

8. přednáška, 18. 11. 2025

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

$$[x]\tilde{*}[y] = [x * y]. \quad (10)$$

**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 (10), tedy  $[x]\tilde{+}[y] = [x + y]$ . Takže

$$[0]\tilde{+}[0] = [0 + 0] = [2 + 6] = [8 + (-14)] = [0],$$

$$[0]\tilde{+}[1] = [0 + 1] = [2 + 7] = [(-6) + 11] = [1],$$

$$[1]\tilde{+}[0] = [1 + 0] = [7 + 6] = [17 + (-2)] = [1],$$

$$[1]\tilde{+}[1] = [1 + 1] = [3 + 13] = [(-7) + 5] = [0]. \quad \square$$

**Tvrzení 5.5.2.** *Mějme kongruenci na množině  $X$  s binární operací  $*$ . Bud'  $\tilde{*}$  binární operace na  $\tilde{X}$  definovaná předpisem (10). 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 operace  $*$ , 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 (10) je zřejmé, že je-li  $*$  komutativní, pak i  $\tilde{*}$  je komutativní.  $\square$

**Důsledek.** *Pro každou (komutativní) grupu a každou kongruenci na této grupě příslušná faktorová množina s operací definovanou předpisem (10) je (komutativní) grupa.*

*Důkaz.* Tvrzení je jednoduchým důsledkem předchozího tvrzení.  $\square$

Jelikož každý prvek množiny s asociativní operací má nejvýše jeden inverzní prvek, viz Tvzení 5.1.2 nebo Tvzení 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 (10) 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  $-[0] = [0]$ ,  $-[1] = [-1] = [1]$ .  $\square$

## 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

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

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

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

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 (10)

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

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  $[x_2 y_2]_m = [x_1 y_1]_m$ .

Na  $\mathbb{Z}_m$  tedy máme i binární operaci  $\cdot$  podle (10)

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

Podle Tvzení 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  $[x]_m$ .  $\square$

**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 |
| $[2]_5$ | $\dots$ |    | -3 |    | 2 |   | 7 |
| $[3]_5$ |         |    | -2 |    | 3 |   | 8 |
| $[4]_5$ |         |    |    | -1 |   | 4 | 9 |

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

| $+$     | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |       | $\cdot$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |
|---------|---------|---------|---------|---------|---------|-------|---------|---------|---------|---------|---------|---------|
| $[0]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ | resp. | $[0]_5$ | $[0]_5$ | $[0]_5$ | $[0]_5$ | $[0]_5$ | $[0]_5$ |
| $[1]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ | $[0]_5$ |       | $[1]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ |
| $[2]_5$ | $[2]_5$ | $[3]_5$ | $[4]_5$ | $[0]_5$ | $[1]_5$ |       | $[2]_5$ | $[0]_5$ | $[2]_5$ | $[4]_5$ | $[1]_5$ | $[3]_5$ |
| $[3]_5$ | $[3]_5$ | $[4]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ |       | $[3]_5$ | $[0]_5$ | $[3]_5$ | $[1]_5$ | $[4]_5$ | $[2]_5$ |
| $[4]_5$ | $[4]_5$ | $[0]_5$ | $[1]_5$ | $[2]_5$ | $[3]_5$ |       | $[4]_5$ | $[0]_5$ | $[4]_5$ | $[3]_5$ | $[2]_5$ | $[1]_5$ |

**Příklad.** Nechť v některém roce připadá Štědrý den na středu. Není-li následující rok přestupný, potom v něm Štědrý den připadá na čtvrtek, protože  $365 = 52 \cdot 7 + 1$ , tedy  $[365]_7 = [1]_7$ . Je-li následující rok přestupný, potom v něm Štědrý den připadá na pátek, protože  $366 = 52 \cdot 7 + 2$ , tedy  $[366]_7 = [2]_7$ .  $\square$

## 6. OKRUHY A POLE

**Definice 6.0.1.** Množina  $P$  se dvěma binárními operacemi  $+$  a  $\cdot$  je *okruh*, jestliže

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

Pokud navíc

- (6) ke každému prvku  $x \neq 0$  existuje inverzní prvek vzhledem k operaci  $\cdot$ ,
- množina  $P$  s operacemi  $+$  a  $\cdot$  je *pole*.

