3. ALGEBRAICKÉ STRUKTURY

Algebraická struktura – je množina nad níž je definována jedna či více operací a zároveň jsou tyto operace na té množině uzavřené
– základní algebraickou strukturou je tedy grupoid a pokud něco není ani grupoid, tak to není algebraická struktura
– $(N,+)$, $(N,+,\cdot)$ jsou
– $(Z,:)$, $(N,-)$ nejsou

Operace

– je nějaké zobrazení $A^n \to A$, A je množina; např.: $A \times A \to A$ je binární operace
– parciální operace – je definovaná jen pro některé prvky té množiny, ne pro všechny

Typy operací

- **Asociativní** – musí platit $(a \circ b) \circ c = a \circ (b \circ c)$ pro všechny $a,b,c \in A$ aby byla operace $\circ$ asociativní
  – $+$ a $\cdot$ jsou asociativní a $:$ není
- **Komutativní** – musí platit $a \circ b = b \circ a$ pro všechny $a,b \in A$ aby byla operace komutativní
  – zase $+$ a $\cdot$ jsou komutativní a $:$ není
- **Distributivní** – doposud to byly vlastnosti operací, ale distributivita je vlastnost jedné operace vzhledem k jiné operaci
  – $\cdot$ je distributivní nad $+$
  – $a \cdot (b+c) = a \cdot b + a \cdot c$
  – $(b+c) \cdot a = b \cdot a + c \cdot a$
- **Operace s dělením**
  $\forall (a,b) \in A^2, \exists (x,y) \in A^2: \overbrace{a \circ x = b}^{\text{levé děl.}} \wedge \overbrace{y \circ a = b}^{\text{pravé děl.}}$ – pokud tohle platí, tak operace $\circ$ je operace s dělením

  levé dělení ~~$y \circ a = b$~~ $a \circ x = b$, x je neznámá a je řešení v A pro každé $a,b \in A$

  pravé dělení $y \circ a = b$, y je neznámá a je řešení v A pro každé $a,b \in A$
  – pokud je $\circ$ komutativní a máme levé a pravé dělení, tak $\circ$ je i operace s dělením
  – zjednodušeně řečeno: pokud pro každou dvojici z množiny najdeme nějakou další dvojici z té množiny aby platilo že první prvek a první dvojice v operaci s (prvním) prvkem té druhé dvojice dá druhý prvek té první dvojice $(a \circ x = b)$ a zároveň prvek té druhé dvojice s prvním prvkem té první dvojice dá zase druhý prvek té druhé první dvojice
  – např. ani reálná čísla a $:$ – tedy $(R,:)$ je algebra s operací s dělením
  – třeba pro $(2,10)$ existuje $(0{,}2; 20)$ $2 : x = 10 \Rightarrow x = 0{,}2$ $y : 2 = 10 \Rightarrow y = 20$

! pokud A není prázdná množina a $\circ$ je asociativní operace tak platí že $\circ$ je operace s dělením a existuje neutrální prvek a každý prvek $a \in A$ je invertibilní (má inverzní prvek)

- **Operace s krácením**
  $\forall a, x_1, x_2, y_1, y_2 \in A: \underbrace{(a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2)}_{\text{levé krácení}} \wedge \overbrace{(y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2)}^{\text{pravé krácení}}$
  – tyto rovnice mají nanejvýš 1 řešení
  – pokud je $\circ$ asociativní tak mají právě jedno řešení

$\Rightarrow$ pro konečnou množinu A platí $\circ$ je operace s dělením $\Leftrightarrow$ $\circ$ je operace s krácením

Speciální prvky algeber

1) Neutrální prvek [e] buď 0 nebo 1

- levý neutrální prvek : $e \circ x = x$
- pravý neutrální prvek : $x \circ e = x$
- neutrální prvek : $e \circ x = x \circ e = x$
- je max. jeden pro každou operaci
  - pro aditivní operace [+] je to nulový prvek 0
  - pro multiplikativní operace [·] je to jednotkový prvek 1

Př.: Na $(\mathbb{Z}, \circ)$
$\circ$ je $a + b - 2$ pro $a \circ b$
$\circ$ je $a + e - 2$ pro $a \circ e$
$\circ$ je $e + a - 2$ pro $e \circ a$

$a + e - 2 = a$
$e = 2$

$e + a - 2 = a$
$e = 2$

2 je neutr. pr.

