobení tak, že to je pole. ■

Definice 7.0.3. Podpole pole $\mathbb{C}$ je *číselné pole*.