Inverzní prvek k  $x$  vzhledem k operaci  $+$  se nazývá *opačný* k  $x$  a značí se  $-x$ . Inverzní prvek k  $x$  vzhledem k operaci  $\cdot$  se značí  $x^{-1}$ .

Podmínka (5) v předchozí definici je *distributivní zákon*.

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

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

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

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

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

(6) Pro každé  $m \in \mathbb{N}$  množina  $\mathbb{Z}_m$  zbytkových tříd s operacemi součet a součin je okruh. Totiž,  $\mathbb{Z}_m$  splňuje podmínky (1)–(4) z definice okruhu podle kapitol 5.5 a 5.6 a to, že splňuje i distributivní zákon (5), lze snadno ověřit (cvičení).

(7) Okruh  $\mathbb{Z}_m$  zbytkových tříd je pole právě tehdy, když  $m$  je prvočíslo (viz Tvzení 6.0.1).

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

|     |     |     |     |         |     |     |
|-----|-----|-----|-----|---------|-----|-----|
| $+$ | $0$ | $1$ |     | $\cdot$ | $0$ | $1$ |
| $0$ | $0$ | $1$ | $a$ | $0$     | $0$ | $0$ |
| $1$ | $1$ | $0$ |     | $1$     | $0$ | $1$ |

Pro operaci  $+$  neutrální prvek je  $0$  a inverzní (opačné) prvky jsou  $-0 = 0$  a  $-1 = 1$ . Pro operaci  $\cdot$  neutrální prvek 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.

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

|     |     |     |     |     |     |         |     |     |     |     |
|-----|-----|-----|-----|-----|-----|---------|-----|-----|-----|-----|
| $+$ | $0$ | $1$ | $2$ | $3$ |     | $\cdot$ | $0$ | $1$ | $2$ | $3$ |
| $0$ | $0$ | $1$ | $2$ | $3$ | $a$ | $0$     | $0$ | $0$ | $0$ | $0$ |
| $1$ | $1$ | $2$ | $3$ | $0$ |     | $1$     | $0$ | $1$ | $2$ | $3$ |
| $2$ | $2$ | $3$ | $0$ | $1$ |     | $2$     | $0$ | $2$ | $0$ | $2$ |
| $3$ | $3$ | $0$ | $1$ | $2$ |     | $3$     | $0$ | $3$ | $2$ | $1$ |

Potom neutrální prvek operace  $+$  je  $0$ , neutrální prvek operace  $\cdot$  je  $1$  a

|          |     |                     |
|----------|-----|---------------------|
| $-0 = 0$ |     | $0^{-1}$ neexistuje |
| $-1 = 3$ | $a$ | $1^{-1} = 1$        |
| $-2 = 2$ |     | $2^{-1}$ neexistuje |
| $-3 = 1$ |     | $3^{-1} = 3$        |

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

**Tvrzení 6.0.1.** Množina  $\mathbb{Z}_m$  zbytkových tříd je pole právě tehdy, když  $m$  je prvočíslo.

*Důkaz.* Podle předchozího Příkladu (6)  $\mathbb{Z}_m$  je okruh. Číslo 1 není prvočíslo a  $\mathbb{Z}_1$  není pole (cvičení). Buď  $m > 1$ . 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 Tvzení 5.6.1 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 Tvzení 5.6.1  $[x]_m$  má inverzi.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 3. Pole].  $\square$

Takže, například,  $\mathbb{Z}_4$  není pole. Čtyřprvkové pole ale existuje, viz následující příklad.