2) Inverzní prvek [$-a$, a^{-1}]

- prvek o jeho inverzní prvek musí dát neutrální prvek $\Rightarrow$ bez neutrálního prvku nemohou být ani inverzní prvky
- y je inverzní prvek k a právě tehdy když $\underbrace{a \circ y}_{\text{pravý inv. pr.}} = e \wedge \underbrace{y \circ a}_{\text{levý inv. pr.}} = e$ a $e = e$
- pokud a má inverzní prvek tak a je invertibilní $a \circ y = y \circ a = e$
  - pro aditivní operace [+] to je $-a$
  - pro multiplikativní operace [·] to je a^{-1}

Př.: Na $(\mathbb{Z}, \circ)$
kde $\circ$ je $a \circ b - 2$ pro $a \circ b$
$e = 2$

$a \circ a' - 2 = 2$
$a' = 4 - a$
$a' \circ a - 2 = 2$
$a' = 4 - a$

Univerzální algebra

$U = (A, (\omega_i)_{i \in I})$ I jsou indexy a A je množina a ω_i je n-ární operace

$(2, 2, 1, 0)$ – je algebra s 2 binárními operacemi, 1 unární a 1 nulární operací

Grupy

- mají vždy jen jednu binární operaci (grupoid a pologrupa mají jen jednu binární, monoid také ale má i jednu unární a grupa má vše předchozí a jednu nulární operaci)

1) Grupoid – výsledek operace (binární) daou hodnot z A končí zase v A (uzavřenost na množině A)

(2) ↳ jedna bin. operace

$\circ$	0	1
0	0	0
1	0	0

je grupoid

$\circ$	0	1
0	0	1
1	1	2

není grupoid

co není grupoid tak není ani algebra

2) Pologrupa – o musí být asociativní operace + je grupoid

(2)

$\circ$	0	1
0	0	0
1	0	0

je pologrupa $(\mathbb{N}, +)$ je pologrupa

$\circ$	0	1
0	1	1
1	1	0

není pologrupa

3) Monoid – musí mít neutrální prvek [e] + je pologrupa

(2, 0) ↳ neutr. prvek

$\circ$	0	1
0	0	1
1	1	0

je monoid $e = 0$ $(\mathbb{N}, +)$ je monoid a $e = 0$

4) Grupa – musí mít inverzní prvek [$-a$, a^{-1}] + je monoid

(2, 0, 1) ↳ inverzní prvek

$\circ$	0	1
0	0	1
1	1	0

je grupa 0 je neutrální prvek a 0 má inv. p. 0 a 1 má inv. p. 1

5) Abelovská grupa – o je komutativní operace + je grupa

(2, 0, 1) – např.

$\circ$	0	1
0	0	1
1	1	0

nebo $(\mathbb{Z}, +, 0, -a)$ – obojí jsou grupy a dokonce jsou Abelovské

Podgrupoid a podgrupa

- **podgrupoid** je část grupoidu pro kterou opět platí pravidlo uzavřenosti na nosné množině

∘	0	1	2
0	0	2	0
1	2	0	1
2	0	1	2

je grupoid

∘	0	1
0	0	2
1	2	0

není jeho podgrupoid ✗

∘	0	2
0	0	0
2	0	2

je jeho podgrupoid ✓

- podgrupoid nebo podgrupa je tedy podmnožina té nosné množiny přičemž operace zůstávají

~~podgrupoid~~

- **podgrupa** – je podgrupoid s vlastnostmi grupy
- **Lagrangeova věta** – počet prvků podgrupy je dělitelem počtu prvků grupy

Algebry s více operacemi (binárními)

1) Okruh – je $(A, +, 0, -a, *)$

$(2,0,1,2)$
$(A,+,0,-a,*)$

- kde $(A,+,0,-a)$ je Abelovská grupa, kde $+$ je uzavřené na A a $+$ je také komutativní a asociativní a 0 je neutrální prvek k $+$ a $-a$ je inverzní prvek k jakémukoliv $a \in A$ vzhledem k operaci $+$
- kde $(A,*)$ je pologrupa a tedy $*$ je uzavřené na A a zároveň je $*$ asoc.
- $*$ je distributivní vzhledem k operaci $+$ (násobení je distributivní vzhledem k operaci sčítání $\rightarrow a \cdot (b+c) = a \cdot b + a \cdot c$)

