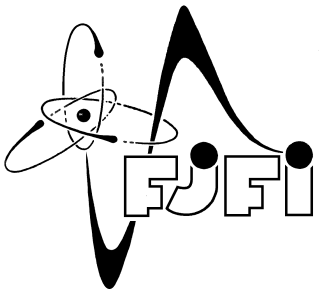


Fakulta jaderná a fyzikálně inženýrská
ČVUT v Praze

# Algebra

*řešené příklady z cvičení*

Podle cvičení předmětu 01ALGE v zimním semestru 2021/22 zpracovala

*Daniela Opočenská*

Praha, 2021

# Obsah

# 1 Množiny, relace, zobrazení, ekvivalence, uspořádání

**Příklad 1.1.** *Popište množinu* $\mathcal{P}(\mathcal{P}(\{1\}))$.

$\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\} \Rightarrow \mathcal{P}(\mathcal{P}(\{1\})) = \mathcal{P}(\{\emptyset, \{1\}\}) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}$.

**Příklad 1.2.** *Mějme relaci* $\mathcal{R} = \{(1,4), (1,2), (2,2), (3,3), (4,3)\}$. *Najděte* $\mathcal{R}^{-1}$, $\mathcal{R} \circ \mathcal{R}^{-1}$, $\mathcal{R}^{-1} \circ \mathcal{R}$, $\mathcal{R} \circ \mathcal{R}$.

- $\mathcal{R}^{-1} = \{(y,x) \in X \times X \mid (x,y) \in \mathcal{R}\} = \{(4,1), (2,1), (2,2), (3,3), (3,4)\}$,
- $\mathcal{R} \circ \mathcal{R}^{-1} = \{(4,4), (4,2), (2,4), (2,2), (3,3)\}$,
- $\mathcal{R}^{-1} \circ \mathcal{R} = \{(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4)\}$,
- $\mathcal{R} \circ \mathcal{R} = \{(1,3), (1,2), (2,2), (3,3), (4,3)\}$.

**Příklad 1.3.** *Nechť* $A = \{1,2,3,4,5\}$. *Sestrojte relaci na* $A$,

*a) která je reflexivní, ale ne tranzitivní,*

*b) která je tranzitivní a ireflexivní, tj.* $(\forall a \in A)((a,a) \notin \mathcal{R})$.

a) Chceme, aby $(\forall x \in A)((x,x) \in \mathcal{R})$ a také $(\exists x,y,z \in A)((x,y),(y,z) \in \mathcal{R} \wedge (x,z) \notin \mathcal{R})$. Takovou relací je například $\mathcal{R} = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,3)\}$.

b) $\mathcal{R} = \{(1,2), (2,3), (1,3)\}$.

**Příklad 1.4.** *Ukažte, že zobrazení* $f : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$ *nemá žádnou pravou inverzi. Najděte dvě levá inverzní zobrazení k* $f$.

Abychom ukázali, že $f$ nemá levou inverzi, stačí ukázat, že $f$ není surjektivní (viz věta z přednášky). To lze ukázat jednoduše, protože například $2 \in \mathbb{N}$, ale $\sqrt{2} \notin \mathbb{N}$. Proto $2 \notin f(\mathbb{N})$ a $f$ není surjektivní.

Levá inverze $g_L : \mathbb{N} \to \mathbb{N}$ je jednoznačně definovaná na $f(\mathbb{N})$, na zbytku $\mathbb{N}$ ji můžeme definovat jakkoliv. Proto například $g_{L1}(x) = \lfloor \sqrt{x} \rfloor$, $g_{L2}(x) = \lceil \sqrt{x} \rceil$ jsou různé levé inverze. (Pro $x = n^2$ opravdu $g_{L1,2}(x) = n$ a pro ostatní $x$ může být hodnota libovolná.)

**Příklad 1.5.** *Najděte všechny ekvivalence na* $\{1,2,3\}$. *(Uveďte příslušné rozklady na disjunktní sjednocení tříd ekvivalence.)*

Uvědomíme si, že každá ekvivalence na množině $M$ odpovídá rozkladu $M$ na disjunktní sjednocení podmnožin. Naopak každý takový rozklad definuje ekvivalenci na $M$.

- $\{1,2,3\}$ všechny prvky jsou si ekvivalentní,
- $\{1\} \cup \{2,3\}$,

- $\{2\} \cup \{1,3\}$,
- $\{3\} \cup \{1,2\}$,
- $\{1\} \cup \{2\} \cup \{3\}$ tato ekvivalence je rovnost mezi čísly ($1 = 1$, $2 = 2$, $3 = 3$).

Celkem máme 5 různých ekvivalencí.

**Příklad 1.6.** *Kolik ekvivalencí lze definovat na* $\{1,2,3,4\}$*?*

Podíváme se na počet způsobů, jak provést rozklad čtyřprvkové množiny na disjunktní sjednocení podmnožin.

- 4 čísla v jedné množině $\to$ 1 způsob
- 3 čísla v jedné a 1 ve druhé množině $\to \binom{4}{1} = 4$ způsoby
- dvě množiny po dvou prvcích $\to \frac{1}{2} \cdot \binom{4}{2} = 3$ způsoby (dělí se 2 kvůli nezávislosti na pořadí množin)
- dva prvky v jedné množině a pak jeden ve druhé a jeden ve třetí $\to \binom{4}{2} = 6$ způsobů
- každý prvek samostatně v množině $\to$ 1 způsob

Celkem tedy máme $1 + 4 + 3 + 6 + 1 = 15$ různých ekvivalencí na množině obsahující 4 prvky.

**Příklad 1.7.** *Nechť* $\sim_1$, $\sim_2$ *jsou ekvivalence na* $X$*. Relaci* $\sim$ *na* $X$ *definujeme následovně:* $a \sim b$*, když* $a \sim_1 b \wedge a \sim_2 b$*. Dokažte, že* $\sim$ *je ekvivalence na* $X$*, a popište třídy této ekvivalence. Co by se stalo, kdyby v definici* $\sim$ *bylo* $\vee$ *místo* $\wedge$*?*

Napřed opět ověříme, zda $\sim$ má všechny vlastnosti ekvivalence.

- **Reflexivita:** Chceme ukázat, že $a \sim a$.
  Ze skutečnosti, že $\sim_1$ i $\sim_2$ jsou ekvivalence, a tedy reflexivní, vyplývá $a \sim_1 a \wedge a \sim_2 a \Rightarrow a \sim a$.
- **Tranzitivita:** Chceme ukázat, že $a \sim b \wedge b \sim c \Rightarrow a \sim c$.
  Máme tedy $a, b, c \in X$ takové, že $a \sim b$ a $b \sim c$. Pak $a \sim_1 b$ a $b \sim_1 c$ a z tranzitivity $\sim_1$ také $a \sim_1 c$. Dále $a \sim_2 b$ a $b \sim_2 c$ a z tranzitivity $\sim_2$ také $a \sim_2 c$. Proto $a \sim c$.
- **Symetrie:** Chceme ukázat, že $a \sim b \Rightarrow b \sim a$.
  Opět si stačí uvědomit, že $\sim_1$ a $\sim_2$ jsou ekvivalence, a proto symetrické. Proto $a \sim_1 b \Rightarrow b \sim_1 a$ a $a \sim_2 b \Rightarrow b \sim_2 a$, takže $b \sim a$.

$\sim$ je tedy ekvivalence na $X$. Dále vidíme, že $a \sim b \Leftrightarrow a \sim_1 b \wedge a \sim_2 b$, a proto $[a]_\sim = [a]_{\sim_1} \cap [a]_{\sim_2}$.

Pokud bychom v definici nahradili $\wedge$ za $\vee$, výsledná relace by již nemusela být ekvivalencí. Nemohli bychom totiž bez dodatečných omezení na $\sim_1$ a $\sim_2$ říci nic o tranzitivitě. Mohlo by totiž nastat, že $x \sim_1 y$ a $y \sim_2 z$. Pak platí, že $x \sim y$ a $y \sim z$, ale již nevíme nic o vztahu $x$ a $z$.

**Příklad 1.8.** *Definujeme relaci na* $\mathbb{Z}^+ \times \mathbb{Z}^+$ *takto* $(a,b) \sim (c,d)$*, když* $ad = bc$*. Dokažte, že* $\sim$ *je ekvivalence, a popište třídy* $\sim$*.*

Opět ověříme reflexivitu, symetrii a tranzitivitu.

- **Reflexivita:** Vidíme, že $a \cdot b = a \cdot b$, proto $(a,b) \sim (a,b)$.
- **Symetrie:** Vidíme, že $ad = bc \Leftrightarrow cb = da$, proto $(a,b) \sim (c,d) \Leftrightarrow (c,d) \sim (a,b)$.
- **Tranzitivita:** Mějme $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f)$. Pak $ad = bc$ a $cf = ed$. Přenásobením první rovnice $f$ a druhé $b$ získáme $adf = bcf = edb$. Nakonec můžeme rovnici zkrátit $d$ a získáme $af = eb$, což znamená $(a,b) \sim (e,f)$.

Zadaná relace je reflexivní, symetrická i tranzitivní a je to tedy ekvivalence.
$[(a,b)]_\sim = \{(c,d) \in \mathbb{N} \times \mathbb{N} \mid ad = bc\} = \left\{(c,d) \in \mathbb{N} \times \mathbb{N} \mid \frac{c}{d} = \frac{a}{b}\right\}$ Tato ekvivalence tedy reprezentuje rovnost mezi kladnými racionálními čísly ($\frac{1}{2} = \frac{2}{4} \dots$).

**Příklad 1.9.** *Definujeme relaci na* $\mathbb{Z}^+ \times \mathbb{Z}^+$ *takto* $(a,b) \sim (c,d)$*, když* $a + d = b + c$*. Dokažte, že* $\sim$ *je ekvivalence, a popište třídy* $\sim$*.*

Opět ověříme reflexivitu, symetrii a tranzitivitu.

- **Reflexivita:** Vidíme, že $a + b = a + b$, proto $(a,b) \sim (a,b)$.
- **Symetrie:** Vidíme, že $a+d = b+c \Leftrightarrow c+b = d+a$, proto $(a,b) \sim (c,d) \Leftrightarrow (c,d) \sim (a,b)$.
- **Tranzitivita:** Mějme $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f)$. Pak $a + d = b + c$ a $c + f = e + d$. Přičtením $f$ k první rovnici a $b$ ke druhé získáme $a + d + f = b + c + f = e + d + b$. Nakonec můžeme od obou stran rovnice odečíst $d$ a získáme $a + f = e + b$, což znamená $(a,b) \sim (e,f)$.

Zadaná relace je reflexivní, symetrická i tranzitivní a je to tedy ekvivalence.
$[(a,b)]_\sim = \{(c,d) \in \mathbb{N} \times \mathbb{N} \mid a + d = b + c\} = \{(c,d) \in \mathbb{N} \times \mathbb{N} \mid a - b = c - d\}$ Třídy ekvivalence jsou tvořeny prvky, které mají stejný rozdíl mezi první a druhou složkou ($[(1,2)]_\sim = \{(1,2),(2,3),(3,4),(4,5)\dots\}$).

**Příklad 1.10.** *Na množině* $A = \{0, 1, \dots, n-1\}$ *definujeme relaci* $\sim$ *následovně:*
$a \sim b$*, pokud* $\exists x \in \mathbb{Z}$*,* $x \perp n$ *tak, že* $ax \equiv b \mod n$*. Dokažte, že* $\sim$ *je ekvivalence na* $A$*. Určete třídy ekvivalence pro* $n = 12$*.*

Ekvivalence musí být reflexivní, symetrická a tranzitivní.

1. **Reflexivita:** Chceme ukázat, že $a \sim a$.
   Položíme-li v definici relace $x := 1$, pak $x \perp n$ a $a \cdot 1 = a \equiv a \mod n$. Tudíž $a \sim a$.

2. **Tranzitivita:** Chceme ukázat, že $a \sim b \wedge b \sim c \Rightarrow a \sim c$.
   Máme tedy $a, b, c \in A$ takové, že $a \sim b$ a $b \sim c$. Pak $\exists x, y \in \mathbb{Z}, x, y \perp n$ takové, že $ax \equiv b \mod n$ a $by \equiv c \mod n$. Po přenásobení první kongruence číslem $y$ získáme

$$a(xy) \equiv by \equiv c \mod n.$$

   Dále víme, že $x, y$ jsou obě s $n$ nesoudělná, proto i $xy \perp n$. Tudíž $a \sim c$.

3. **Symetrie:** Chceme ukázat, že $a \sim b \Rightarrow b \sim a$.
   $a \sim b \Rightarrow (\exists x \in \mathbb{Z}, x \perp n)\ (ax \equiv b \mod n)$. Ze skutečnosti, že $\text{nsd}(x, n) = 1$ dle Bézoutova lemmatu vyplývá, že $\exists k, l \in \mathbb{Z}$ takové, že $kx - ln = 1$. Dále můžeme vidět, že jistě $k \perp n$ (jinak by jejich největší společný dělitel dělil levou stranu, musel by pak ale dělit i pravou, na které je 1). Z rovnice získáme, že $kx \equiv 1 \mod n$. Přenásobením definičního vztahu pro relaci číslem $k$ získáme

$$axk \equiv a \cdot 1 \equiv bk \mod n.$$

   Nakonec si uvědomíme, že kongruence je ekvivalence, a tudíž je symetrická. Proto $b \sim a$.

Zadaná relace má všechny vlastnosti potřebné k tomu, aby to byla ekvivalence. Dále nalezneme třídy ekvivalence. Uvědomíme si, že pokud za $x$ v definici ekvivalence vezmeme číslo větší než 12, bude výsledek stejný, jako když vezmeme číslo $x - 12$ (nesoudělnost s číslem 12 se také zachovává). Proto stačí uvažovat $x < 12$. Dále kvůli podmínce nesoudělnosti $x \in \{1, 5, 7, 11\}$. Proto

- $[0]_\sim = \{0\}$
- $[1]_\sim = \{1, 5, 7, 11\} = [5]_\sim = [7]_\sim = [11]_\sim$
- $[2]_\sim = \{2, 10\} = [10]_\sim$ protože $(2 \cdot 7 = 14 \equiv 2 \mod 12,\ 2 \cdot 11 = 22 \equiv 10 \mod 12)$
- $[3]_\sim = \{3, 9\} = [9]_\sim$ protože $(3{\cdot}5 = 15 \equiv 3 \mod 12, 3{\cdot}7 = 21 \equiv 9 \mod 12, 3{\cdot}11 = 33 \equiv 9 \mod 12)$
- $[4]_\sim = \{4, 8\} = [8]_\sim$ protože $(4{\cdot}5 = 20 \equiv 8 \mod 12, 4{\cdot}7 = 28 \equiv 4 \mod 12, 4{\cdot}11 = 44 \equiv 8 \mod 12)$
- $[6]_\sim = \{6\}$ protože $(6 \cdot 5 = 30 \equiv 6 \mod 12,\ 6 \cdot 7 = 42 \equiv 6 \mod 12,\ 6 \cdot 11 = 66 \equiv 6 \mod 12)$

Disjunktních tříd ekvivalence je tedy 6.