**Příklad.** Necht'  $X = \{0, 1, a, b\}$  a binární operace  $+$  a  $\cdot$  na  $X$  jsou takové, že

| $+$ | 0 | 1 | a | b |   | $\cdot$ | 0 | 1 | a | b |
|-----|---|---|---|---|---|---------|---|---|---|---|
| 0   | 0 | 1 | a | b |   | 0       | 0 | 0 | 0 | 0 |
| 1   | 1 | 0 | b | a | a | 1       | 0 | 1 | a | b |
| a   | a | b | 0 | 1 |   | a       | 0 | a | b | 1 |
| b   | b | a | 1 | 0 |   | b       | 0 | b | 1 | a |

Množina  $X$  s těmito operacemi  $+$  a  $\cdot$  je pole.  $\square$

**Poznámka.** Buď  $n$  libovolné přirozené číslo. Potom existuje  $n$ -prvkové pole právě tehdy, když  $n$  je mocnina prvočísla, čili  $n = p^k$ , kde  $p$  je prvočíslo a  $k$  je přirozené číslo.

**Tvrzení 6.0.2.** *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)

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

(ii)

$$\begin{aligned}
 x + x \cdot (-1) &= x \cdot 1 + x \cdot (-1) = x \cdot (1 + (-1)) = x \cdot 0 = 0 \\
 x \cdot (-1) + x &= x \cdot (-1) + x \cdot 1 = x \cdot (-1 + 1) = x \cdot 0 = 0
 \end{aligned}$$

takže  $x \cdot (-1) = -x$ .

(iii) Cvičení.  $\square$

**Cvičení.** Dokažte, že v každém okruhu platí:

- (1)  $(-1) \cdot (-1) = 1$ ,
- (2)  $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ .  $\square$

**Tvrzení 6.0.3.** *Buď  $P$  pole a buďte  $x, y, z \in P$ .*

- (1)  $x \cdot y = 0$  právě tehdy, když  $x = 0$  nebo  $y = 0$ .
- (2) Jestliže  $x \cdot y = x \cdot z$  a  $x \neq 0$ , pak  $y = z$ .

*Důkaz.* (1) Jestliže  $x = 0$  nebo  $y = 0$ , pak podle Tvzení 6.0.2(i) také  $x \cdot y = 0$ .

Nechť  $x \cdot y = 0$ . Předpokládejme, že jeden z prvků  $x, y$  je nenulový, například  $x \neq 0$ . Potom s využitím Tvzení 6.0.2(i) dostaneme

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

(2)

$$\begin{aligned} y &= 1 \cdot y & (1 &= x^{-1} \cdot x) \\ &= x^{-1} \cdot x \cdot y & (x \cdot y &= x \cdot z) \\ &= x^{-1} \cdot x \cdot z & (x^{-1} \cdot x &= 1) \\ &= 1 \cdot z = z \end{aligned}$$

□

**Příklad.** (1) V příkladu (9) máme okruh, v němž  $2 \cdot 2 = 0$  a  $2 \cdot 1 = 2 \cdot 3$ . To ukazuje, že předchozí tvrzení neplatí pro okruhy.

(2) Pro okruh  $P[x]$  ale předchozí tvrzení platí, viz kapitolu o polynomech. □

Obdobně jako v kapitole 5  $P^*$  označuje množinu  $P \setminus \{0\}$ .

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

**Tvrzení 6.0.4.** *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 Tvzení 6.0.3(i)  $x \cdot y \neq 0$ , 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. □

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

**Definice 6.0.2.** Buď  $P$  pole. Buď  $Q \subseteq P$  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 vzhledem 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)  $\mathbb{Z}$  není podpole pole  $\mathbb{Q}$ , neboť 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 součet a součin tak, že to je pole. □

**Definice 6.0.3.** Podpole pole  $\mathbb{C}$  je *číselné pole*.



## 7. USPOŘÁDÁNÍ A SVAZY

### 7.1. Uspořádané množiny

**Definice 7.1.1.** Relace  $\rho$  na množině  $X$  je *uspořádání*, jestliže je

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

Potom dvojice  $(X, \rho)$  je *uspořádaná množina*.

**Příklad.** (1) Pro libovolnou množinu  $X$  relace  $=$  je uspořádání.

(2)  $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{R}, \leq)$ , kde  $\leq$  je obvyklé uspořádání podle velikosti, jsou uspořádané množiny.

