- Algebry jsou množiny, na kterých jsou definovány nějaké operace. Tyto operace jsou různých typů:
  - nulární, unární, binární či obecně n-ární
- Příklady typů algeber:
  - $(A, \cdot)$ je algebra typu (2), tj. algebra s binární operací, taková algebra se označuje též grupoid.
  - $(A, \cdot, ^{-1}, 1)$ je algebra typu $(2,1,0)$, kde $\cdot$ je binární operace inverze $^{-1}$ je unární operace a 1 je nulární operace. Taková algebra se označuje grupa.
  - algebra, která je bez typu je samotná množina A, na které není definovaná žádná operace.
- <u>Základní algebry s jednou operací</u>
  - grupoid je algebra A, která je uzavřená na operaci $\cdot$
  - pologrupa je algebra, kde pro operaci $\cdot$ platí asociativní zákon, tj. pro $\forall a_1, a_2, a_3 \in A : (a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$ neboli platí zde libovolné uzávorkování

- monoid je algebra $(A, \cdot, 1)$ typu $(2,0)$, pokud existuje zde neutrální prvek, tj. pro tento prvek $\underline{e}$ platí:

$$\boxed{\forall a \in A: \quad \begin{array}{l} e \cdot a = a \\ a \cdot e = a \end{array}} \quad \begin{array}{l} \text{- levý neutrální prvek} \\ \text{- pravý neutrální prvek} \end{array} \Big\} \Rightarrow \text{neutrální prvek}$$

- grupa je algebra $(A, \circ, ^{-1}, 1)$ typu $(2,1,0)$, pokud každý prvek je <u>invertibilní</u>, tj. ke každému prvku existuje jeden inverzní prvek:

$$\boxed{\forall x \in A, \exists y \in A: \quad \begin{array}{l} x \cdot y = e \\ y \cdot x = e \end{array}} \quad \begin{array}{l} \text{- pravý inverzní prvek} \\ \text{- levý inverzní prvek} \end{array} \Big\} \Rightarrow \text{inverzní prvek}$$

- komutativní (abelovská) grupa je algebra, kde její operace $\circ$ je komutativní, tj.: $\boxed{\forall x, y \in A: \quad x \cdot y = y \cdot x}$

Př 1] Máme algeru $(A, \circ)$, kde $A = \{a, b, c\}$ a operace $\circ$ je definovaná pomocí tzv. Cayleyovy tabulky:

$\circ$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

<u>Úkol</u>: Zjistěte zda je operace $\circ$ komutativní, asociativní a zda zde existuje neutrální prvek.

- komutativita: aby operace $\circ$ byla komutativní, musela by tabulka být souměrná podle diagonály.
  → zde to neplatí
- neutrální prvek: aby zde existoval neutrální prvek, musel by v tabulce být sloupec i řádek obsahující stejné prvky jako v hlavičce tabulky.
  → zde jsou sloupce, které obsahují stejné prvky jako v hlavičce tabulky, tj. právě neutrální prvky tu jsou, ale není zde ani jeden řádek, pro který by to platilo ⇒ neutrální prvek tady neexistuje
- asociativní zákon: musí se vyzkoušet všechny možné kombinace

$(a \circ \_) \circ \_ = a \circ (\_ \circ \_)$
(_ … cokoliv)

$a \circ \_ = a \circ \_$
$a = a$ ✓

$(b \circ \_) \circ \_ = b \circ (\_ \circ \_)$
$b \circ \_ = b \circ \_$
$b = b$ ✓

$(c \circ \_) \circ \_ = c \circ (\_ \circ \_)$
$c \circ \_ = c \circ \_$
$c = c$ ✓

- nezáleží zde na uzávorkování, tedy operace je asociativní
  (jediné na čem záleželo, bylo, který prvek je první)

Př 2 | Stejné zadání jako v Př 1, pouze tabulka se změní:

∘	a	b	c
a	b	a	c
b	a	b	c
c	c	c	c

- komutativita: tabulka je souměrná podle diagonály, tj. operace je komutativní.