**Příklad 1.11.** *Rozhodněte, zda následující relace jsou uspořádání na daných množinách.*

*a)* $(\mathbb{N} \times \mathbb{N}, \preceq)$*, kde* $(a, b) \preceq (c, d)$*, když* $a \leq c$*,*

*b)* $(\mathbb{N} \times \mathbb{N}, \preceq)$*, kde* $(a, b) \preceq (c, d)$*, když* $a \leq c \wedge b \geq d$*.*

*Pokud ano, je toto uspořádání úplné? Je dobré?*

a) Podíváme-li se na předpis, můžeme vidět, že problematickým bodem by mohla být antisymetrie, zkontrolujeme tedy napřed tu.
**Antisymetrie:** Chceme ukázat, že $(a,b) \preceq (c,d) \wedge (c,d) \preceq (a,b) \Rightarrow (a,b) = (c,d)$.
Z definice pak $a \leq c \wedge c \leq a$, proto $a = c$. Již ale není nutné, aby $b = d$. Relace proto není ekvivalencí a nemusíme kontrolovat další body (ty ale jsou splněny).

b) **Antisymetrie:** Chceme ukázat, že $(a,b) \preceq (c,d) \wedge (c,d) \preceq (a,b) \Rightarrow (a,b) = (c,d)$.
Z definice $(a \leq c \wedge b \geq d) \wedge (c \leq a \wedge d \geq b)$. Proto $a = c$ a $b = d$.
**Reflexivita:** Chceme ukázat, že $(a,b) \preceq (a,b)$.
Víme, že $a \leq a$ a $b \geq b$, proto $(a,b) \preceq (a,b)$.
**Tranzitivita:** Chceme ukázat, že $(a,b) \preceq (c,d) \wedge (c,d) \preceq (e,f) \Rightarrow (a,b) \preceq (e,f)$.
Podíváme se napřed na první složky: $a \leq c \leq e \Rightarrow a \leq e$. (Využíváme tranzitivity $\leq$ na $\mathbb{N}$.)
U druhých složek $b \geq d \geq f \Rightarrow b \geq f$. Proto $(a,b) \preceq (e,f)$.

Toto uspořádání není úplné. Stačí se podívat například na dvojici $(1,2),(3,4)$, která dle definice není porovnatelná. (Obecně jsou neporovnatelné dvojice $a \leq c \wedge b \leq d$ nebo $a \geq c \wedge b \geq d$.) Protože toto uspořádání není úplné, není ani dobré.

**Příklad 1.12.** *Mějme* $X = \{\{1\},\{2\},\{4\},\{1,2\},\{1,4\},\{2,4\},\{3,4\},\{1,3,4\},\{2,3,4\}\}$ *s uspořádáním inkluzí. Najděte*

*a) všechny maximální a minimální prvky v* $X$*,*

*b) nejmenší a největší prvek,*

*c) všechny horní závory množiny* $\{\{2\},\{4\}\}$*,*

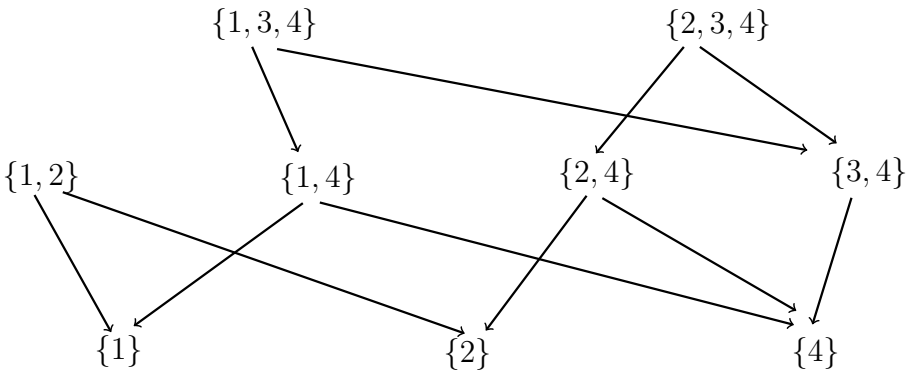
*d) všechny dolní závory množiny* $\{\{1,3,4\},\{2,3,4\}\}$*.*

a) Z obrázku 1 můžeme vidět, že maximálními prvky množiny jsou ty, do kterých nevchází hrana seshora, tedy $\{1,3,4\},\{2,3,4\}$ a $\{1,2\}$. Naopak minimální prvky jsou ty, ze kterých nevychází hrana dolů, tedy $\{1\},\{2\},\{4\}$.

b) $X$ nemá nejmenší ani největší prvek.

c) Horní závory množiny $\{\{2\},\{4\}\}$ jsou prvky $\{2,4\},\{2,3,4\}$.

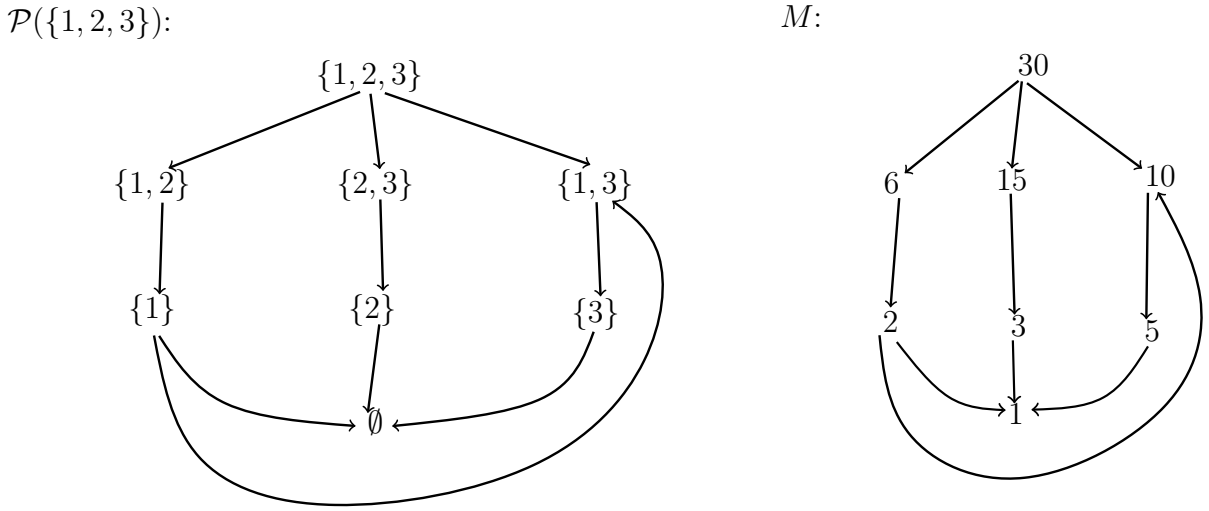
d) Dolní závory množiny $\{\{1,3,4\},\{2,3,4\}\}$ jsou prvky $\{3,4\}$ a $\{4\}$.




Obrázek 1: Hasseho diagram k příkladu 1.12

**Příklad 1.13.** *Najděte izomorfismus (podobnost) mezi uspořádanými množinami* $\mathcal{P}(\{1,2,3\})$ *s inkluzí a* $M = \{d \in \mathbb{N} \mid d \text{ dělí } 30\}$ *s dělením. Kolik je takových izomorfismů?*

Napřed si uvědomíme, že izomorfní zobrazení mezi konečnými uspořádanými množinami musí zachovat Hasseho diagram, takže si ho napřed pro obě množiny nakreslíme.




Obrázek 2: Hasseho diagram k příkladu 1.13

Zkonstruujeme izomorfismus $f : \mathcal{P}(\{1,2,3\}) \to M$. Izomorfismus $f$ musí zachovat vlastnost být největším nebo nejmenším prvkem, proto

- $f(\emptyset) = 1$
- $f(\{1,2,3\}) = 30$

V další volbě máme díky symetrii Hasseho diagramu jistou volbu, můžeme zvolit vždy jednu uspořádanou dvojici ze tří prvků, další prvky jsou pak jasně určeny. Například zvolíme

- $f(\{1\}) = 2$
- $f(\{2\}) = 3$

Pak již nemáme jinou možnost než

- $f(\{3\}) = 5$
- $f(\{1,2\}) = 6$
- $f(\{2,3\}) = 15$
- $f(\{1,3\}) = 10$

Při jiné volbě, například

- $f(\{2\}) = 2$
- $f(\{3\}) = 3$

Získáme

- $f(\{1\}) = 5$
- $f(\{1,2\}) = 10$
- $f(\{2,3\}) = 6$
- $f(\{1,3\}) = 15$

Jak již bylo řečeno, izomorfismus není jediný, je tu jistá volnost při vybírání ze druhé resp. třetí řady. Proto mezi množinami existuje 6 různých izomorfismů.

**Příklad 1.14.** *Nechť $M$ je dobře uspořádaná množina. Najděte* úplné *uspořádání na $\mathcal{P}(M)$. (Využijte symetrickou diferenci množin.)*

Napřed připomeňme, co je symetrická diference množin $A, B$: $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Pak pro $A, B \in \mathcal{P}(M)$ definujeme $A \leq B$, pokud $A = B$ nebo nejmenší prvek z množiny $A \triangle B$ leží v $A$. Nejmenší prvek vždy existuje a je dán jednoznačně, protože $A \triangle B \subset M$ je úplně uspořádaná množina. Nyní musíme ukázat, že jsme opravdu definovali uspořádání:

- **Reflexivita:** $A = A$, proto i $A \leq A$ z definice.
- **Antisymetrie:** Předpokládejme $A \leq B$ a $B \leq A$. Z prvního vztahu buď $A = B$ a antisymetrie je splněna, nebo nejmenší prvek $A \triangle B$ leží v $A$. Z druhého vztahu pak nejmenší prvek $B \triangle A = A \triangle B$ leží v B, což je spor, protože nejmenší prvek je jen jeden a $A \cap B \cap (A \triangle B) = \emptyset$.
- **Tranzitivita:** Předpokládejme, že $A \leq B$ a $B \leq C$. Pak v případě $A = B$ nebo $B = C$ jistě platí $A \leq C$. Uvažujme tedy případ $A \neq B \neq C$. Určitě $A \neq C$, protože jinak by se jejich symetrické diference s B rovnaly a nemohlo by zároveň nastat $A \leq B$ a $B \leq C$.

  Nechť $a \in A \triangle B$, $b \in B \triangle C$ a $c \in C \triangle A$ jsou nejmenší prvky příslušných množin. Stačí nám uvažovat, že nejmenší prvky množin $A, B, C$ jsou si rovny, jinak by nejmenší prvky z diferencí byly zároveň nejmenšími prvky množin a tranzitivita by byla splněna.

  Pak situace vypadá následovně:

  - Množiny $A$ a $B$ mají společné všechny prvky od nejmenšího až do $a$, kde $a \in A$, $a \notin B$.
  - Množiny $B$ a $C$ mají společné všechny prvky od nejmenšího až do $b$, kde $b \in B$, $b \notin C$.

– Nenastává $a = b$.

– Množiny $A$ a $C$ mají společné všechny prvky od nejmenšího až do $\min\{a, b\}$.

Uvažujme dvě situace:

$a < b$: Pak množiny $A$ a $C$ mají společné všechny prvky až do $a$. Protože $C$ má s $B$ společné všechny prvky, jistě $a \notin C$. Proto $c = a \in A$.

$a > b$: Pak jistě $b \in B \Rightarrow b \in A$, protože $A$ a $B$ mají společné všechny prvky do $a > b$. Dále $b \notin C$ z definice, a proto $b$ je nejmenším prvkem množiny $A \triangle C$.

V obou případech dostáváme $c \in A$, tudíž $A \leq C$.

Dále musíme ukázat, že uspořádání je úplné, tzn. každé dvě podmnožiny $M$ dokážeme porovnat. To je ale jistě splněno, protože buď $A = B$, nebo symetrická diference má nejmenší prvek, který musí ležet v jedné z množin (a nemůže ležet v obou současně).

**Příklad 1.15.** *Nechť $\mathcal{F}$ je systém všech řetězců v uspořádané množině $M$. Dokažte, že platí: Je-li $\mathcal{F}' \subset \mathcal{F}$ řetězcem v $\mathcal{P}(M)$ (při uspořádání inkluzí), pak $\bigcup_{F \in \mathcal{F}'} F$ je řetězcem v $M$.*

Připomeňme, že řetězec v uspořádané množině je neprázdná úplně uspořádaná podmnožina. Chceme ukázat, že každý pár prvků $x, y \in \subset \bigcup_{F \in \mathcal{F}'} F$ je porovnatelný. Zřejmě existují množiny $A_x, A_y \in \mathcal{F}'$ takové, že $x \in A_x, y \in A_y$. Protože $\mathcal{F}'$ je řetězec, množiny $A_x, A_y$ jsou inkluzí porovnatelné, tedy bez újmy na obecnosti například $A_x \subset A_y$, a tedy $A_y$ obsahuje oba prvky $x, y$. Navíc $A_y \in \mathcal{F}' \subset \mathcal{F}$, takže $A_y$ je řetězec v $M$. Proto jsou prvky $x, y$ porovnatelné.

# 2 Mohutnost, ekvivalence množin, ordinální čísla

**Příklad 2.1.** *Jsou-li $X, Y, S, T$ množiny, $\simeq$ ekvivalence množin (tzn. existence bijekce mezi nimi), dokažte*

*a)* $(S \times T)^X \simeq S^X \times T^X$,

*b)* $S^{X \times Y} \simeq (S^X)^Y$,

*c)* $S^{X \dot\cup Y} \simeq S^X \times S^Y$.

Zpracováno ve skriptech.

**Příklad 2.2.** *Definujme aritmetiku na kardinalitách množin takto: Jsou-li $A, B$ množiny $\kappa = \mathrm{card}A$, $\lambda = \mathrm{card}B$, pak*

- $\kappa + \lambda := \mathrm{card}(A \dot\cup B)$,
- $\kappa \cdot \lambda := \mathrm{card}(A \times B)$,
- $\kappa^\lambda := \mathrm{card}(A^B)$,

1. *Vysvětlete, proč u konečných množin jsou tyto operace kompatibilní s operacemi v $\mathbb{N}_0$.*
2. *Dokažte*
   - $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$,
   - $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$,
   - $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$,
   - *pro $\kappa \leq \lambda$ platí $\kappa^\mu \leq \lambda^\mu$,*
   - *pro $0 < \lambda \leq \mu$ platí $\kappa^\lambda \leq \kappa^\mu$,*
   - $1^\lambda = 1$.

1. U konečných množin kardinalita odpovídá počtu prvků. Disjunktní sjednocení odpovídá součtu prvků. Kartézský součin má tolik prvků, kolik je možných dvojic, což je $|A| \cdot |B|$. Nakonec počet zobrazení z $B$ do $A$ odpovídá počtu možností, jak lze každému prvku z $B$ přiřadit jeden z $A$, což je $|A|^{|B|}$.

2. Budeme hojně využívat výsledků příkladu 2.1.
   - $(\kappa \cdot \lambda)^\mu = \mathrm{card}((A \times B)^C) = \mathrm{card}(A^C \times B^C) = \mathrm{card}(A^C)\mathrm{card}(B^C) = \kappa^\mu \cdot \lambda^\mu$,
   - $\kappa^{\lambda+\mu} = \mathrm{card}(A^{(B \dot\cup C)}) = \mathrm{card}(A^B \times A^C) = \mathrm{card}(A^B)\mathrm{card}(A^C) = \kappa^\lambda \cdot \kappa^\mu$,
   - $(\kappa^\lambda)^\mu = \mathrm{card}((A^B)^C) = \mathrm{card}(A^{B \times C}) = \kappa^{\lambda \cdot \mu}$,
   - pro $\kappa \leq \lambda$ platí $\kappa^\mu \leq \lambda^\mu$:
     $\mathrm{card}(A) \leq \mathrm{card}(B)$ říká, že existuje prosté zobrazení $f : A \to B$. Pak vezmeme-li $\varphi : C \to A$ a položíme $g : A^C \to B^C : \varphi \mapsto f \circ \varphi$, pak $g$ je prosté. ($g(\varphi) = g(\psi) \Rightarrow \varphi = \psi$ – z prostoty zobrazení $f$.) Proto $\mathrm{card}(A^C) \leq \mathrm{card}(B^C)$.
   - pro $0 < \lambda \leq \mu$ platí $\kappa^\lambda \leq \kappa^\mu$,
     $\mathrm{card}(B) \leq \mathrm{card}(C)$, proto opět máme $f : B \to C$ prosté zobrazení. K prostému zobrazení existuje levá inverze. Dále definujeme $g : A^B \to A^C : \varphi \mapsto \varphi \circ f_L^{-1}$. Pak

$g$ je prosté. Vezmeme $\varphi, \psi : B \to A$ Pak $g(\varphi) = g(\psi) \Rightarrow \varphi \circ f_L^{-1} = \psi \circ f_L^{-1}$. Nyní můžeme funkce složit zprava s $f$ a získáme $\varphi = \psi$. Našli jsme tedy prosté zobrazení z $A^B$ do $A^C$ a proto $\mathrm{card}(A^B) \leq \mathrm{card}(A^C)$.