(3) Buďte  $X$  množina a  $\mathcal{P}(X)$  množina všech podmnožin množiny  $X$ . Inkluze  $\subseteq$  je uspořádání na  $\mathcal{P}(X)$ .

(4) Relace  $|$  (dělí) na množině  $\mathbb{N}$  (tj.  $x | y$  právě tehdy, když existuje  $n \in \mathbb{N}$  takové, že  $x \cdot n = y$ ) je uspořádání, nazývá se *relace dělitelnosti*. Je zřejmé, že tato relace je reflexivní a tranzitivní.

Ukážeme, že  $|$  je i antisymetrická relace. Předpokládejme, že  $x | y$  a  $y | x$ , tedy existují  $m, n \in \mathbb{N}$  taková, že  $xm = y$  a  $yn = x$ . Potom  $xmn = x$  a jelikož  $x \neq 0$ ,  $mn = 1$ . V přirozených číslech to lze jedinečně tak, že  $m = 1$  a  $n = 1$ . Tedy  $x = x \cdot 1 = y$ .

Upozorníme, že obdobně definovaná relace dělitelnosti na  $\mathbb{Z}$  není antisymetrická, protože  $1 \neq -1$ , přestože  $1 | -1$  a  $-1 | 1$  (rovnice  $mn = 1$  má v celých číslech další řešení  $m = -1$  a  $n = -1$ ).  $\square$

Buď  $\rho$  uspořádání na množině  $X$ . Inverzní (opačná) relace  $\rho^{-1}$  (tj. relace definovaná předpisem „ $x \rho^{-1} y$  právě tehdy, když  $y \rho x$ “) je také uspořádání. Nazývá se *duální uspořádání*. Máme-li uspořádání  $\leq$ , potom duální uspořádání  $\leq^{-1}$  se označuje symbolem  $\geq$ . Podobně je to se symboly  $\subseteq$  atp.

**Definice 7.1.2.** Buď  $(X, \leq)$  uspořádaná množina,  $Y \subseteq X$ . Relace  $\leq_Y$  na množině  $Y$  zadaná předpisem  $x \leq_Y y \Leftrightarrow x \leq y$  je *indukované uspořádání* na množině  $Y$  a značí se rovněž  $\leq$ .

**Definice 7.1.3.** Prvky  $x, y$  uspořádané množiny jsou *srovnatelné*, platí-li  $x \leq y$  nebo  $y \leq x$ . Uspořádaná množina je *řetězec*, jsou-li každé dva její prvky srovnatelné.

**Příklad.**  $(\mathbb{R}, \leq), (\mathbb{Z}, \leq), (\mathbb{N}, \leq)$  jsou řetězce.  $\square$

Buď  $\leq$  uspořádání na  $X$ . Označme  $x < y$ , jestliže  $x \leq y$  a zároveň  $x \neq y$ . Dále zavedme označení  $x \triangleleft y$ , jestliže  $x < y$  a neexistuje  $z \in X$  takové, že  $x < z, z < y$ . Je-li  $x \triangleleft y$ , pak říkáme, že  $x$  je *bezprostředním předchůdcem*  $y$ , nebo  $y$  *pokrývá*  $x$ .

**Příklad.** (1) V množině  $\mathbb{N}$  s přirozeným uspořádáním podle velikosti platí  $1 < 2$  a  $1 \triangleleft 2$ ,  $1 < 3$ , ale neplatí  $1 \triangleleft 3$ .

(2) V množině  $\mathbb{N}$  s relací dělitelnosti 6 pokrývá 3.

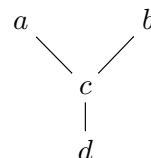
(3) V množině  $\mathbb{Q}$  všech racionálních čísel s přirozeným uspořádáním podle velikosti neplatí  $x \triangleleft y$  pro žádnou dvojici  $x, y \in \mathbb{Q}$ . Pro libovolné  $x, y \in \mathbb{Q}$  takové, že  $x < y$ , platí  $z = \frac{1}{2}(x + y) \in \mathbb{Q}$  a  $x < z, z < y$ .  $\square$

Konečnou uspořádanou množinu  $(X, \leq)$  můžeme znázornit diagramem. Prvky množiny  $X$  znázorníme jako body v rovině. Prvky  $x, y$  splňující  $x \triangleleft y$  vyznačíme tak, že  $x$  leží níže než  $y$  a spojíme je úsečkou.