- neutrální prvek: 2. sloupec a 2. řádek obsahují stejné prvky jako jsou v hlavičce tabulky, tj. $e = b$

- asociativita:
  - pokud se kdekoliv v posloupnosti $(\_ \circ \_) \circ \_$ či $\_ \circ (\_ \circ \_)$ objeví prvek e pak se tyto výrazy rovnají e.
  - protože prvek b je neutrálním prvkem, nemá vliv na výsledek rovnice.
  - zbývající kombinace prvků je $(a \circ a) \circ a = a \circ (a \circ a)$
    $b \circ a = a \circ b$
    $a = a$ ✓

⇒ asociativita zde platí.

- Mají zde všechny prvky k sobě inverzní prvek?
  - NE, protože $c \circ c = c \neq b$, ale e není neutrální prvek!
  ⇒ nejsou zde invertibilní prvky, tj. tato algebra $(A, \circ)$ není grupa.

Pozn. Operace s dělením je taková operace, kde platí:

$$\text{pro } \forall a,b \in A, \exists x,y \in A: \quad a \circ x = b \quad \text{- levý zákon o dělení}$$
$$y \circ a = b \quad \text{- pravý zákon o dělení}$$

pokud platí pravý a zároveň levý zákon o dělení, je to operace s dělením.

- je operace $\circ$ z příkladu 2 operace s dělením?
  - ↳ všechny sloupce a všechny řádky tabulky by musely obsahovat všechny prvky algebry alespoň jednou.
  - v Př 2 poslední sloupec i poslední řádek neobsahují všechny prvky, tj. není to operace s dělením.

Pozn. Operace s krácením je taková operace, kde platí:

$$\text{pro } \forall a, x_1, x_2, y_1, y_2 \in A: \quad a \circ x_1 = a \circ x_2 \implies x_1 = x_2 \quad \text{- levý zákon o krácení}$$
$$y_1 \circ a = y_2 \circ a \implies y_1 = y_2 \quad \text{- pravý zákon -"-}$$

pokud platí pravý i levý zákon o krácení, je to operace s krácením.

- je operace z Př 2 operace s krácením?
  - ↳ všechny sloupce i řádky tabulky by musely obsahovat každý prvek maximálně jednou.
  - v Př 2 opět poslední sloupec i řádek obsahuje prvek e vícekrát, tj. není to operace s krácením.

Pozn. Pro konečné algebry jsou zákony o dělení ekvivalentní zákonům o krácení.

Př 3. Přirozená čísla s operací násobení, tj. $(\mathbb{N}, \cdot)$ jsou nekonečná algebra, kde platí zákon o krácení, ale neplatí zde zákon o dělení.

Př 4. Máme algebru $(A, \circ)$, kde A je množina uspořádaných dvojic nad celými čísly, tj. $A = \{(x,y) \mid x, y \in \mathbb{Z}\}$, a operace $\circ$ je definována následovně: $(x,y) \circ (s,t) = (x+s, y+t)$

Co to je za algebru?

- grupoid? pro $\forall x,y,s,t \in \mathbb{Z}$ platí $(x,y) \circ (s,t) = (x+s, y+t)$, kde $x+s \in \mathbb{Z}$ a $y+t \in \mathbb{Z}$, tj. tato operace je uzavřená na celé množině A.
  → je to grupoid.

- pologrupa? musí zde platit asociativní zákon:
  - $[(x,y) \circ (s,t)] \circ (u,v) = (x+s, y+t) \circ (u,v) = (x+s+u, y+t+v)$
  - $(x,y) \circ [(s,t) \circ (u,v)] = (x,y) \circ (s+u, t+v) = (x+s+u, y+t+v)$ ✓

  ⇒ je to pologrupa.

- monoid? existuje zde neutrální prvek?

$(x,y)\circ(\underline{0},\underline{0}) = (x,y)$

$(x+\underline{0}, y+\underline{0}) = (x,y) \Rightarrow$ neutrální prvek je $(0,0)$

$(0,0) \in \mathbb{R}\times\mathbb{R}$ ✓

→ je to monoid.

- grupa? jsou zde inverzní prvky?