- $1^\lambda = 1$. Existuje pouze jediné zobrazení $f \in \{1\}^A$, a to $f(a) = 1$, $\forall a \in A$. Proto množina $1^A$ obsahuje 1 prvek.

**Věta 2.1** (Cantorova-Bernsteinova-Schröderova, CBS)**.** *Nechť $M, N$ jsou množiny takové, že $\exists f : M \to N$ a $g : N \to M$ obě injektivní. Pak $N, M$ jsou ekvivalentní.*

**Příklad 2.3.** *Pomocí CBS dokažte, že $\mathbb{N}$ je ekvivalentní systému všech konečných podmnožin množiny $\mathbb{N}$.*

Systém všech konečných podmnožin $\mathbb{N}$ označíme $M$. Najdeme dvě injektivní zobrazení $f : \mathbb{N} \to M$ a $g : M \to \mathbb{N}$. Pak z CBS vyplyne, že $N$ je ekvivalentní s $M$. Možností, jak definovat tato prostá zobrazení je několik, uvedeme pouze jeden příklad.

$f$: $f(n) := \{n\}$ pro všechna $n \in \mathbb{N}$. Takové zobrazení je jistě prosté a jeho oborem hodnot je podmnožina $M$.

$g$: Vezměme libovolnou konečnou podmnožinu $A \subset \mathbb{N}$. Označme $k$ její největší prvek vzhledem k běžnému uspořádání na $\mathbb{N}$. Pak položíme

$$g(A) := u_k u_{k-1} \dots u_2 u_1,$$

jako zápis cifer ve dvojkové soustavě, kde $u_i = 1$ když $i \in A$ a $u_i = 0$ jinak, tj. $u_i = \chi_A(i)$.

Například pro $A = \{3, 4, 6\}$ získáme $g(A) = 101100$. Zjevně $g(M) \subset \mathbb{N}$ a zobrazení $g$ je prosté.

**Příklad 2.4.** *Pomocí CBS dokažte, že $(0, 1) \sim (0, 1) \times (0, 1)$.*

Opět nalezneme dvě prostá zobrazení $f : (0, 1) \to (0, 1) \times (0, 1)$ a $g : (0, 1) \times (0, 1) \to (0, 1)$

$f$: Volíme $x_0 \in (0, 1)$ libovolně a položíme $f(x) = (x_0, x)$ pro všechna $x \in (0, 1)$.

$g$: Pro $x, y \in (0, 1)$ uvažujme jejich zápisy v desítkové soustavě, tj. $x = 0, x_0 x_1 x_2 \dots$ a $y = 0, y_0 y_1 y_2 \dots$, kde předpokládáme, že rozvoje nekončí na nekonečně 9 (a tudíž jsou jednoznačné). Pokládáme $g(x, y) := 0, x_0 y_0 x_1 y_1 x_2 y_2 \dots$. I toto zobrazení je díky jednoznačnosti rozvojů prosté.

**Příklad 2.5.** *Jestliže $(M_1, \leq_1)$ a $(M_2, \leq_2)$ jsou dobře uspořádané množiny, dokažte, že jejich uspořádané sjednocení $M_1 + M_2$ a jejich uspořádaný kartézský součin $M_1 \cdot M_2$ jsou rovněž dobře uspořádané množiny.*

- $M_1 + M_2$: Víme, že $M_1 + M_2 = (M_1 \dot\cup M_2, \leq)$, kde $x \leq y$ pokud $x, y \in M_i$ a $x \leq_i y$, nebo $x \in M_1$ a $y \in M_2$.

  Vezmeme $K \subset M_1 + M_2, K \neq \emptyset$. Pak množiny $K \cap M_1 \subset M_1$ a $K \cap M_2 \subset M_2$ jsou buď prázdné, nebo obsahují nejmenší prvek z vlastnosti dobrého uspořádání $M_1, M_2$. Pokud je jedna z množin prázdná, pak $K$ je celé podmnožinou $M_i$ a nejmenší prvek v $K$ je zároveň nejmenším prvkem v $K \cap M_i$. Obě nemohou být zároveň prázdné, protože $K \neq \emptyset$. Pokud jsou obě neprázdné, pak víme, že $\forall x \in K \cap M_1$ a $\forall y \in K \cap M_2$, $x < y$, proto nejmenší prvek z množiny $K \cap M_1$ je zároveň nejmenším prvkem množiny $K$.

  V obou případech jsme nalezli nejmenší prvek množiny $K$, která byla vybrána libovolně, $M_1 + M_2$ je tedy dobře uspořádaná.

- $M_1 \times M_2$: $(x_1, y_1) \leq (x_2, y_2)$, pokud $y_1 < y_2$, nebo $y_1 = y_2$ a $x_1 \leq x_2$.

  Opět vezmeme $K \subset M_1 \times M_2, K \neq \emptyset$. $K$ je tedy množina uspořádaných dvojic. Definujme množinu $K_y := \{y \in M_2 \mid (\exists x \in M_1)((x, y) \in K)\} \subset M_2$. Z neprázdnosti $K$ vyplývá neprázdnost $K_y$, a proto $K_y$ obsahuje nejmenší prvek, označme ho $y_{min}$. Dále definujme $K_x = \{x \in M_1 \mid (x, y_{min}) \in K\} \subset M_1$. Tato množina je neprázdná a obsahuje proto nejmenší prvek, označme ho $x_{min}$. Pak prvek $(x_{min}, y_{min})$ je nejmenším prvek množiny $K$.

  Opět jsme nalezli nejmenší prvek množiny $K$, která byla vybrána libovolně. $M_1 \times M_2$ je proto dobře uspořádaná.

**Příklad 2.6.** *Dokažte, že sčítání a násobení ordinálních čísel jsou asociativní operace.*

- $\lambda + (\kappa + \mu) = (\lambda + \kappa) + \mu$:

$$\lambda + (\kappa + \mu) = \lambda + \mathrm{ord}(B \dot\cup C) = \mathrm{ord}(A \dot\cup (B \dot\cup C))$$
$$(\lambda + \kappa) + \mu = \mathrm{ord}(A \dot\cup B) + \mu = \mathrm{ord}((A \dot\cup B) \dot\cup C)$$

  Nyní si stačí uvědomit, že disjunktní sjednocení je asociativní operace a uspořádání množin $A \dot\cup (B \dot\cup C)$ a $(A \dot\cup B) \dot\cup C)$ je také stejné (v obou případech máme $a_1 < a_2 < \cdots < b_1 < b_2 < \cdots < c_1 < c_2 < \cdots$). Proto se i jejich ordinální čísla budou rovnat.

- $\lambda \cdot (\kappa \cdot \mu) = (\lambda \cdot \kappa) \cdot \mu$:

$$\lambda \cdot (\kappa \cdot \mu) = \lambda \cdot \mathrm{ord}(B \times C) = \mathrm{ord}(A \times (B \times C))$$
$$(\lambda \cdot \kappa) \cdot \mu = \mathrm{ord}(A \times B) \cdot \mu = \mathrm{ord}((A \times B) \times C)$$

  Nyní si musíme uvědomit, že $A \times (B \times C) = \{(a, (b, c)) \mid a \in A, b \in B, c \in C\}$ a platí $(a_1, (b_1, c_1)) \leq (a_2, (b_2, c_2))$, pokud

  - $c_1 < c_2$,
  - $c_1 = c_2$ a $b_1 < b_2$,
  - $c_1 = c_2$ a $b_1 = b_2$ a $a_1 \leq a_2$.

Proto máme $(a_1,(b_1,c_1)) < (a_2,(b_1,c_1)) < \cdots < (a_1,(b_2,c_1)) < (a_2,(b_2,c_1)) < \cdots < (a_1,(b_1,c_2)) < \cdots$.

Obdobně $(A \times B) \times C = \{((a,b),c) \mid a \in A, b \in B, c \in C\}$ a platí $((a_1,b_1),c_1)) \leq ((a_2,b_2),c_2)$, pokud

- $c_1 < c_2$,
- $c_1 = c_2$ a $b_1 < b_2$,
- $c_1 = c_2$ a $b_1 = b_2$ a $a_1 \leq a_2$.

Proto máme stejné uspořádání $((a_1,b_1),c_1) < ((a_2,b_1),c_1) < \cdots < ((a_1,b_2),c_1) < ((a_2,b_2),c_1) < \cdots < ((a_1,b_1),c_2) < \cdots$.

Proto vezmeme-li $f : A \times (B \times C) \to (A \times B) \times C : (a,(b,c)) \mapsto ((a,b),c)$, pak jsme našli izomorfismus dobře uspořádaných množin, jejich ordinální čísla se tedy rovnají.

**Příklad 2.7.** *Dokažte, že pro ordinální čísla platí levý distributivní zákon, tj.*

$$(\forall \alpha, \beta, \gamma)(a(\beta + \gamma) = \alpha\beta + \alpha\gamma).$$

*Dokažte, že pravý distribuční zákon obecně neplatí.*

Napřed ukážeme, že pravý distributivní zákon neplatí, protože například $(1+1)\omega = 2 \cdot \omega = \omega \neq \omega + \omega$, jak bylo ukázáno na přednášce.

$$(\alpha + \beta) \cdot \gamma = \operatorname{ord}(A \times (B + C))$$
$$\alpha\gamma + \beta\gamma = \operatorname{ord}(A \times B + A \times C)$$

Nyní si stačí uvědomit, že množiny $A \times (B + C)$ a $A \times B + A \times C$ jsou podobně uspořádané. $(a_1,b_1) < (a_2,b_1) < \cdots < (a_1,b_2) < (a_2,b_2) < \cdots < (a_1,c_1) < (a_2,c_1) < \cdots < (a_1,c_2) < \cdots$, proto se i jejich ordinální čísla rovnají.

# 3 Obecné algebry, grupoid, pologrupa, monoid

**Příklad 3.1.** *Pro která $u \in \mathbb{R}_0^+$ tvoří množina $A_u = \{z \in \mathbb{C} \mid |z| = u\}$ podalgebru algebry*

*a)* $(\mathbb{C}, +)$, *b)* $(\mathbb{C}, \cdot)$, *c)* $(\mathbb{C} \setminus \{0\}, :)$*?*

a) $(\mathbb{C}, +)$: Víme, že $(\forall u \in \mathbb{R}_0^+)(u \in A_u)$ a $u + u = 2u$. Dále $2u \in A_u$ pouze v případě, kdy $u = 0$. Naopak pro $u = 0$ vidíme, že vznikla triviální algebra $(\{0\}, +)$, která je podalgebrou algebry $(\mathbb{C}, +)$.

b) $(\mathbb{C}, \cdot)$: Vezměme $z, w \in A_u$, pak $z \cdot w = |z||w|e^{i(\phi_z+\phi_w)} = u^2 e^{i(\phi_z+\phi_w)}$. Proto $|zw| = u \Leftrightarrow u = u^2 \Leftrightarrow u = 1 \vee u = 0$.

c) $(\mathbb{C} \setminus \{0\}, :)$ Opět vezměme $z, w \in A_u$, pak $|\frac{z}{w}| = |\frac{u}{u}e^{i(\phi_z-\phi_w)}| = 1$. Proto podíl $\frac{z}{w}$ leží v $A_u$ právě tehdy, když $u = 1$.

**Příklad 3.2.** *Pro která $u \in \mathbb{Z}$ tvoří množina $A_u = \left\{ \begin{pmatrix} a & b \\ ub & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ podalgebru algebry celočíselných matic $2 \times 2$ s operacemi násobení a sčítání matic?*

Prověříme, zda je množina $A_u$ uzavřená na operace násobení a sčítání.

- **Násobení:**
$$\begin{pmatrix} a_1 & b_1 \\ ub_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ ub_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + ub_1b_2 & a_1b_2 + a_2b_1 \\ u(b_1a_2 + a_1b_2) & a_1a_2 + ub_1b_2 \end{pmatrix}$$
Množina $A_u$ je uzavřená na násobení matic pro všechna $u \in \mathbb{Z}$.

- **Sčítání:**
$$\begin{pmatrix} a_1 & b_1 \\ ub_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ ub_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ u(b_1 + b_2) & a_1 + a_2 \end{pmatrix}$$
Množina $A_u$ je uzavřená na sčítání matic pro všechna $u \in \mathbb{Z}$.

Množina $A_u$ je proto podalgebrou algebry $(\mathbb{Z}^{2\times2}, +, \cdot)$ pro všechna $u \in \mathbb{Z}$.

**Příklad 3.3.** *Najděte nekonečné množství podalgeber algebry $(\mathbb{N}, +, \cdot)$.*

Vezměme $k \in \mathbb{N}$ libovolně a definujme

- Množiny $U_k := \{n \in \mathbb{N} \mid n \geq k\}$. Pak $U_k$ je podalgebrou algebry $(\mathbb{N}, +, \cdot)$. Vyplývá to z následujících nerovností $m, l \in U_k \Rightarrow m \cdot l \geq k^2 \geq k \wedge m + l \geq 2k > k$.

- Množiny $V_k := \{n \in \mathbb{N} \mid k \text{ dělí } n\}$. Pak $V_k$ je podalgebrou algebry $(\mathbb{N}, +, \cdot)$. Vyplývá to z vlastností dělitelnosti. $k$ dělí $m, l$, pak $k$ dělí i $m + l$ a $m \cdot l$.

Protože $k$ bylo bráno libovolně, v obou systémech je těchto množin opravdu nekonečně mnoho.

**Příklad 3.4.** *Najděte všechny podalgebry algebry $A = (\{a, b, c, d\}, f)$, kde $f$ je unární operace $f(a) = f(b) = c$, $f(c) = f(d) = d$.*

Podalgebra musí být uzavřena na operaci $f$. Proto získáme následující podalgebry:

- $\{d\}$,
- $\{c, d\}$,
- $\{a, c, d\}$,
- $\{b, c, d\}$,
- $\{a, b, c, d\}$.

**Příklad 3.5.** *Najděte všechny podalgebry grupoidu* $(\{a, b, c, d, e\}, \circ)$*, kde operace* $\circ$ *je dána tabulkou*

| $\circ$ | a | b | c | d | e |
|---|---|---|---|---|---|
| a | a | e | c | a | a |
| b | e | d | e | b | b |
| c | a | e | c | a | c |
| d | c | b | a | e | e |
| e | a | e | a | d | b |

Chceme najít všechny množiny, které jsou uzavřené na operaci $\circ$.