Z diagramu pak můžeme určit uspořádání množiny  $X$ :  $x \leq y$  právě tehdy, když  $x$  leží níže než  $y$  a existuje zdola nahoru směřující konečná posloupnost na sebe navazujících úseček z bodu  $x$  do bodu  $y$ .

**Příklad.** V uspořádané množině  $Y = \{a, b, c, d\}$  s diagramem vpravo platí:

- $d \triangleleft c$ ,  $c \triangleleft a$ ,  $c \triangleleft b$ ,
- $d < a$ , ale nikoliv  $d \triangleleft a$ ,
- prvky  $a, b$  nejsou srovnatelné.



□

**Definice 7.1.4.** Bud'  $(X, \leq)$  uspořádaná množina,  $Y \subseteq X$ . Prvek  $x \in X$  je

- *dolní závora* množiny  $Y$ , je-li  $x \leq y$  pro každé  $y \in Y$ ;
- *horní závora* množiny  $Y$ , je-li  $y \leq x$  pro každé  $y \in Y$ .

**Příklad.** V uspořádané množině  $Y$  z předchozího příkladu platí:

- $c, d$  jsou dolní závory podmnožiny  $\{a, b\}$ ,
- podmnožina  $\{a, b\}$  nemá žádnou horní závoru.

□

**Definice 7.1.5.** Bud'  $(X, \leq)$  uspořádaná množina. Prvek  $x \in X$  je

- *nejmenší (minimální)* prvek množiny  $X$ , je-li  $x \leq y$  pro každé  $y \in X$ , v takovém případě píšeme  $x = \min X$ ;
- *největší (maximální)* prvek množiny  $X$ , je-li  $x \geq y$  pro každé  $y \in X$ , v takovém případě píšeme  $x = \max X$ .

**Příklad.** V uspořádané množině  $Y$  z předchozího příkladu platí:

- $d$  je její nejmenší prvek,
- její největší prvek neexistuje.

□

**Cvičení.** Každá uspořádaná množina má nejvýše jeden největší prvek a nejvýše jeden nejmenší prvek. □

**Definice 7.1.6.** Bud'  $(X, \leq)$  uspořádaná množina,  $Y \subseteq X$ . Prvek  $x \in X$  je

- *infimum* množiny  $Y$ , je-li  $x$  největší prvek množiny všech dolních závor množiny  $Y$ , v takovém případě píšeme  $x = \inf Y$ ,
- *supremum* množiny  $Y$ , je-li  $x$  nejmenší prvek množiny všech horních závor množiny  $Y$ , v takovém případě píšeme  $x = \sup Y$ .

**Příklad.** V uspořádané množině  $Y$  z předchozího příkladu platí:

- množina dolních závor podmnožiny  $\{a, b\}$  je  $\{c, d\}$ , její největší prvek je  $c$ , a proto  $\inf\{a, b\} = c$ ,
- podmnožina  $\{a, b\}$  nemá žádnou horní závoru, čili množina horních závor je prázdná, nemá tedy nejmenší prvek, a proto  $\sup\{a, b\}$  neexistuje. □

**Cvičení.** (1) Každá podmnožina má nejvýše jedno supremum a nejvýše jedno infimum.

- (2) Jestliže  $x \leq y$ , pak  $\inf\{x, y\} = x$  a  $\sup\{x, y\} = y$ .
- (3) Jestliže  $\inf\{x, y\} = x$ , pak  $x \leq y$ .
- (4) Jestliže  $\sup\{x, y\} = y$ , pak  $x \leq y$ . □

**Cvičení.** Buď  $X$  uspořádaná množina. Supremum prázdné množiny je nejmenší prvek množiny  $X$  (pokud existuje) a infimum prázdné množiny je největší prvek množiny  $X$  (pokud existuje). □