$(x,y)\circ(u,v) = (0,0)$

$(x+u, y+v) = (0,0) \Rightarrow x+u=0 \quad y+v=0$

$u = -x \in \mathbb{R}$ ✓ $\quad v = -y \in \mathbb{R}$ ✓

- inverzní prvek k (x,y) je $(-x,-y)$

→ je to grupa

- komutativita?

$(x,y)\circ(s,t) = (x+s, y+t) = (s+x, t+y) = (s,t)\circ(x,y)$

sčítání je komutativní

→ je to komutativní (abelovská) grupa

Př 5| a) Máme pozitivní iteraci abecedy Σ^+ s operací konkatenace.

- konkatenace je asociativní: $v,w,x \in \Sigma^+$: $(v\cdot w)\cdot x = v\cdot(w\cdot x)$

⇒ je to pologrupa

b) pokud máme Σ^* s konkatenací, je zde i neutrální prvek prázdné slovo ε, tj. je to monoid.

Př 6] Máme algebru tvořenou množinou matic velikosti 2×2 nad reálnými čísly $\mathbb{R}$. Tvoří tato algebra společně s operací násobení matic grupu?

Pozn. Tyto matice jsou regulární, tj. lze je upravit do schodovitého tvaru a jejich řádky/sloupce jsou lineárně nezávislé.

- grupoid? $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & c \\ d & e \end{pmatrix} = \begin{pmatrix} 0 & ac \\ bd & 0 \end{pmatrix}$ ← je to regulární matice nad $\mathbb{R}$ ✓

- asociativita?

  - $\left[\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}\right] \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} 0 & ac \\ bd & 0 \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} 0 & acf \\ bde & 0 \end{pmatrix}$

  - $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \left[\begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix}\right] = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & cf \\ de & 0 \end{pmatrix} = \begin{pmatrix} 0 & acf \\ bde & 0 \end{pmatrix}$

  ↪ je to asociativní ⇒ je to pologrupa

- neutrální prvek, tj. monoid?

  ↪ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ jednotková matice je regulární maticí nad $\mathbb{R}$. ✓

- grupa? (inverzní prvky)

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\hookrightarrow \left(\begin{array}{cc|cc} a & 0 & 1 & 0 \\ 0 & b & 0 & 1 \end{array}\right) \begin{matrix} :a \\ :b \end{matrix} \sim \left(\begin{array}{cc|cc} 1 & 0 & 1/a & 0 \\ 0 & 1 & 0 & 1/b \end{array}\right), \quad \frac{1}{a}, \frac{1}{b} \in \mathbb{R} \checkmark$$

- inverzní prvek k $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ je prvek $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix}$

→ je to grupa.

Pozn.: Pokud by v zadání bylo, že matice jsou definovány pouze nad celým čísly $\mathbb{Z}$, pak by zde neexistovaly inverzní prvky, protože $\frac{1}{a}, \frac{1}{b} \notin \mathbb{Z}$!

- komutativita?

$$\cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} = \begin{pmatrix} 0 & ac \\ bd & 0 \end{pmatrix} \neq \text{ nerovnají se}$$

$$\cdot \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & cb \\ da & 0 \end{pmatrix}$$

→ není to komutativní grupa.

Základní algebry se 2 operacemi

- algebra $(A, +, \cdot)$ je **okruh** pokud platí:
  1) $(A, +)$ je komutativní grupa
  2) $(A, \cdot)$ je pologrupa
  3) mezi operacemi $+$ a $\cdot$ platí distributivní zákon

tj. pro $\forall a, b, c \in A$ platí: $a \cdot (b+c) = a \cdot b + a \cdot c$ – levý distri. zákon

$(b+c) \cdot a = b \cdot a + c \cdot a$ – pravý — " —

- algebra je **pologokruh**, pokud $(A, +)$ je pouze monoid
- **Komutativní okruh**, pokud $(A, \cdot)$ je komutativní.
- **Komutativní okruh s jednotkou**, pokud $(A, \cdot)$ má neutrální prvek tzv. jedničku okruhu
- **obor integrity** pokud je netriviální, tj: $0 \neq 1$, je to komutativní okruh s jednotkou a nemá dělitele nuly, tj. $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

- Příklad dělitelů nuly:
  - $(\mathbb{Z}_6, +, \cdot)$ jsou dělitelé nuly prvky $[2]_6$ a $[3]_6$
    protože $[2]_6 \cdot [3]_6 = [2 \cdot 3]_6 = [6]_6 = [0]_6$
    a přitom $[2]_6 \neq [0]_6 \wedge [3]_6 \neq [0]_6$
  - algebra je <u>těleso</u> pokud $(A \setminus \{0\}, \cdot)$ tvoří grupu a je netriviální tj. $0 \neq 1$.
  - <u>pole</u> je komutativní těleso.