- $a \circ a = a$, proto $(\{a\}, \circ)$ je podalgebra.
- $c \circ c = c$, proto $(\{c\}, \circ)$ je podalgebra. Další jednoprvkové již nejsou.
- Dále $a \circ c = c$, $c \circ a = a$, proto $(\{a, c\}, \circ)$ je podalgebra.
- $(\{b, d, e\}, \circ)$
- $(\{a, b, c, d, e\}, \circ)$

Tyto podalgebry jsou všechny možné, protože přidáme-li do množiny $e$, pak musíme přidat i $e \circ e = b$ a následně i $d$. Pokud je v množině $e$ a $c$, pak musíme přidat $b, d$ kvůli $e$ a dále $e \circ c = a$. Pokud je v množině $e$ a $a$, pak musíme přidat $b, d$ kvůli $e$ a dále $d \circ a = c$. Obdobně pro $d$, $b$ namísto $e$.

**Příklad 3.6.** *Dokažte, že každá pologrupa obsahující neutrální prvek* $e$ *a absorpční prvek* $a$ *takový, že* $e = a$*, je triviální.*

Vezmeme prvek $b$ z grupy. Pak $b = b * e = b * a = a$, kde první rovnost vyplývá z neutrality prvku $e$ a druhá z toho, že $a$ je absorpční prvek. Množina tedy obsahuje pouze prvek $a = e$.

**Příklad 3.7.** *Formulujte, jak lze v Cayleyově tabulce konečné pologrupy zjistit*

1. *existenci neutrálního prvku,*
2. *existenci absorpčního prvku,*
3. *existenci inverzního prvku k danému* $x$*,*
4. *vlastnost pravéhp/levého krácení.*

1. **Existence neutrálního prvku:** Neutrální prvek $e$ znamená $e \circ a = a \circ e = a$ pro všechna $a$ z pologrupy. Proto v Cayleyově tabulce bude ve sloupci, resp. řádku příslušném k $e$ opsaný první sloupec, resp. řádek.

2. **Existence absorpčního prvku:** Absorpční prvek $a$ znamená $a \circ b = b \circ a = a$ pro všechna $b$ z pologrupy. Řádek i sloupec Cayleyovy tabulky příslušný k $a$ tedy bude mít na všech pozicích $a$.

3. **Existence inverzního prvku k danému $x$:** Inverzní prvek $x^{-1}$ splňuje $x \circ x^{-1} = x^{-1} \circ x = e$, kde $e$ je neutrální prvek. V Cayleyově tabulce proto musí být neutrální prvek $e$ (viz první bod), dále v řádku příslušném k $x$ se musí vyskytovat právě $e$ a nakonec se $e$ musí vyskytovat i ve sloupci k $x$ symetricky podle diagonály (aby stejný prvek byl pravou i levou inverzí).

4. **Vlastnost krácení:** Pravé krácení znamená, že binární operace $\circ$ musí splňovat $a \circ c = b \circ c$ implikuje $a = b$. V jednom sloupci Cayleyovy tabulky nemohou být dva stejné prvky. Protože prvků i pozic ve sloupci je stejný počet, obsahuje každý sloupec právě všechny prvky pologrupy. Podobně pro levé krácení $a \circ c = b \circ c$ implikuje $a = b$, a tedy totéž platí pro řádky. Má-li pologrupa pravé i levé krácení, pak Cayleyova tabulka je latinský čtverec.

**Příklad 3.8.** *Popište všechny dvouprvkové pologrupy (až na izomorfismus pologrup).*

Pologrupa je algebra s jednou binární asociativní operací. Obecně musíme sestrojit všechny možné Cayleyovy tabulky nad 2 prvky – 16 tabulek, a poté zkontrolovat, zda nejsou vzájemně izomorfní (například by stačilo prohodit názvy prvků) a zda Cayleyova tabulka zadává **asociativní** operaci. Pokud toto provedeme, získáme 4 tabulky.

| $\circ$ | a | b |
|---|---|---|
| a | a | a |
| b | a | a |

| $\circ$ | a | b |
|---|---|---|
| a | a | a |
| b | a | b |

| $\circ$ | a | b |
|---|---|---|
| a | a | a |
| b | b | b |

| $\circ$ | a | b |
|---|---|---|
| a | a | b |
| b | b | a |

Čtenář může sám ověřit, že tyto tabulky definují asociativní operaci $\circ$.

**Příklad 3.9.** *Najděte monoid $M$ s podpologrupou $N$, která je sama monoidem, ale neutrální prvek v $N$ je jiný než v $M$. Zkuste tak, aby monoid $(N, *, e_N)$ nebyl triviální.*

Triviální příklad je $M = (\mathbb{N}_0, \cdot)$, kde neutrálním prvkem je 1. Jeho podpologrupa je $(\{0\},\cdot)$, kde roli neutrálního prvku hraje 0.

Vezmeme-li například monoid ($\mathbb{N}_0 \times \mathbb{N}_0$, násobení po složkách), pak neutrálním prvkem je $(1, 1)$. Jeho podpologrupou je ($\mathbb{N}_0 \times \{0\}$, násobení po složkách), která je sama monoidem, ale roli neutrálního prvku zde hraje (1,0).

**Příklad 3.10.** *Dokažte, že pologrupy* $(\mathbb{R}, +)$ *a* $(\mathbb{R}^+, \cdot)$ *jsou izomorfní.*

Chceme najít bijekci $f : \mathbb{R} \to \mathbb{R}^+$ takovou, že $f(x + y) = f(x) \cdot f(y)$ pro všechny $x, y \in \mathbb{R}$. Stačí položit $f(x) := e^x$, o tomto zobrazení je dobře známo, že je bijektivní a opravdu $e^{x+y} = e^x e^y$.

**Příklad 3.11.** *Dokažte, že pologrupy* $(\mathbb{R}, +)$ *a* $(\mathbb{R} \setminus \{0\}, \cdot)$ *nejsou izomorfní.*

Důkaz provedeme sporem, budeme předpokládat, že existuje bijekce $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, která splňuje $f(x \cdot y) = f(x) + f(y)$ pro všechna $x, y \in \mathbb{R} \setminus \{0\}$. Uvědomíme si, že zadané pologrupy jsou dokonce grupami s operacemi, jak je známe. Můžeme tedy využít vlastnosti krácení.

Pak ale

$$f(-1) = f(1 \cdot (-1)) = f(1) + f(-1) \Rightarrow f(1) = 0$$
$$f(1) = f((-1) \cdot (-1)) = 2 \times f(-1) \Rightarrow f(-1) = 0 \ ,$$

V poslední implikaci jsme využili známé vlastnosti reálných čísel, a to že $2 \times x = 0 \Rightarrow x = 0$. To je ale spor s prostotou zobrazení $f$.

**Příklad 3.12.** *Najděte všechny endomorfismy pologrupy* $(\mathbb{N}, +)$.

Napřed si uvědomíme, že pologrupa $(\mathbb{N}, +)$ je generována číslem 1, protože $\forall n \in \mathbb{N}$, $n = n \times 1$. Chceme najít endomorfismus pologrupy, proto zobrazení $f : \mathbb{N} \to \mathbb{N}$ musí splňovat $f(n \times 1) = n \times f(1)$. Zobrazení $f$ je proto jednoznačně určeno hodnotou $f(1) = k$. Pro každé $k \in \mathbb{N}$ je zobrazení $f : \mathbb{N} \to \mathbb{N}$ definované pomocí $f(n) = kn$ endomorfizmem pologrupy $(\mathbb{N}, +)$.

**Příklad 3.13.** *Dokažte, že pokud v pologrupě* $M$ *existuje levý neutrální prvek* $e$ *a ke každému* $x \in M$ *existuje levý inverzní prvek* $x'$ *vzhledem k* $e$*, pak* $M$ *je grupa,* $e$ *je její neutrální prvek a* $x'$ *je inverze k* $x$.

Již víme, že existuje levý neutrální prvek a levá inverze. Stačí dokázat, že tyto prvky mají stejnou vlastnost i při působení zprava.

- $x'$ je pravá inverze k $x$:

  $x * x' = x * (e * x') = x * (x' * x) * x' = (x * x') * (x * x')$. V prvním bodě jsme využili, že $e$ je levý neutrální prvek, ve druhém, že $x'$ je levá inverze k $x$ a v posledním to, že $*$ je asociativní. Dále víme, že $(x * x')$ je prvek z pologrupy, a proto k němu také existuje levý inverzní prvek. Nakonec získáme $(x * x')' * (x * x') = e = e * (x * x') = x * x'$. Proto $x'$ je pravá inverze k $x$.

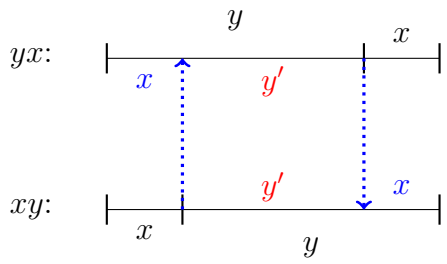
- $e$ je pravý neutrální prvek:

  $x * e = x * (x' * x) = (x * x') * x = e * x = x$, kde v první rovnosti je využito, že $x'$ je levá inverze, ve druhé asociativita $*$ a ve třetí předchozí bod. Proto $e$ je zároveň i pravým neutrálním prvkem.

**Příklad 3.14.** *Nechť* $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{N}_0 \wedge ad - bc = 1 \right\}$. *Dokažte, že pro* $A, B \in M$ *platí* $AB = BA \Rightarrow (\exists C \in M)(\exists k, j \in \mathbb{N}_0)(A = C^j, B = C^k)$.

V rámci monoidu matic je toto náročné ukázat. Využijeme proto izomorfismu ukázaného na přednášce, který říká, že $\mathrm{SL}(2, \mathbb{N}_0) \simeq \mathcal{A}^*$, kde $\mathcal{A}^*$ je monoid konečných slov nad $\{\mathtt{a}, \mathtt{b}\}$. Pak rovnost $AB = BA$ znamená, že existují slova $x, y \in \mathcal{A}^*$ tak, že $xy = yx$. Chceme ukázat, že $x, y$ jsou zřetězením stejného slova $z$. Důkaz provedeme indukcí na délku slova $xy$.

- Pokud $|x| = |y|$, pak z rovnosti $xy = yx$ plyne rovnost jejich prefixů délky $|x| = |y|$, a proto $x = y = x^1$. Rovnost je tedy jistě splněna. V maticích to znamená rovnost matic. Dále tedy můžeme bez újmy na obecnosti uvažovat $|x| < |y|$ (jinak zaměníme $x$ a $y$).
- Pokud $|x| = 0$, tzn. $x$ je prázdné slovo, pak jistě pro jakékoliv $y$ platí $\varepsilon y = y = y\varepsilon$ a $y = y^1$, $x = y^0$. Rovnost je tedy splněna. V maticích by matice $A$ odpovídala jednotkové matici, matice $B$ pak libovolné matici s jednotkovým determinantem.
- Uvažujme $x, y \neq \varepsilon$, $|x| < |y|$. Pak získáme $y = xy' = y'x$ (viz obr. 3), kde $|y'| < |y|$, a proto můžeme využít indukční předpoklad. Existuje tedy $z \in \mathcal{A}^*$ a $i, j \in \mathbb{N}_0$ tak, že $x = z^j$, $y' = z^i$. Nakonec $y = xy' = z^j z^i = z^{j+i}$.



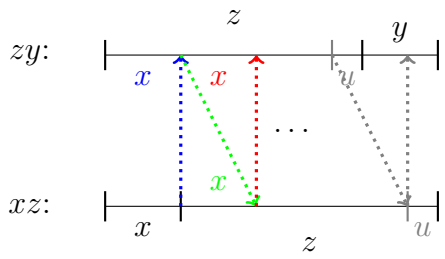

Obrázek 3: $xy = yx$

Poznamenejme, že v důkazu jsme nevyužili faktu, že uvažujeme slova nad dvouprvkovou abecedou. U slov nad víceprvkovou abecedou však nemáme odpovídající tvrzení v maticích.

**Příklad 3.15.** *Nechť* $A$ *je konečná abeceda. Dokažte, že* $(\forall x, y, z \in A^*)$ *splňující* $zx = yz$ *existují* $u, v \in A^*$ *taková, že* $x = uv, y = vu$ *a* $z = u(vu)^j$ *pro nějaké* $j \in \mathbb{N}_0$.

Nutně platí $|x| = |y|$. Dále z rovnosti $xz = zy$ vyplývá, že $zy$ má $x$ jako prefix (viz obrázek 4). Tuto úvahu lze provádět opakovaně. Najdeme tedy $n \in \mathbb{N}$ tak, že $(n-1)|x| < |z| \leq n|x|$. Pak na začátku $z$ najdeme $n-1$ faktorů $x$ a zbytek $u$. Obdobným postupem získáme, že na konci $z$ je $(n-1)$ faktorů $y$ a zbytek tvoří nějaký faktor $v$. Proto $z = x^{n-1}u = vy^{n-1}$, kde $|u| = |v| = |z| - (n-1)|x|$. Dále z rovnosti $xz = zy$ získáme $xz = x^n u = vy^n$, a proto se musí rovnat i jejich prefixy a sufixy. Proto $x = vk$ a $y = ku$ pro nějaké $k \in A^*$. Nakonec si uvědomíme, že v posledním kroku dojde k překryvu $x$ a $y$ tak, že $xv = uy$, proto $v = u$.

Celkem tedy získáme $x = uk$, $y = ku$ a $z = x^{n-1}u = (uk)^{n-1}u = u(ku)^{n-1}$.




Obrázek 4: $xz = zy$

# 4 Grupy

**Příklad 4.1.** *Klasifikujte grupy o 1, 2, 3 a 4 prvcích až na izomorfismy.*

Využijeme poznatky z příkladu 3.7.

1. Máme jedinou možnou grupu, a to triviální $\{e\}$.

2. Máme dva různé prvky $\{a, e\}$. Jestliže $e$ označuje neutrální prvek, musí platit $ae = ea = a$, $ee = e$ a k $a$ musí existovat inverze, tou může být jen $a$. Tato grupa je tedy určena jednoznačně a je vždy izomorfní se $\mathbb{Z}_2$.