2) Komutativní okruh – víme, že $+$ je ~~...~~ komutativní, protože to je Abelovská grupa

$(2,0,1,2)$
$(A,+,0,-a,*)$

- nyní musí být i $*$ komutativní $(a * b = b * a)$ $\forall a,b \in A$
- zároveň je to okruh takže $(A,*)$ je pologrupa a $(A,+,0,-a)$ je AG

3) Okruh s jednotkovým prvkem

$(2,0,1,2,0)$
$(A,+,0,-a,*,1)$

- kde nemusí být $*$ komutativní jako ve 2)
- víme, že $+$ má neutrální prvek 0 – tedy nulový prvek
- zde potřebujeme neutrální prvek pro $*$ tedy 1 – tedy jednotkový prvek
- $(A,*,1)$ – je monoid

4) Komutativní okruh s jednotkovým prvkem

$(2,0,1,2,0)$
$(A,+,0,-a,*,1)$

- slučuje 2) a 3)
- $(A,+,0,-a,*)$ je komutativní okruh a má jednotkový prvek 1 pro operaci $*$

5) Obor integrity

$(2,0,1,2,0)$
$(A,+,0,-a,*,1)$

- je komutativní okruh s jednotkovým prvkem 1
- tedy $(A,*,1)$ je komutativní monoid (má neutrální, v tomto př. jednotkový prvek 1)
- A neobsahuje jen $0 \Longrightarrow A \setminus \{0\} \neq \emptyset$
- nejsou dělitelé $0 \Longrightarrow \forall a,b \in A \setminus \{0\}: a * b \neq 0$ a tedy $1 \neq 0$
- ! součin žádných dvou nenulových prvků nedá nulový prvek

6) Těleso

$(2,0,1,2,0,1)$
$(A,+,0,-a,*,1,a^{-1})$

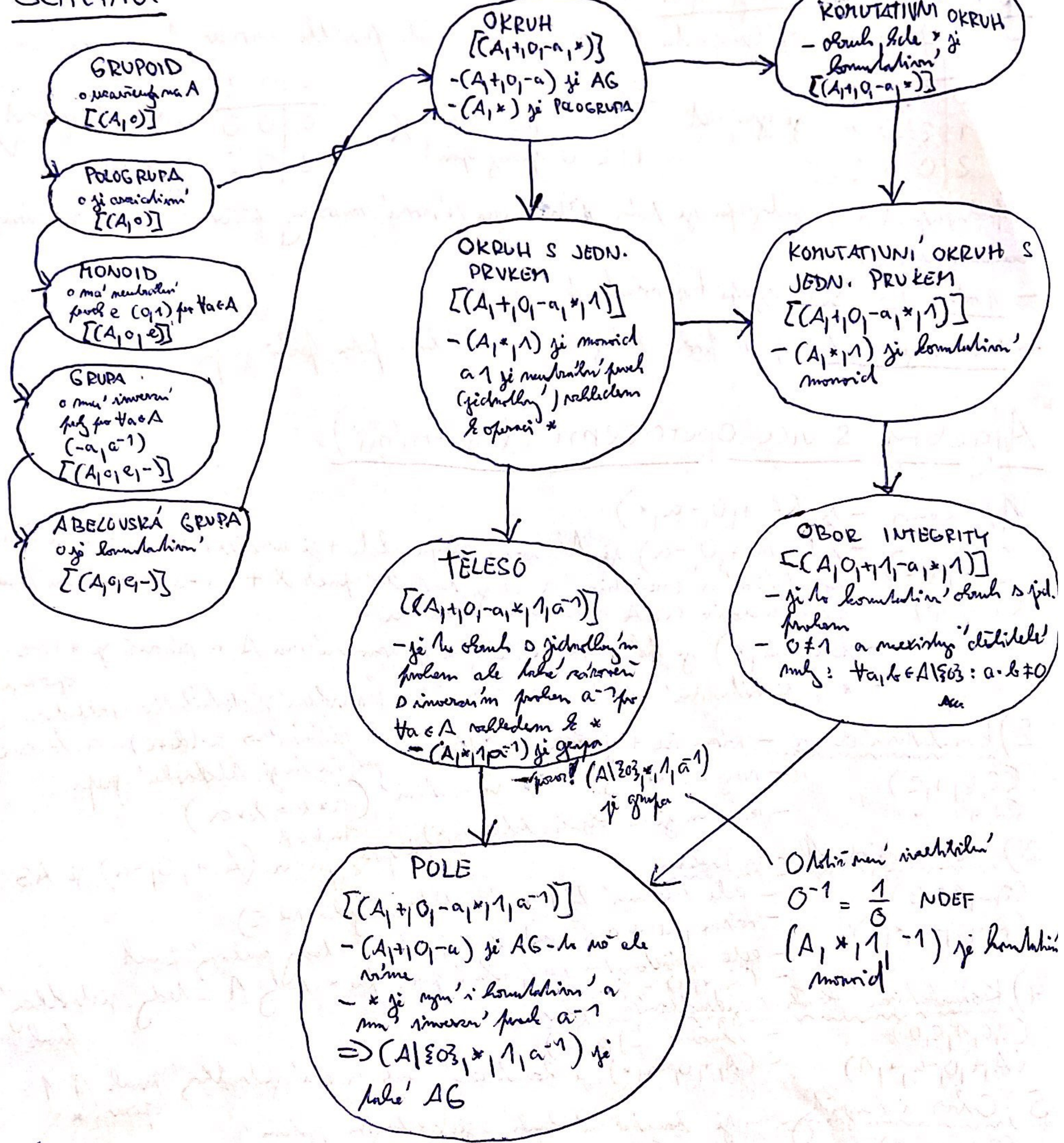
- víme že $(A,+,0,-a)$ je Abelovská grupa
- nyní musí platit, že $(A \setminus \{0\}, *, 1, a^{-1})$ je grupa