<u>Př 7</u>| Mějme algebru $(A, \oplus, \odot)$, kde A je množina uspořádaných dvojic (x, y) nad racionálními čísly $\mathbb{Q} \times \mathbb{Q}$.
Operace jsou definovány následovně:

$\oplus$: $(x, y) \oplus (s, t) = (x + s, y + t)$

$\odot$: $(x, y) \odot (s, t) = (xs + 2yt, xt + ys)$

- <u>okruh?</u> 1) $(A, \oplus)$ je komutativní grupa, což bylo dokázáno v <u>Př 4</u>| jen je to zde rozšířené nad racionální čísla.

2) $(A, \odot)$ je pologrupa?

- grupoid: $(x,y)\odot(s,t) = (\underbrace{xs+2yt}_{\in\mathbb{Q}}, \underbrace{xt+ys}_{\in\mathbb{Q}}) \in \mathbb{Q}\times\mathbb{Q}$ ✓

- asociativita:
  - $[(x,y)\odot(s,t)]\odot(u,v) = (xs+2yt, xt+ys)\odot(u,v) =$
    $= (xsu + 2ytu + 2xtv + 2ysv,\ xsv + 2ytv + xtu + ysu)$
  - $(x,y)\odot[(s,t)\odot(u,v)] = (x,y)\odot(su+2tv, sv+tu) =$
    $= (xsu + 2xtv + 2ysv + 2tu,\ xsv + xtu + ysu + 2ytv)$

✓ ((

$\Rightarrow (A,\odot)$ je pologrupa

3) distributivní zákon?

$(x,y)\odot[(s,t)\oplus(u,v)] = (x,y)\odot(s+u, t+v) = (xs+xu+2yt+2yv,\ xt+xv+ys+yu)$

$((x,y)\odot(s,t))\oplus((x,y)\odot(u,v)) = (xs+2yt, xt+ys)\oplus(xu+2yv, xv+yu) =$
$= (xs+xu+2yt+2yv,\ xt+xv+ys+yu)$ ✓

↪ levý distributivní zákon platí
pravý distributivní zákon se spočítá analogicky

$\Rightarrow$ je to okruh

- Komutativita operace $\odot$?

$$(x,y)\odot(s,t) = (xs+2yt,\ xt+ys) = (sx+2ty,\ tx+sy) = (s,t)\odot(x,y)$$

násobení je komutativní

$\Rightarrow$ abelovský okruh

- $(A,\odot)$ má neutrální prvek?

$$(x,y)\odot(\underline{1},\underline{0}') = (x,y) \qquad \Rightarrow (1,0)\in\mathbb{Q}\times\mathbb{Q},$$
$$(x\cdot\underline{1}+2y\cdot\underline{0}',\ x\cdot\underline{0}'+y\cdot\underline{1}) = (x,y)$$

neutrální prvek je $(1,0)$.

- obor integrity:
  - tento okruh je netriviální tj.: $(0,0)\neq(1,0)$ ✓
  - je komutativní ✓
  - má dělitele nuly?
    - musela by platit $(x,y)\odot(s,t)=(0,0) \Rightarrow (x,y)\neq(0,0)\wedge(s,t)\neq(0,0)$

$$(x,y)\odot(s,t)=(0,0)$$
$$(xs+2yt,\ xt+ys)=(0,0) \Rightarrow xs+2yt=0 \ \wedge\ xt+ys=0$$
$$\Downarrow$$
$$x=-\frac{2yt}{s}$$

- pokud by $y=0$, pak i $x=0$ a není splněna podmínka, že $(x,y)\neq(0,0)$. Totéž platí i pro s a t.