3. Máme 3 různé prvky $\{a, b, e\}$. Jestliže $e$ označuje neutrální prvek v grupě, binární operace v tříprvkové grupě má následující tabulku.

| $\circ$ | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | | |
| b | b | | |

   Protože v grupě platí krácení, Cayleyova tabulka je latinský čtverec, lze ji doplnit jediným způsobem, a to takto:

| $\circ$ | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | **b** | e |
| b | b | e | **a** |

4. Již víme, že $e$ je neutrální prvek. Daná Cayleyova tabulka tedy jistě splňuje:

| $\circ$ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | | | |
| b | b | | | |
| c | c | | | |

   Dále musíme doplnit zbývající čtverec. Projdeme-li si všechny možnosti tak, aby byla zachována vlastnost latinského čtverce i existence oboustranné inverze (viz příklad 3.7), získáme následující čtyři tabulky. Doplňujeme vždy nejdříve neutrální prvek $e$ symetricky kolem diagonály. Umístíme-li ho jako výsledek $ac = e$ nebo $ab = e$, tabulku už jednoznačně doplníme (tabulky v prvním sloupci). Umístíme-li neutrální prvek jako výsledek $a^2 = e$, zůstanou ještě dvě možnosti, jak doplnit latinský čtverec (tabulky ve druhém sloupci).

| ∘ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | b | c | **e** |
| b | b | c | **e** | a |
| c | c | **e** | a | b |

$\simeq \mathbb{Z}_4$, kde
$e \leftrightarrow 0$,
$a \leftrightarrow 1$,
$b \leftrightarrow 2$,
$c \leftrightarrow 3$

| ∘ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | **e** | c | b |
| b | b | c | **e** | a |
| c | c | b | a | **e** |

$= \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_4$, kde
$e \leftrightarrow (0,0)$,
$a \leftrightarrow (1,0)$,
$b \leftrightarrow (0,1)$,
$c \leftrightarrow (1,1)$

| ∘ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | c | **e** | b |
| b | b | **e** | c | a |
| c | c | b | a | **e** |

$\simeq \mathbb{Z}_4$, kde
$e \leftrightarrow 0$,
$a \leftrightarrow 1$,
$c \leftrightarrow 2$,
$b \leftrightarrow 3$

| ∘ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | **e** | c | b |
| b | b | c | a | **e** |
| c | c | b | **e** | a |

$\simeq \mathbb{Z}_4$, kde
$e \leftrightarrow 0$,
$b \leftrightarrow 1$,
$a \leftrightarrow 2$,
$c \leftrightarrow 3$

**Příklad 4.2.** *Doplňte Cayleyovu tabulku grupy s prvky a, b, c, d, e:*

| ∘ | e | a | b | c | d |
|---|---|---|---|---|---|
| e | e | | | | |
| a | | b | | | e |
| b | | c | d | e | |
| c | | d | | a | b |
| d | | | | | |

Napřed si uvědomíme, že jediným neutrálním prvek v tabulce může být $e$, protože ostatní sloupce nesplňují předpoklady řečené v příkladu 3.7. Můžeme tedy rovnou doplnit první sloupec a řádek. Dalším krokem je doplnit $e$ do tabulky tak, aby byly splněny předpoklady pro existenci inverzního prvku opět z příkladu 3.7. Nakonec doplníme tabulku na latinský čtverec. Lze také využít asociativity:

- $b \cdot d = b \cdot (c \cdot a) = (b \cdot c) \cdot a = e \cdot a = a.$
- $d \cdot b = d \cdot (a \cdot a) = (d \cdot a) \cdot a = e \cdot a = a.$
- $d \cdot c = d \cdot (b \cdot a) = (d \cdot b) \cdot a = a \cdot a = b.$
- $d \cdot d = d \cdot (c \cdot a) = (d \cdot c) \cdot a = b \cdot a = c.$
- $a \cdot b = a \cdot (d \cdot c) = (a \cdot d) \cdot c = e \cdot c = c.$
- $a \cdot c = a \cdot (b \cdot a) = (a \cdot b) \cdot a = c \cdot a = d.$

| ∘ | e | a | b | c | d |
|---|---|---|---|---|---|
| e | e | a | b | c | d |
| a | a | b | c | d | e |
| b | b | c | d | e | a |
| c | c | d | e | a | b |
| d | d | e | a | b | c |

**Příklad 4.3.** *Označme v monoidu $M$ množinu invertibilních prvků jako $M^\times$. Dokažte, že $M^\times$ je grupa. Popište $M^\times$ pro $M = (\mathbb{Z}_n, \cdot \bmod n, 1)$.*

- Jistě $M^\times \neq \emptyset$, protože $e$ jako neutrální prvek v $M$ je invertibilní $e \cdot e = e \Rightarrow e \in M^\times$.

- Nechť $a \in M^\times$. Pak $a$ je invertibilní a víme, že platí $(a^{-1})^{-1} = a \Rightarrow a^{-1} \in M^\times$.
- Nakonec $a, b \in M^\times$. Pak z invertibility $a, b$ a pravidla pro inverzi součinu získáme $(ab)^{-1} = b^{-1}a^{-1}$, proto i $ab \in M^\times$.

$M^\times$ je tedy grupa.

Je-li $M = \{\mathbb{Z}_n, \cdot \bmod n, 1\}$, pak z Bezoutovy rovnosti získáme, že invertovatelné jsou právě ty prvky, které jsou nesoudělné s $n$. Prvky soudělné s $n$ jistě invertibilní nejsou, protože po vynásobení jakýmkoliv celým číslem bude výsledek vždy dělitelný $1 \neq \text{nsd}(k, n) < n$. Naopak pro $k \in \mathbb{Z}_n$ nesoudělné s $n$ existuje $x, y \in \mathbb{Z}$ tak, že $kx + ny = \text{nsd}(k, n) = 1$, a proto $k \cdot x \equiv 1 \mod n$. Navíc $x$ lze volit tak, aby bylo ze $\mathbb{Z}_n$ (jinak k $x$ přičteme celočíselný násobek $n$, což výslednou kongruenci nezmění).

Proto $M^X = \{k \in \mathbb{Z}_n \mid k \neq 0 \wedge k \perp n\}$.

**Příklad 4.4.** *Najděte všechny podgrupy grupy $\mathbb{Z}_{18}$.*

Využijeme tvrzení, že všechny podgrupy cyklické grupy jsou rovněž cyklické. Lagrangeova věta říká, že pokud je $H$ podgrupa grupy $G$, pak $|H|$ dělí $|G|$. Protože $|\mathbb{Z}_{18}| = 18$, dostaneme 6 různých řádů podgrup, $|H| \in \{1, 2, 3, 6, 9, 18\}$.

- $\{0\}$, $\mathbb{Z}_{18}$ jsou triviální podgrupy.
- $\{0, 9\} = \langle 9 \rangle$ je grupa izomorfní s $\mathbb{Z}_2$.
- $\{0, 6, 12\} = \langle 6 \rangle = \langle 12 \rangle$ je podgrupa izomorfní s $\mathbb{Z}_3$.
- $\{0, 3, 6, 9, 12, 15\} = \langle 3 \rangle = \langle 15 \rangle$ je podgrupa izomorfní s $\mathbb{Z}_6$.
- $\{0, 2, 4, 6, 8, 10, 12, 14, 16\} = \langle 2 \rangle = \langle 4 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 14 \rangle = \langle 16 \rangle$ je podgrupa izomorfní s $\mathbb{Z}_9$.

**Příklad 4.5.** *V grupě $(\mathbb{Z}_n, +\bmod n)$ popište podgrupu generovanou dvěma prvky, tj. $\langle a, b \rangle_{\mathbb{Z}_n}$ pro $a, b \in \mathbb{Z}_n$.*

$$\langle a, b \rangle_{\mathbb{Z}_n} = \{(k \cdot a + \ell \cdot b) \mod n \mid k, \ell \in \mathbb{Z}\} = \langle g \rangle \text{ pro } g = \text{nsd}(a, b)$$

Stačí si totiž uvědomit, že $(\exists k, \ell \in \mathbb{Z})(ka + \ell b = c) \Leftrightarrow \text{nsd}(a, b)$ dělí $c$. Proto $c = m \cdot g$ pro nějaké $m \in \mathbb{Z}$ a $c \in \langle g \rangle$.

**Příklad 4.6.** *Pro grupu $(G, \circ)$ definujeme $(G^{op}, \bullet)$ tak, že $G = G^{op}$ a $\forall x, y \in G$ je $x \bullet y = y \circ x$. Najděte izomorfismus $G$ a $G^{op}$.*

Hledáme izomorfismus $f : G \to G^{op}$. Zobrazení $f$ tedy musí splňovat $(\forall x, y \in G)(f(x \circ y) = f(y) \circ f(x))$.

Položíme-li $f(x) := x^{-1}$, pak můžeme vidět, že splňuje všechny požadavky kladené na izomorfismus. Prosté i surjektivní jistě je, ke každému prvku existuje právě jedna inverze. Navíc $f(x \circ y) = (x \circ y)^{-1} = y^{-1} \circ x^{-1} = f(x) \bullet f(y)$.

**Příklad 4.7.** *Dokažte, že každá netriviální grupa, která nemá vlastní podgrupy, je cyklická a má prvočíselný řád.*

$G \neq \{e\}$ je netriviální grupa. Vezměme $a \in G, a \neq e$. Pak $\langle a \rangle \neq \{e\}$ je podgrupa $G$. Protože $G$ nemá žádné vlastní podgrupy, $\langle a \rangle = G$ a $G$ je cyklická. $G$ nemůže být nekonečná, protože jinak by $\langle a^2 \rangle$ byla vlastní podgrupa grupy $G = \langle a \rangle$.

Pokud $|a| = G = n \in \mathbb{N}$, pak pro všechna $d \in \mathbb{N}, d \mid n$ platí $\langle a^d \rangle$ je podgrupa $G$. Protože všechny tyto podgrupy musí být nevlastní, tzn. $d \in \{1, n\}$, pak $n$ je prvočíslo.

**Příklad 4.8.** *Dokažte, že grupa, ve které je každý prvek svou inverzí, je abelovská.*

Víme, že $(\forall a \in G)(a^{-1} = a)$. Pak $(\forall a, b \in G)(a \cdot b = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a)$. Proto $G$ je abelovská grupa.

**Příklad 4.9.** *Dokažte, že grupa $G = (\mathbb{Q}, +)$ je generovaná množinou $M := \left\{ \frac{1}{n!} \mid n \in \mathbb{N} \right\}$.*

Jistě $\langle M \rangle_G \subset G$. Stačí tedy ukázat $G \subset \langle M \rangle_G$. Vezměme si $\frac{p}{q} \in \mathbb{Q}$, $p \in \mathbb{Z}, q \in \mathbb{N}$ libovolně. Pak $(q-1)! \cdot p \in \mathbb{Z}$ a $\frac{1}{q!} \in M$, proto $((q-1)! \cdot p) \times \frac{1}{q!} = \frac{p}{q} \in \langle M \rangle_G$ a $G \subset \langle M \rangle_G$.

**Příklad 4.10.** *Dokažte, že grupa $G = (\mathbb{Q}^+, \cdot)$ je generovaná množinou $\mathbb{P}$ všech prvočísel.*

Chceme ukázat, že $\langle \mathbb{P} \rangle = \mathbb{Q}^+$, jistě $\mathbb{P} \subset \mathbb{Q}^+$, proto i $\langle \mathbb{P} \rangle \subset \mathbb{Q}^+$.

- Ukážeme napřed, že $\mathbb{N} \subset \langle \mathbb{P} \rangle$. Využijeme rozkladu přirozených čísel na prvočísla

  $$(\forall n \in \mathbb{N})(\exists p_1, p_2, \ldots, p_N \in \mathbb{N})(\exists e_1, e_2, \ldots, e_N \in \mathbb{N})(n = p_1^{e_1} p_2^{e_2} \ldots p_N^{e_N})$$

  Grupa $\langle \mathbb{P} \rangle$ je uzavřená na násobení, a proto $n \in \langle \mathbb{P} \rangle$.

- Vezmeme $x \in \mathbb{Q}^+$. Pak $x = \frac{a}{b}$ pro nějaké $a, b \in \mathbb{N}$. Z uzavřenosti grupy $\langle \mathbb{P} \rangle$ na inverze získáme $b \in \langle \mathbb{P} \rangle \Rightarrow \frac{1}{b} \in \langle \mathbb{P} \rangle$, a proto i $\frac{a}{b} \in \langle \mathbb{P} \rangle$.

**Příklad 4.11.** *Nechť $G$ a $H$ jsou konečné cyklické grupy nesoudělných řádů. Dokažte, že $G \times H$ je rovněž cyklická.*

Víme, že $G = \langle a \rangle$, kde $|a| = n \in \mathbb{N}$, $H = \langle b \rangle$, kde $|b| = m \in \mathbb{N}$ a $n \perp m$. Ukážeme, že $|(a, b)| = n \cdot m$, tudíž $G \times H$ bude cyklická generovaná právě tímto prvkem. (Již totiž víme, že $|G \times H| = |G| \cdot |H|$.)

- $(a, b)^k = (a^k, b^k) = (e_g, e_H) \Leftrightarrow n \mid k \wedge m \mid k \Rightarrow |(a, b)| \geq m \cdot n$, kde v poslední implikaci využíváme nesoudělnosti $m$ a $n$.

- $(a, b)^{(m \cdot n)} = ((a^n)^m, (b^m)^n) = (e_G^m, e_H^n) = (e_G, e_H) \Rightarrow |(a, b)| \leq m \cdot n$

Proto $|(a, b)| = m \cdot n = |G \times H|$ a zároveň $\langle (a, b) \rangle$ je jistě podgrupou $G \times H$, proto $\langle (a, b) \rangle = G \times H$.

**Příklad 4.12.** *Nechť prvky $a$, $b$ mají v grupě $G$ řády $|a|$, $|b|$ tak, že $|a| \perp |b|$. Dokažte, že $\langle a \rangle_G \cap \langle b \rangle_G = \{e\}$.*

Označme si $H := \langle a \rangle_G \cap \langle b \rangle_G$. Víme, že průnik konečného počtu podgrup grupy $G$ je opět podgrupa grupy $G$. Dále $H$ je podgrupa obou grup $\langle a \rangle_G$ i $\langle b \rangle_G$. S využitím Lagrangeovy věty získáme $|H|$ dělí $|a|$ a zároveň $|H|$ dělí $|b|$. Z nesoudělnosti $|a|$ a $|b|$ získáme $|H| = 1$, a proto $H$ je triviální podgrupa $H = \{e\}$.

**Příklad 4.13.** *V grupě* $\mathrm{GL}(2, \mathbb{R})$ *dokažte, že prvky* $a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *mají konečný řád, ale součin $ab$ má nekonečný řád.*

- Napřed určíme řád $a$:

$$a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$
$$a^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$
$$a^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

  Proto $|a| = 3$

- Dále určíme řád $b$:

$$b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$b^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$b^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$b^4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

  Proto $|b| = 4$

- Nakonec najdeme řád $ab$:

$$ab = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

  Ukážeme, že $(ab)^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$ pro všechna $n \in \mathbb{N}$, použijeme k tomu indukci, pro $n = 1$ to jistě platí, dále

$$(ab)^{n+1} = (ab)^n (ab) = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -n-1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -(n+1) & 1 \end{pmatrix}$$

  Můžeme vidět, že tato matice se nerovná jednotkové matici pro žádné $n \in \mathbb{N}$, proto $|ab| = +\infty$.

**Příklad 4.14.** *Najděte všechny endomorfismy grupy $\mathbb{Z}_n$. V případě $\mathbb{Z}_9$ pro každý endomorfismus $f$ určete podgrupu* $\mathrm{Im} f$ *grupy $\mathbb{Z}_9$.*

Protože grupa $\mathbb{Z}_n$ je cyklická, je každý homomorfizmus na ní definovaný jednoznačně určený obrazem jejího generátoru, tedy např. hodnotou $f(1)$. Nutně pak pro každé $j \in \mathbb{Z}_n$ máme $f(j) =$

$jf(1) \mod n$. Endomorfizmus dostaneme pro libovolně zvolenou hodnotu $f(1) = k \in \mathbb{Z}_n$. Z teorie víme, že pro každý endomorfizmus $f$ je $\mathrm{Im}f$ je podgrupa grupy $\mathbb{Z}_n$.

Pro $n = 9$ podle Lagrangeovy věty zjistíme, že $|\mathrm{Im}f| \in \{0, 3, 9\}$. Kromě nevlastních podgrup velikost9 1 a 9 může tedy $\mathrm{Im}f$ být pouze tříprvková, a to $\langle 3\rangle = \langle 6\rangle = \{0, 3, 6\}$. Víme, že generátory grupy $\mathbb{Z}_9$ jsou $1, 2, 4, 5, 7, 8$ (všechny prvky $\mathbb{Z}_9$ nesoudělné s 9). Pokud $f : \mathbb{Z}_9 \to \mathbb{Z}_9$ zadáme tak, že $f(1)$ je generátor, pak $f$ je automorfizmus a $\mathrm{Im}f = \mathbb{Z}_9$. Je-li $f(1) \in \{3, 6\}$, pak $\mathrm{Im}f = \{0, 3, 6\}$, což je grupa izomorfní $\mathbb{Z}_3$. Konečně pokud $f(1) = 0$, máme $\mathrm{Im}f = \{0\}$.

**Příklad 4.15.** *Dokažte, že grupa automorfismů grupy $\mathbb{Z}_n$ je izomorfní grupě $(\mathbb{Z}_n^\times, \cdot \bmod n)$.*

V minulém příkladu 4.14 jsme zjistili, že endomorfizmy $f$ grupy $\mathbb{Z}_n$ jsou jednoznačně určeny obrazem $f(1) = k$, přičemž pro $j \in \mathbb{Z}_n$ je $f(j) = kj \mod n$. Zobrazení $f$ bude automorfizmem, pokud $f(1)$ je generátor grupy $\mathbb{Z}_n$. Generátory grupy $\mathbb{Z}_n$ tvoří množinu $\mathbb{Z}_n^\times$ prvků množiny $\mathbb{Z}_n$ invertibilních vzhledem k násobení modulo $n$, tj. nesoudělných s $n$.

Definujme zobrazení $\varphi : \mathrm{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^\times$ předpisem $\varphi(f) = f(1)$. Z toho, co jsme řekli výše, je zřejmé, že $\varphi$ je bijekce. Zbývá ověřit, že $\varphi$ je homomorfizmus. Máme

$$\varphi(f \circ g) = (f \circ g)(1) = f(g(1)) = f(1)g(1) = \varphi(f)\varphi(g).$$

**Příklad 4.16.** *Dokažte, že grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ (sčítání $\bmod n$ po složkách) má 6 automorfismů a $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathrm{S}_3$.*

Prvky $\mathbb{Z}_2 \times \mathbb{Z}_2$ jsou $\{(0,0), (1,0), (0,1), (1,1)\}$. Aby zobrazení $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ byl automorfismus, musí zobrazovat neutrální prvek sám na sebe. Proto vždy $f((0,0)) = (0,0)$.

K určení zobrazení tedy musíme určit obrazy 3 zbývajících prvků $M := \{(1,0), (0,1), (1,1)\}$. Libovolná volba taková, že $f(M) = M$ bude odpovídat automorfizmu, protože $a + a = (0,0)$ pro kterýkoliv prvek $a \in M$ a $a + b = c$, kde $a, b, c \in M, a \neq b \neq c \neq a$. Každý automorfizmus $f$ grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ zúžený na množinu $M$ je tedy permutace množiny M. Je zřejmé, že přiřazení $\varphi(f) = f|_M$ definuje izomorfizmus $\varphi : \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \to \mathrm{S}_3$.

**Příklad 4.17.** *Nechť $G$ je grupa a $a \in G$ je jediný prvek řádu 2. Dokažte, že $\forall x \in G$ platí $ax = xa$.*

Protože $|a| = 2$, $aa = e$ a proto $a^{-1} = a$. Pak pro všechna $x \in G$ položíme $z_x = x^{-1}ax$.

- Jistě $z_x \neq e$, jinak $e = x^{-1}ax \Rightarrow x = ax \Rightarrow a = e$ spor.
- $z_x^2 = x^{-1}axx^{-1}ax = x^{-1}aeax = x^{-1}ex = e$. Proto $|z_x| = 2$.

Pak ale $z_x = a$ pro všechna $x \in G$ a platí $x^{-1}ax = a \Rightarrow ax = xa$ pro všechna $x \in G$.

**Příklad 4.18.** *Dokažte, že tzv. centrum grupy $G$, tedy $Z_G = \{z \in G \mid \forall x \in G : xz = zx\}$ je podgrupa grupy $G$.*

Abychom ukázali, že to je podgrupa, ukážeme $e \in Z_G$, dále uzavřenost na operaci a nakonec uzavřenost na inverze.

- $\forall x \in G$ platí $xe = x = ex$, proto $e \in Z_G$.
- $\forall a, b \in Z_G$ a $\forall x \in G$ platí $(ab)x = a(bx) = (bx)a = (xb)a = x(ba) = x(ab)$, kde v první a předposlední rovnosti jsme využili asociativity a v dalších to, že $bx, x, b \in G$ a $a, b \in Z_G$. Proto $ab \in Z_G$.
- $\forall a \in Z_G$ a $\forall x \in G$ platí $a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1}$, kde v prostřední nerovnosti jsme využili $x^{-1} \in G$. Proto $a^{-1} \in Z_G$.

# 5 Grupy - normální podgrupy, kongruence, okruhy

**Příklad 5.1.** *Dokažte, že zobrazení $\psi : SL(n,\mathbb{C}) \to SL(n,\mathbb{C}) : \psi(M) = (M^{-1})^T$ je automorfismus, přičemž je vnitřní pro $n = 2$ a vnější pro $n \geq 3$.*

- $\psi$ je dobře definováno a opravdu zobrazuje zpět do $SL(n,\mathbb{C})$, protože $\det(M^{-1})^T = \det(M^{-1}) = (\det(M))^{-1} = 1$.
- $\psi(AB) = ((AB)^{-1})^T = (B^{-1}A^{-1})^T = (A^{-1})^T(B^{-1})^T = \psi(A)\psi(B)$. Je to tedy homomorfismus.
- Zobrazení $\psi$ je bijekce, protože má oboustrannou inverzi. Tou je zobrazení $\psi^{-1}$ definované $\psi^{-1}(A) := (A^T)^{-1}$. Ověříme, že $\psi^{-1}$ je levá inverze:

  $$\psi^{-1}\psi(A) = \psi^{-1}((A^{-1})^T) = (((A^{-1})^T)^T)^{-1} = (A^{-1})^{-1} = A$$

  a také pravá inverze:

  $$(\psi \circ \psi^{-1})(A) = \psi((A^T)-1) = (((A^T)^{-1})^{-1})^T = (A^T)^T = A.$$

- Pro $n = 2$ je to vnitřní automorfismus, tj.

  $$(\exists B \in SL(2,\mathbb{C}))(\forall A \in SL(2,\mathbb{C}))((A^{-1})^T = BAB^{-1}).$$

  Položme $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, pak $B^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ a platí

  $$BAB^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix} = \begin{pmatrix} a_{2,2} & -a_{2,1} \\ -a_{1,2} & a_{1,1} \end{pmatrix}^T$$

  Protože $\det A = 1$, pak je vzniklá matice opravdu inverzní k $A^T$.
- Pro $n \geq 3$ to již vnitřní automorfismus není. Pokud by byl, musela by se zachovávat například stopa matice (protože podobné matice mají stejnou stopu). Uvažujeme-li ale matici, která je diagonální a na úhlopříčce má na $n-1$ pozicích $\frac{1}{2}$ a na poslední pozici je $2^{n-1}$, pak $Tr(A) = (n-1)\cdot\frac{1}{2} + 2^{n-1}$ a $Tr((A^{-1})^T) = (n-1)\cdot 2 + \frac{1}{2^{n-1}}$. Tato dvě čísla se však mohou rovnat pouze pro $n \leq 2$.

**Příklad 5.2.** *Dokažte, že centrum grupy $G$ je normální podgrupa a platí $G/Z(G) \simeq Inn(G)$.*

V příkladu 4.18 jsme již dokázali, že centrum $Z(G)$ grupy $G$je podgrupa grupy $G$. Nyní stačí ukázat, že je normální. Ukážeme, že $Z(G)$ je uzavřeno vůči všem vnitřním automorfismům grupy $G$. Nechť $a \in G$, $h \in Z(G)$, pak $aha^{-1} = haa^{-1} = h \in Z(G)$, kde v první rovnosti jsme použili to, že $h$ komutuje se všemi prvky z $G$.

Vezměme zobrazení $\alpha : G \to Aut(G) : a \mapsto \alpha_a$, kde $\alpha_a(x) = axa^{-1}$. Na přednášce bylo ukázáno, že toto zobrazení je homeomorfismus. Dále Im$\alpha$ je rovno $Inn(G)$, tedy množině všech vnitřních automorfismů grupy $G$. Nakonec Ker$\alpha = \{a \in G \mid \alpha_a = Id\} = \{a \in G \mid (\forall x \in G)(axa^{-1} = x)\} = \{a \in G \mid (\forall x \in G)(ax = xa)\} = Z(G)$. Můžeme proto využít 1. větu o izomorfismu a získáme $G/Z(G) \simeq Inn(G)$.

**Příklad 5.3.** *Nechť $G$ je grupa s podgrupou $H$ indexu 2 (tzn. $|G/H| = 2$). Dokažte, že $H \triangleleft G$.*

Protože index $H$ je 2, máme právě 2 množiny ekvivalence, a to $H$ a $G \setminus H$.

- Je-li $a \in H$, pak jistě $aH = H = Ha$.
- Je-li naopak $a \in G \setminus H$, pak pro všechna $h \in H$ platí $ah \in G \setminus H$, $ha \in G \setminus H$ (vyplývá to z toho, že třídy ekvivalence jsou disjunktní). Proto $aH \subset G \setminus H, Ha \subset G \setminus H$.

Nakonec si uvědomíme, že $G = H \dot\cup (G \setminus H)$ je disjunktní rozklad, a proto $\forall a \in G$ platí $aH = Ha$, a $H$ je proto normální podgrupa $G$.

**Příklad 5.4.** *Určete*

$$|(\mathbb{Z}_6 \times \mathbb{Z}_8)/(\langle 3\rangle_{\mathbb{Z}_6} \times \langle 2\rangle_{\mathbb{Z}_8})|.$$

Využijeme Lagrangeovu větu, tzn.

$$|(\mathbb{Z}_6 \times \mathbb{Z}_8)/(\langle 3\rangle_{\mathbb{Z}_6} \times \langle 2\rangle_{\mathbb{Z}_8})| = \frac{|\mathbb{Z}_6 \times \mathbb{Z}_8|}{|\langle 3\rangle_{\mathbb{Z}_6} \times \langle 2\rangle_{\mathbb{Z}_8}|}$$

Dále víme, že $|\langle 3\rangle_{\mathbb{Z}_6}| = |\{0, 3\}| = 2$, $|\langle 2\rangle_{\mathbb{Z}_8}| = |\{0, 2, 4, 6\}| = 4$. Proto

$$|(\mathbb{Z}_6 \times \mathbb{Z}_8)/(\langle 3\rangle_{\mathbb{Z}_6} \times \langle 2\rangle_{\mathbb{Z}_8})| = \frac{6 \cdot 8}{2 \cdot 4} = 6.$$

**Příklad 5.5.** *Určete*

$$|(\mathbb{Z}_{15} \times \mathbb{Z}_{24})/\langle (5, 4)\rangle_{\mathbb{Z}_{15}\times\mathbb{Z}_{24}}|.$$

Opět využijeme Lagrangeovu větu, tzn.

$$|(\mathbb{Z}_{15} \times \mathbb{Z}_{24})/\langle (5, 4)\rangle_{\mathbb{Z}_{15}\times\mathbb{Z}_{24}}| = \frac{|\mathbb{Z}_{15} \times \mathbb{Z}_{24}|}{|\langle (5, 4)\rangle_{\mathbb{Z}_{15}\times\mathbb{Z}_{24}}|}$$

Nalezneme řád prvku $(5, 4)$: $\langle (5, 4)\rangle_{\mathbb{Z}_{15}\times\mathbb{Z}_{24}} = \{(5, 4), (10, 8), (0, 12), (5, 16), (10, 20), (0, 0)\}$ a získáme

$$|(\mathbb{Z}_{15} \times \mathbb{Z}_{24})/\langle (5, 4)\rangle_{\mathbb{Z}_{15}\times\mathbb{Z}_{24}}| = \frac{15 \cdot 24}{6} = 60$$

**Příklad 5.6.** *Dokažte, že podgrupa grupy $S_3$ generovaná transpozicí* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *není normální podgrupa.*

K ověření, že podgrupa $H$ není normální, stačí najít jediný prvek $a \in G$ takový, že $aH \neq Ha$. Máme $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$, za prvek $a$ volíme $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Potom

$$aH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} \neq \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} = Ha.$$

**Příklad 5.7.** *Klasifikujte abelovské grupy řádu $p^2$, kde $p$ je prvočíslo.*

Využijeme tvrzení, které klasifikuje koečně generované abelovské grupy. Je zřejmé, že grupa $G$ řádu $p^2$ je torzní. Nutně tedy $G \simeq \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}$ pro prvočísla $p_i$, která dělí řád grupy $G$. V tomto případě je jediné takové prvočíslo $p$. Grupa $G$ může být tedy izomorfní buď grupě $\mathbb{Z}_{p^2}$ nebo grupě $\mathbb{Z}_p \times \mathbb{Z}_p$.

**Příklad 5.8.** *Uvažujte akci grupy $GL(2,\mathbb{R})$ na $\mathbb{R}^2$ násobením: $A \cdot \vec{x} = A\vec{x}$. Najděte orbitu a stabilizátor vektoru $\vec{x} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.*

Vezměme $A \in GL(2,\mathbb{R})$. Pak $A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,1} \\ a_{2,1} \end{pmatrix}$.

- **Stabilizátor** $\vec{x}$ je matice $A \in GL(2,\mathbb{R})$ taková, že $A\vec{x} = \vec{x}$. Proto $a_{1,1} = 1$, $a_{2,1} = 0$ a také $a_{2,2} \neq 0$ aby matice byla regulární. Celkem $G_{\vec{x}} = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathbb{R}, b \in \mathbb{R} \setminus \{0\} \right\}$
- **Orbita** $\vec{x}$ je množina $\{A\vec{x} \mid A \in GL(2,\mathbb{R})\}$. Aby $A \in GL(2,\mathbb{R})$, musí platit $0 \neq \det A = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$. Na členy $a_{1,1}, a_{2,1}$ máme tedy podmínku, že se nemohou oba zároveň rovnat 0. Jinak pro všechny ostatní kombinace vždy najdeme $a_{2,2}, a_{1,2}$ tak, aby determinant byl nenulový. Z toho vyvodíme, že pro $\vec{x} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ je orbita $O_{\vec{x}} = \mathbb{R}^2 \setminus \{\vec{0}\}$.

**Příklad 5.9.** *Určete orbity prvků při akci grupy $S_3$ na sobě konjugací: $g \cdot x := gxg^{-1}$.*

$S_3$ je konečná grupa, můžeme proto použít větu dokázanou na přednášce: $|O_x| = \frac{|S_3|}{|G_x|}$, kde $G_x$ je stabilizátor prvku $x$. Dále víme, že $|S_3| = 6$.

- $x = Id$: Pak $G_{Id} = S_3$, protože $\forall g \in S_3$ platí $g \circ Id \circ g^{-1} = g \circ g^{-1} = Id$. Proto $|O_{Id}| = 1$ a orbita obsahuje pouze jediný prvek a tím je $Id$.
- Sudé permutace (bez identity): Tyto permutace odpovídají cyklickým záměnám, je to množina $M = \{(3,1,2), (2,3,1)\}$. Také platí $(3,1,2)^{-1} = (2,3,1)$. Proto $\{Id, (3,1,2), (2,3,1)\} \subset G_x$ pro $x \in M$, a orbita prvku má tedy nejvýše 2 prvky. Tyto dva prvky nalezneme.

  Víme, že liché permutace jsou inverzní samy k sobě a jednoduše ověříme, že $(2,1,3) \circ (3,1,2) \circ (2,1,3) = (2,1,3) \circ (3,2,1) = (2,3,1)$. Proto $O_{(3,1,2)} = \{(3,1,2), (2,3,1)\} = O_{(3,1,2)}$. (Poslední rovnost vyplývá z toho, že pokud $y \in O_x$, pak jistě $O_y \subset O_x$ a dále $y = g \cdot x \Rightarrow x = g^{-1} \cdot y$, proto $x \in O_y$ a nakonec $O_x \subset O_y$.