Tedy máme rovnice $xs+2yt=0$ a $xt+ys=0$

$\Downarrow$

$x=-\frac{2yt}{s}$ dosadíme do $xt+ys=0$

$\hookrightarrow -\frac{2yt}{s}\cdot t+ys=0$

$ys=\frac{2yt^2}{s}$ / vynásobíme s

$ys^2=2yt^2$ / vydělíme y

$s^2=2t^2$

$\frac{s^2}{t^2}=2$

$\frac{s}{t}=\pm\sqrt{2}$

$s,t\in\mathbb{Q} \Rightarrow \frac{s}{t}\in\mathbb{Q}$, ale $\pm\sqrt{2}\notin\mathbb{Q}$ (není to racionální číslo, ale iracionální)

$\Rightarrow$ tedy tyto dvě rovnice mají jediné řešení, a to, že jedna z uspořádaných dvojic se musí rovnat $(0,0)$

$\Rightarrow$ tj. nejsou zde dělitele nuly

$\Rightarrow$ je to obor integrity

- těleso? $(A\setminus\{0\},\cdot)$ obsahuje invertibilní prvky?

$(x,y)\odot(s,t)=(1,0)$

$(xs+2yt, xt+ys)=(1,0) \Rightarrow xs+2yt=1$ $\quad xt+ys=0$

$x=\frac{1-2yt}{s}\in\mathbb{Q}$ ✓ $\quad y=-\frac{xt}{s}\in\mathbb{Q}$ ✓

- inverzní prvek k (x,y) je $\left(\frac{1-2yt}{s}, -\frac{xt}{s}\right)$. $\Rightarrow$ je to těleso

Př 8| Máme algebru celých čísel $\mathbb{Z}$, kde jsou definované dvě operace:

$\oplus$: $x \oplus y = x + y - 1$, $\odot$: $x \odot y = x \cdot y - 1$

Pozn| Operace $\oplus$ a $+$ nejsou totéž a stejně i $\odot$ a $\cdot$ jsou dvě rozdílné operace!

- Zjistěte zda je to okruh?

1) $(\mathbb{Z}, \oplus)$ abelovská grupa?

- asociativita: $(x \oplus y) \oplus z = (x+y-1) \oplus z = x+y-1+z-1 = x+y+z-2$

$x \oplus (y \oplus z) = x \oplus (y+z-1) = x+(y+z-1)-1 = x+y+z-2$ ✓

- neutrální prvek: $x \oplus \_ = x$

$x + \underset{\uparrow}{\_} - 1 = x$

zde musí být $1 \in \mathbb{Z}$ ✓

tj. $x \oplus 1 = x$

$x + 1 - 1 = x$

$x = x$

neutrální prvek je 1.

- inverzní prvek: $x \oplus y = 1$

$x + y - 1 = 1$

$y = 2 - x \in \mathbb{Z}$

↳ inverzní prvek k x je $2-x$.

- komutativita: $x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$

sčítání je komutativní

$\Rightarrow$ je to abelovská grupa

2) $(\mathbb{Z}, \odot)$ je pologrupa?

- asociativita:

$$(x \odot y) \odot z = [illegible]$$
$$= (x \cdot y - 7) \odot z = (x \cdot y - 7) \cdot z - 7 = xyz - z - 7$$

$$x \odot (y \odot z) = x \odot (y \cdot z - 7) = x \cdot (y \cdot z - 7) - 7 = xyz - x - 7$$

$\not\equiv$ Nerovnají se !

↳ neplatí asociativita a tedy tato algebra není ani okruh.
(distributivita se tedy už nemusí dokazovat)

Pozn.: Využití vlastností algeber například u tzv. exponentiation by squaring
→ metoda pro rychlejší počítání mocnin.
př. protože platí asociativita můžeme vypočítat 3^4 více způsoby:
- $((3 \cdot 3) \cdot 3) \cdot 3$ což jsou 3 operace
- $(3 \cdot 3) \cdot (3 \cdot 3)$ což jsou pouze 2 operace

- obecně pro výpočet a^n je potřeba zhruba $\log_2 n$ násobení díky asociativitě.