- Liché permutace: Jsou inverzní samy k sobě, proto $|G_x| \geq 2$ a $O_x \leq 3$. Najdeme tedy 3 prvky v orbitě. Vezměme prvek $(2,1,3)$. Pak $(3,1,2) \circ (2,1,3) \circ (2,3,1) = (3,1,2) \circ (3,2,1) = (1,3,2)$ a $(2,3,1) \circ (2,1,3) \circ (3,1,2) = (2,3,1) \circ (1,3,2) = (3,2,1)$. Proto $O_{(2,1,3)} = \{(2,1,3),(1,3,2),(3,2,1)\} = O_{(1,3,2)} = O_{(3,2,1)}$.

**Příklad 5.10.** *Nechť $F$ je grupa všech funkcí $[0,1] \to \mathbb{R}$ s operací sčítání $(f+g)(x) := f(x) + g(x)$. Označme $N = \{f \in F | f(\frac{1}{4}) = 0\}$. Dokažte, že $N \triangleleft F$ a platí $F/N \simeq \mathbb{R}$.*

Protože $F$ je abelovská grupa, stačí ukázat, že $N$ je podgrupa. $N$ je neprázdná, protože obsahuje nulovou funkci. Pro $f, g \in N$ je

$$(f-g)(\tfrac{1}{4}) = f(\tfrac{1}{4}) - g(\tfrac{1}{4}) = 0,$$

a tedy $f - g \in N$. $N$ je tedy podgrupa grupy $F$.

Definujme zobrazení $\varphi : F \to \mathbb{R}$ předpisem $\varphi(f) = f(\frac{1}{4})$. $\varphi$ je homomorfizmus, protože pro $f, g \in F$ platí

$$\varphi(f+g) = (f+g)(\tfrac{1}{4}) = f(\tfrac{1}{4}) + g(\tfrac{1}{4}) = \varphi(f) + \varphi(g).$$

Zřejmě $\mathrm{Ker}\varphi = N$ a $\mathrm{Im}\varphi = \mathbb{R}$. Podle 1. věty o izomorfizmu platí $F/N \simeq \mathbb{R}$.

# 6 Okruhy, tělesa

**Příklad 6.1.** *Najděte všechny podokruhy okruhu $\mathbb{Z}_4 \times \mathbb{Z}_4$.*

- $(1,1)$ musí ležet v každém podokruhu, proto $\{(0,0),(1,1),(2,2),(3,3)\}$ je nejmenší možný podokruh (prvookruh).
- $\{(0,0),(1,1),(2,2),(3,3)\} \cup \{(0,2),(1,3),(2,0),(3,1)\}$ je podokruh.
- Pokud bychom přidali prvek $(0,1)$, resp. $(0,3)$, pak přičítáním prvku $(1,1)$ dokážeme získat každý prvek $\mathbb{Z}_4 \times \mathbb{Z}_4$. Obdobně pro prvky $(1,0),(3,0)$. Např. $(k,l) = k \times (1,1) + (l - k \bmod 4) \times (0,1)$. Toto jsou tedy všechny podokruhy.

**Příklad 6.2.** *Najděte všechny podokruhy tělesa $\mathbb{Q}$.*

Uvažujme podokruh $S$ tělesa $\mathbb{Q}$. Pak jistě $0, 1 \in S$. Z uzavřenosti na sčítání a odčítání vyplývá, že jistě $\mathbb{Z} \subset S$, kde $\mathbb{Z}$ je již okruh, a proto $\mathbb{Z}$ je nejmenší takový podokruh.

Dále pokud $\frac{m}{n} \in S$, kde $n \in \mathbb{Z}$, $m \in \mathbb{N}$ nesoudělné (jinak můžeme zkrátit), pak z Bézoutova lemmatu získáme, že $\exists x, y \in \mathbb{Z}$ tak, že $mx + ny = 1$, a proto $x \cdot \frac{m}{n} + y \cdot \frac{n}{n} = \frac{1}{n}$. Z toho získáme, že $\frac{m}{n} \in S \Rightarrow \frac{1}{n} \in S$.

Z uzavřenosti na sčítání a odčítání dále získáme $\frac{k}{n} \in S$ pro všechny $k \in \mathbb{Z}$.

Dosud jsme nevyužili uzavřenosti na násobení. Definujme množinu $A := \left\{p \in \mathbb{P} \mid \exists n \in \mathbb{N}, p \mid n \text{ a } \frac{1}{n} \in S\right\}$ kde $\mathbb{P}$ je množina všech prvočísel. Pak z uzavřenosti $S$ na násobení plyne

$$S = \left\{ \frac{k}{p_1 p_2 \dots p_r} \mid k \in \mathbb{Z}, r \in \mathbb{N}_0, (\forall i \in \hat{r})(p_i \in A) \right\}.$$

Pomocí množiny $A$ můžeme definovat podokruhy $\mathbb{Q}$. Pokud $A = \emptyset$, pak $S_A = \mathbb{Z}$, pokud například $A = P \setminus \{2\}$, pak $S_A$ je podokruh všech racionálních čísel s lichým jmenovatelem.

**Příklad 6.3.** *Nechť $T$ je těleso. Které prvky jsou invertibilní v $T[x]$, v $T[[x]]$, v $T[x,y]$?*

Prvek 0 jistě inverzi nemá v žádném z okruhů, nebudeme ji proto dále uvažovat.

- $T[x]$: Z definice $f \in T[x]$ má inverzi právě tehdy, když existuje $g \in T[x]$ tak, že $fg = 1$. Víme ale, že $deg(fg) = deg(f) + deg(g)$ a $deg(1) = 0$. Proto $deg(f) = 0 = deg(g)$. Jediné prvky, které mohou mít inverzi, jsou tedy $f = cx^0$, kde $c \in T \setminus \{0\}$. Tyto prvky opravdu inverzi mají, stačí za $g$ volit $g = c^{-1}x^0$, kde $c^{-1}$ je inverze v tělese.
- $T[x]]$ : Zde již nemůžeme použít argument se stupněm polynomu. Ukážeme si, že nyní existuje inverze ke každému prvku, pro který je nenulový konstantní člen, tzn. $f_0 \neq 0$. Vezměme $f \in T[[x]]$, $f = \sum_{k=0}^{+\infty} f_k x^k$ a předpokládejme, že $f_0 \neq 0$. Nalezneme $g = \sum_{k=0}^{+\infty} g_k x^k \in T[[x]]$ tak, že $f \cdot g = 1$.

$f \cdot g = \sum_{n=0}^{+\infty} h_n x^n$, kde $h_n = \sum_{k=0}^{n} f_k g_{n-k}$. Získáme tak soustavu rovnic, kterou dokážeme vyřešit.

$$1 = h_0 = f_0 g_0 \Rightarrow g_0 = f_0^{-1}$$
$$0 = h_n = f_0 g_n + \sum_{k=1}^{n} f_k g_{n-k} \Rightarrow g_n = -f_0^{-1} \sum_{k=1}^{n} f_k g_{n-k}$$

Kde $f_0^{-1}$ je inverze v tělese a další členy $g_n$ se počítají rekurentně ze znalosti členů do $n-1$.

**Příklad 6.4.** *Rozhodněte, pro která $m, n \in \mathbb{N}$ existuje okruhový homomorfismus mezi $\mathbb{Z}_m$ a $\mathbb{Z}_n$.*

Nechť existuje okruhový homomorfismus $f : \mathbb{Z}_m \to \mathbb{Z}_n$. Pak jistě $f(1) = 1$ a $f(0) = 0$. Dále $f(k) = f(k \times 1) = k \times f(1)$. Vezměme si $k, l \in \mathbb{Z}_m$ tak, aby $k + l = m$. Pak musí platit

$$0 = f(0) = f(l + k) = f(k) + f(l) = k \times f(1) + l \times f(1) = k +_{\mod n} l = m \mod n.$$

- Pokud $m < n$, pak $m = m \mod n$, a proto $f(k + l) \neq 0$, což je spor s tím, že $f$ je homomorfismus.
- Pokud $m = n$, pak homomorfismus jistě existuje, stačí vzít $f = Id$.
- Pokud $m > n$. Pak z vlastnosti $0 = m \mod n$ vyplývá $m = dn, d \in \mathbb{N}$. Ukážeme, že pak $f$ dané předpisem $f(k) = k \mod n$ je okruhový homomorfismus.
  - $f(k + l) = k + l \mod n = f(k) + f(l)$ je jistě splněno.
  - $f(1) = 1$ také.
  - Nechť $k, l \in \mathbb{Z}_m$. Pak $k = nx_k + r_k$, $l = nx_l + r_l$, kde $r_k, r_l \in \mathbb{Z}_n$. Pak $f(k \cdot l) = (nx_k + r_k) \cdot (nx_l + r_l) \mod n = r_k r_l + n(nx_k x_l + x_k r_l + x_l r + k) \mod n = r_k r_l = f(k) f(l)$.

  $f$ je tedy okruhový homomorfismus.

Abychom to shrnuli, mezi $\mathbb{Z}_m$ a $\mathbb{Z}_n$ existuje okruhový homomorfismus právě tehdy, když existuje $d \in \mathbb{N}$ tak, že $m = dn$.

**Příklad 6.5.** *Najděte inverzi v okruhu s dělením $\mathbb{H}$ k nenulovému kvaternionu $g = a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$.*

Napřed připomeneme tabulku násobení jednotek v okruhu $\mathbb{H}$.

| $\cdot$ | 1 | $i$ | $j$ | $k$ |
|---|---|---|---|---|
| 1 | 1 | $i$ | $j$ | $k$ |
| $i$ | $i$ | -1 | $k$ | $-j$ |
| $j$ | $j$ | $-k$ | -1 | $i$ |
| $k$ | $k$ | $j$ | $-i$ | -1 |

Inspirujeme se v komplexních číslech a definujeme pro $g \in \mathbb{H}$, $g = a + bi + cj + dk$, kde $a, b, c, d \in \mathbb{R}$, prvek kvaternionově sdružený $\overline{g} := a - bi - cj - dk$. Zkusíme vypočítat

$$\begin{aligned} g\overline{g} &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + bai - b^2i^2 - bcij - bdik + caj - \\ &\quad - bcji - c^2j^2 - cdjk + dak - dbki - dckj - d^2k^2 \\ &= a^2 + (-abi + abi) + (acj - acj) + (-adk + adk) + b^2 - \\ &\quad - (bcij + bcji) - (bdik + bdki) + c^2 - (cdjk + cdkj) + d^2. \end{aligned}$$

Z antisymetrie násobení jednotek získáme, že členy v závorkách se vždy odečtou. Proto $g\overline{g} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$. Nakonec tedy získáme, že $g^{-1} := \frac{\overline{g}}{a^2+b^2+c^2+d^2} \in \mathbb{H}$.

**Příklad 6.6.** *Dokažte, že jediné prvky okruhu kvaternionů, které komutují se všemi kvaterniony, jsou reálná čísla, tj.* $\{g \in \mathbb{H} \mid \forall r \in \mathbb{H}, gr = rg\} = \mathbb{R}$.

Nechť $g \in \mathbb{H}, g = a + bi + cj + dk$. Pokud $g$ komutuje se všemi prvky, musí komutovat i s jednotkami $i, j, k$.

- Jednotka $i$: $gi = ai - b - ck + dj = ig = ai - b + ck - dj$, aby se rovnaly, musí $c = 0 = d$.
- Z předchozího bodu uvažujme $g = a + bi$. Pak $gj = aj + bk = jg = aj - bk$, aby se rovnaly, musí $b = 0$. Proto $g = a \in \mathbb{R}$.

Získali jsme $\{g \in \mathbb{H} \mid (\forall r \in \mathbb{H})(gr = rg)\} \subset \mathbb{R}$. Nakonec si uvědomíme, že reálná čísla opravdu komutují se všemi kvaterniony, proto $\{g \in \mathbb{H} \mid \forall r \in \mathbb{H}, gr = rg\} = \mathbb{R}$

**Příklad 6.7.** *Najděte všechny ideály v* $\mathbb{Z} \times \mathbb{Z}$.

Víme, že $\pi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \mapsto a$, resp. $\hat{\pi} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \mapsto b$ jsou homomorfismy okruhů. Obrazy ideálů při homomorfismech $\pi, \hat{\pi}$ v $\mathbb{Z} \times \mathbb{Z}$ musí být ideály v $\mathbb{Z}$ – musí to být tedy ideál v každé složce. Jediné ideály v $\mathbb{Z}$ jsou $n\mathbb{Z}$, $n \in \mathbb{N}_0$. Dále si uvědomíme, že díky definici operací po složkách nemáme žádné další omezení na „provázání“ složek. Proto ideály v $\mathbb{Z} \times \mathbb{Z}$ jsou $k\mathbb{Z} \times l\mathbb{Z}$, kde $k, l \in \mathbb{N}_0$.

**Příklad 6.8.** *Najděte všechny ideály v* $T \times \hat{T}$, *kde* $T, \hat{T}$ *jsou tělesa.*

Víme, že $\pi : T \times \hat{T} \to T : (a, b) \mapsto a$, resp. $\hat{\pi} : T \times \hat{T} \to \hat{T} : (a, b) \mapsto b$ jsou homomorfismy okruhů. Obrazy ideálů při homomorfismech $\pi, \hat{\pi}$ v $T \times \hat{T}$ musí být ideály v $T$, resp. $\hat{T}$ – musí to být tedy ideál v každé složce.

Dále si uvědomíme, že jedinými ideály v tělese jsou $\{0\}$ a $T$. Ideály v $T \times \hat{T}$ jsou tedy $\{0\} \times \{\hat{0}\}$, $\{0\} \times \hat{T}$, $T \times \{\hat{0}\}$, $T \times \hat{T}$. Snadno se ověří, že to jsou opravdu ideály.

**Příklad 6.9.** *Popište faktorokruhy* $\mathbb{Z}[x]/6\mathbb{Z}[x]$ *a* $\mathbb{Z}[x]/(3\mathbb{Z}[x] + x\mathbb{Z}[x])$.

- $\mathbb{Z}[x]/6\mathbb{Z}[x] \simeq \mathbb{Z}_6[x]$: Vezměme zobrazení $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_6[x] : \sum_{k=0}^{n} f_k x^k \mapsto \sum_{k=0}^{n} (f_k \mod 6)x^k$. Toto zobrazení je homomorfismus. Im$\varphi$ je jistě celé $\mathbb{Z}_6[x]$.

$$\begin{aligned}\text{Ker}\varphi &= \{f \in \mathbb{Z}[x] \mid f_k \mod 6 = 0 \text{ pro všechna } k\} \\ &= \{f \in \mathbb{Z}[x] \mid f_k \in 6\mathbb{Z} \text{ pro všechna } k\} = 6\mathbb{Z}[x].\end{aligned}$$

  Využijeme tedy první větu o izomorfismu a získáme $\mathbb{Z}[x]/6\mathbb{Z}[x] \simeq \mathbb{Z}_6[x]$.

- $\mathbb{Z}[x]/(3\mathbb{Z}[x] + x\mathbb{Z}[x]) \simeq \mathbb{Z}_3$: Vezměme zobrazení $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_3 : \sum_{k=0}^{n} f_k x^k \mapsto f_0 \mod 3$. Toto zobrazení je homomorfismus. Im$\varphi$ je jistě celé $\mathbb{Z}_3$.

$$\begin{aligned}\text{Ker}\varphi &= \{f \in \mathbb{Z}[x] \mid f_0 \mod 3 = 0\} \\ &= \{f \in \mathbb{Z}[x] \mid f_0 \in 3\mathbb{Z}\}.\end{aligned}$$

  Dále si uvědomíme, jak množina $3\mathbb{Z}[x] + x\mathbb{Z}[x]$ vypadá. Jsou to polynomy tvaru $3g + xf$, tzn. $\sum_{k=0}^{n} 3g_k x^k + \sum_{k=0}^{n} f_k x^{k+1} = 3g_0 + \sum_{k=1}^{n} (g_k + f_{k-1})x^k$. Z toho vyplývá $3\mathbb{Z}[x] + x\mathbb{Z}[x] = \{f \in \mathbb{Z}[x] \mid f_0 \in 3\mathbb{Z}\} = \text{Ker}\varphi$.

  Opět můžeme využít první větu o izomorfismu a získáme $\mathbb{Z}[x]/(3\mathbb{Z}[x] + x\mathbb{Z}[x]) \simeq \mathbb{Z}_3$.

**Příklad 6.10.** *Dokažte, že množina $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ je ideál v $\mathbb{Z}[x]$, který není hlavní.*

Napřed si uvědomíme, jak množina $H := 2\mathbb{Z}[x] + x\mathbb{Z}[x]$ vypadá.

$$2\mathbb{Z}[x]+x\mathbb{Z}[x] = \left\{\sum_{k=0}^{n} 2g_k x^k + \sum_{k=0}^{n} f_k x^{k+1} \mid f_k, g_k \in \mathbb{Z}\right\} = \left\{2g_0 + \sum_{k=1}^{n} (2g_k + f_{k-1})x^k \mid f_k, g_k \in \mathbb{Z}\right\}.$$

- $f, g \in H$, pak $f + g = 2(f_0 + g_0) + \sum_{k=1}^{n} (g_k + f_k)x^k \in H$.
- $f \in H$, $g \in \mathbb{Z}[x]$, pak $fg = 2f_0 g_0 + \sum_{k=1}^{n} h_k x^k$, kde $h_k = \sum_{i=0}^{k} f_i g_{k-i}$. Proto i $fg \in H$.

H je proto ideál v $\mathbb{Z}[x]$. Předpokládejme pro spor, že existuje $g \in \mathbb{Z}[x]$ tak, že $2\mathbb{Z}[x] + x\mathbb{Z}[x] = (g) = g\mathbb{Z}[x]$.

- Jistě $2 = 2 \cdot 1x^0 + 0 \in 2\mathbb{Z}[x] + x\mathbb{Z}[x] = g\mathbb{Z}[x]$, musí proto existovat $h \in \mathbb{Z}[x]$ tak, aby $2 = gh$. Protože $\mathbb{Z}$ je obor integrity, platí $\deg(2) = 0 = \deg(g) + \deg(h)$, proto $\deg(g) = 0$ a $g \in \mathbb{Z}$. Dále $g \in 2\mathbb{Z}[x] + x\mathbb{Z}[x]$, proto $g \in \{2, -2\}$.
- Dále $x = 0 + x \cdot 1x^0 \in 2\mathbb{Z}[x] + x\mathbb{Z}[x] = g\mathbb{Z}[x]$, proto existuje $h' \in \mathbb{Z}[x]$ tak, že $gh' = \pm 2h' = x$, což pro žádné $h' \in \mathbb{Z}[x]$ nastat nemůže. Dostali jsme tedy spor a $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ není hlavní ideál.

**Příklad 6.11.** *Dokažte, že pro komutativní okruh $R$ je $(x, y) := xR[x, y] + yR[x, y]$ ideál v $R[x, y]$ a platí $R[x, y]/(x, y) \simeq R$.*

Napřed si uvědomíme, že prvky $(x, y)$ jsou právě ty polynomy, které mají nulový absolutní člen.

$$f \in (x,y) \Leftrightarrow f = \sum_{k,l=0}^{n} f_{k,l} x^k y^l = x \sum_{k,l=0}^{n} f'_{l,k} x^k y^l + y \sum_{k,l=0}^{n} f''_{l,k} x^k y^l \Leftrightarrow f_{0,0} = 0$$

Máme-li dva polynomy s nulovým absolutním členem, bude nulový i absolutní člen jejich součtu. Dále z definice násobení polynomů získáme, že pokud polynom s nulovým absolutním členem vynásobíme libovolným polynomem, i výsledek bude mít nulový absolutní člen. $(x, y)$ je tedy ideál.

Nakonec ukážeme, že $\varphi : R[x, y] \to R : f \mapsto f_{0,0}$ je homomorfismus.

- $\varphi(f + g) = f_{0,0} + g_{0,0} = \varphi(f) + \varphi(g)$,
- $\varphi(1) = 1$,
- $\varphi(f \cdot g) = f_{0,0} g_{0,0} = \varphi(f)\varphi(g)$,
- $f \in \mathrm{Ker}\varphi \Leftrightarrow f_{0,0} = 0 \Leftrightarrow f \in (x, y)$,
- $\mathrm{Im}\varphi = R$, protože pro $u \in R$, $\varphi(u) = u$.

Můžeme tedy využít 1. větu o izomorfismu pro okruhy a získáme $R[x, y]/(x, y) \simeq R$.

**Příklad 6.12.** *Nechť $R$ je komutativní okruh. Dokažte, že $R[x]/(x+1) \simeq R$ a $R[x]/(x-y) \simeq R[x]$.*

Definujeme $\varphi : R[x] \to R : f \mapsto f(-1)$, které je zjevně homomorfizmus. Jeho jádrem je $\mathrm{Ker}\varphi = (x + 1)R[x]$ a obrazem $\mathrm{Im}\varphi R$. Podle 1. věty o izomorfismu pro okruhy získáme $R[x]/(x + 1) \simeq R$.

Definujeme nyní $\psi : R[x, y] \to R : f \mapsto f(x, x)$. Toto zobrazení je opět homomorfizmus. Jeho jádrem je $\mathrm{Ker}\varphi = (x-y)R[x, y]$, tj. množina polynomů, které se anulují při dosazení $x$ za $y$. Obrazem je $\mathrm{Im}\varphi R[x]$. Podle 1. věty o izomorfismu pro okruhy získáme $R[x, y]/(x - y) \simeq R[x]$.

**Příklad 6.13.** *Dokažte, že množina $R = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}, n$ liché $\}$ je s obvyklými operacemi $+$ a $\cdot$ okruh hlavních ideálů. Najděte maximální ideál a faktorizujte podle něj.*

Daná množina je zjevně podokruh okruhu racionálních čísel, protože obsahuje $1 = \frac{1}{1}$, $0 = \frac{0}{1}$, je uzavřená na sčítání, odčítání i násobení. Ukážeme, že ideály v $R$ jsou pouze hlavní. Nulový ideál $I = \{0\} = (0)$ je hlavní. Uvažujme $I \neq \{0\}$. Všechny nenulové prvky v $I$ lze zapsat ve tvaru $\frac{2^j k}{n}$, kde $k, n$ jsou lichá čísla a $j \in \mathbb{N}_0$. Vybereme takový prvek $\frac{2^j k}{n}$, aby $j$ bylo minimální. Dokážeme, že $I = 2^j R = (2^j)$. Vezměme $\frac{r}{s} \in I$. Pak $r = 2^t u$, kde $u \in \mathbb{Z}$ je liché a $t \geq j$. Proto

$$\frac{r}{s} = \frac{2^t u}{s} = 2^j \frac{2^{t-j} u}{s} \in 2^j R.$$

Z výše uvedeného plyne, že všechny ideáy v $R$ jsou tvaru $2^j R = (2^j)$, $j \in \mathbb{N}_0$. Zjevně všechny ideály tvoří řetězec vůči inkluzi

$$(1) = R \supsetneqq (2) \supsetneqq (2^2) \supsetneqq (2^3) \supsetneqq \cdots,$$

a proto (2) je jediný maximální ideál v $R$. Provedeme-li faktorizaci podle ideálu $I = (2)$, vyjde faktorokruh $R/(2) = \{[0], [1]\} \simeq \mathbb{Z}_2$.

**Příklad 6.14.** *Dokažte, že každý konečný nenulový obor integrity je těleso.*

Důkaz provedeme sporem. Nechť $G$ je konečný nenulový obor integrity. Předpokládejme, že existuje $a \in G \setminus \{0\}$ tak, že k němu neexistuje v $G$ inverze, tzn. $(\forall b \in G)(ab \neq 1)$. Pak ale zobrazení $f : G \to G : b \mapsto ab$ není surjektivní. Protože $f$ je zobrazení mezi konečnými prostory o stejném počtu prvků, nemůže být ani prosté. Proto existují prvky $b_1, b_2 \in G, b_1 \neq b_2$ tak, že $f(b_1) = f(b_2)$. Z této rovnosti ale vyplývá $ab_1 = ab_2$, a proto $a(b_1 - b_2) = 0$, což je ale spor s tím, že $G$ je obor integrity.

**Příklad 6.15.** *Dokažte, že* $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{R}[x]/(x^2+x+1) \simeq \mathbb{C}$.

Z teorie víme, že $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{R}(i) = \{a+bi \mid a, b \in \mathbb{R}\}$ a $\mathbb{R}[x]/(x^2+x+1) \simeq \mathbb{R}(\omega) = \{a+b\omega \mid a, b \in \mathbb{R}\}$, kde $i$ je kořen polynomu $x^2+1$ a $\omega = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ je kořen polynomu $x^2+x+1$. Najdeme izomorfizmus $\psi : \mathbb{R}(\omega) \to \mathbb{R}(i)$. Stačí definovat

$$\psi(a) = a \text{ pro } a \in \mathbb{R} \text{ a } \psi(\omega) = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2},$$

pro zbylé hodnoty z $\mathbb{R}(\omega)$ dodefinujeme podle $\psi(a+b\omega) = a + b\psi(\omega)$. Toto zobrazení je bijekce a navíc je to homomorfizmus. Kompatibilita se s čítáním je zřejmá z definice. Kompatibilitu s násobením ověříme. Máme

$$\psi(\omega^2) = \psi(-\omega - 1) = \tfrac{1}{2} - i\tfrac{\sqrt{3}}{2} - 1 = -\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2},$$

ale také

$$(\psi(\omega))^2 = (-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2})^2 = -\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}.$$

Zobrazení $\psi$ je tedy izomorfizmus.

**Příklad 6.16.** *Najděte všechny kořeny polynomu* $x^2 - 1$ *v* $\mathbb{Z}_{15}$.

Máme konečnou množinu $\mathbb{Z}_{15} = \{0, 1, 2, \ldots, 14\}$. Všechny kořeny najdeme prostý dosazením a ověřením, zda $f(a) = a^2 - 1 = 0$. Při výpočtu nám může pomoci, že $k \equiv k - 15 \mod 15$. Tyto kořeny jsou $\{1, 4, 11, 14\}$.

**Příklad 6.17.** *Zjistěte, zda jsou polynomy* $x^2 - 2$, $x^3 + x + 2$ *reducibilní nad tělesy* $\mathbb{Z}_3$, *resp.* $\mathbb{Z}_5$.

- $x^2 - 2$ nad $\mathbb{Z}_3$. Dosazením zjistíme, že nad $\mathbb{Z}_3$ tento polynom nemá žádný kořen. Kdyby byl reducibilní, musel by jít rozložit na dva polynomy prvního stupně, tudíž by musel mít kořen. Tento polynom je proto nad $\mathbb{Z}_3$ ireducibilní.

- $x^2 - 2$ nad $\mathbb{Z}_5$. Provedeme stejnou úvahu jako v předchozím bodě a dosazením zjistíme, že ani nad $\mathbb{Z}_5$ nemá tento polynom kořen. Je ireducibilní.

- $x^3 + x + 2$ Zkusme obecně dosadit prvek $p - 1$. Pak

$$(p-1)^3 + (p-1) + 2 = p^3 - 3p^2 + 3p + p.$$

  Toto se nad $\mathbb{Z}_p$ rovná nule. Proto nad $\mathbb{Z}_3$ má polynom kořen 2 a jde ho rozložit na $(x-2)g$ pro $g \in \mathbb{Z}_3[x]$. Nad $\mathbb{Z}_5$ je kořenem číslo 4 a jde ho rozložit na $(x-4)\tilde{g}$ pro $\tilde{g} \in \mathbb{Z}_5[x]$, kde $\deg g, \deg \tilde{g} \geq 2$. V obou případech je polynom $x^3 + x + 2$ reducibilní.

**Příklad 6.18.** *Nechť $a$ je kořen polynomu $x^3 - 6x^2 + 9x + 3 \in \mathbb{Q}[x]$. V tělese $\mathbb{Q}(a)$ vyjádřete prvky $a^4$, $\frac{1}{a+1}$, $\frac{1}{a^2-6a+8}$ jako racionální lineární kombinace $1, a, a^2$.*

$a$ je kořenem zadaného polynomu, platí tedy $a^3 - 6a^2 + 9a + 3 = 0$.

- Napřed vypočítáme $a^4$ ze znalosti $a^3 = 6a^2 - 9a - 3$.

$$a^4 = aa^3 = a(6a^2 - 9a - 3) = 6a^3 - 9a^2 - 3a = 6(6a^2 - 9a - 3) - 9a^2 - 3a = 27a^2 - 57a - 18$$

- Pro výpočet $\frac{1}{a+1}$ potřebujeme zlomek nějak „chytře“ rozšířit. Využijeme proto dělení se zbytkem, kdy $(a^3 - 6a^2 + 9a + 3) : (a + 1) = a^2 - 7a + 16 - \frac{13}{a+1}$. Proto

$$\frac{1}{a+1} = \frac{a^2 - 7a + 16}{(a+1)(a^2 - 7a + 16)} = \frac{a^2 - 7a + 16}{a^3 - 6a^2 + 9a + 3 + 13} =$$
$$= \frac{a^2 - 7a + 16}{0 + 13} = \frac{1}{13}a^2 - \frac{7}{13}a + \frac{16}{13} \in \mathbb{Q}[x]$$

- Opět využijeme dělení se zbytkem, protože $(a^3 - 6a^2 + 9a + 3) : (a^2 - 6a + 8) = a + \frac{a+3}{a^2-6a+8}$ a $(a^3 - 6a^2 + 9a + 3) : (a + 3) = a^2 - 9a + 36 - \frac{105}{a+3}$, získáme

$$\frac{1}{a^2 - 6a + 8} = \frac{a}{a^3 - 6a^2 + 9a - a + 3 - 3} = \frac{-a}{a+3} = \frac{-a(a^2 - 9a + 36)}{(a^2 - 9a + 36)(a+3)} =$$
$$= \frac{-(6a^2 - 9a - 3) + 9a^2 - 36a}{0 + 105} = \frac{1}{35}a^2 - \frac{9}{35}a + \frac{1}{35} \in \mathbb{Q}[x]$$

**Příklad 6.19.** *Nechť $R, \hat{R}$ jsou okruhy charakteristik $charR = m$, $char\hat{R} = n$. Najděte $char(R \times \hat{R})$.*

Chceme najít nejmenší $k \in \mathbb{N}$ takové, že $k \times (1,1) = (k \times 1_r, k \times 1_{\hat{R}}) = 0$. Z $\mathrm{char}R = m$ a $\mathrm{char}\hat{R} = n$ vyplývá $m \mid k$ a $n \mid k$. Z minimality pak $k = \mathrm{nsn}(m,n)$. Proto $\mathrm{char}(R \times \hat{R}) = \mathrm{nsn}(m,n)$.

**Příklad 6.20.** *Dokažte, že každé podtěleso tělesa, které má $p^n$ prvků, kde $p$ prvočíslo, $n \in \mathbb{N}$, má $p^m$ prvků, kde $m \mid n$.*

Nechť $T$ je podtěleso tělesa $GF(p^n)$. Označme $q = |T|$. Protože $GF(p^n)$ je vektorový prostor nad $T$, musí $q|p^n$. Nutně tedy $q = p^m$ pro nějaké přirozené $m \leq n$. Označme $r$ dimenzi $[GF(p^n) : T]$. To znamená, že $GF(p^n)$ má $q^r$ prvků. Nyní porovnáme $q^r = (p^m)^r = p^{mr} = p^n$, odkud už snadno plyne $m|n$.