7) Pole

$(2,0,1,2,0,1)$
$(A,+,0,-a,*,1,a^{-1})$

- je komutativní těleso a tedy $(A,+,0,-a)$ je Abelovská grupa a $(A \setminus \{0\}, *, 1, a^{-1})$ je taky Abelovská grupa

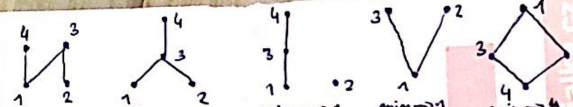
Schéma



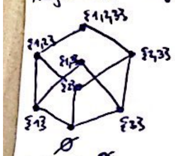
Př.: OKRUH − celá čísla s operacemi + a *

TĚLESO − ~~celá~~ racionální čísla s operacemi + a *
a asi i pole

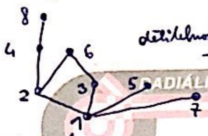
− ideálně asi říct že pole je Abelovská grupa a pologrupa která má jednotkový prvek a inverzní prvky (bez 0) a nejsou dělitelé nuly a je komutativní



min → 1,2	min → 1,2	min → 2,1	min → 1	min → 4
max → 3,4	max → 4	max → 4,2	max → 3,2	max → 1
nejv → X	nejv → 4	nejv → X	nejv → X	nejv → 1
nejm → X	nejm → X	nejm → X	nejm → 1	nejm → 4



min → ∅
max → {1,2,3}
nejv → {1,2,3}
nejm → ∅



dělitelnost – pokud by to dělitelnost na N tak by byl min a nejm ale nebyl by nejv ani max

min → 1
max → 8,6,5,7
nejv → X
nejm → 1

Základní a hlavní relace na množinách jsou relace (částečného) uspořádání a relace ekvivalence

≤ – relace částečného uspořádání porovnává a řadí prvky – proto je antisymetrická

≡ – relace ekvivalence rozděluje množinu do tříd ekvivalentních prvků (prvků, které mají stejné vlastnosti) – proto je symetrická

Relace uspořádání a svazy

částečně uspořádaná množina = uspořádaná množina

Částečně uspořádaná množina (A, R)

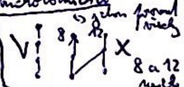
A → množina, R → relace uspořádání, (A, R) → (částečně) uspořádaná množina

- je to množina na které je dána relace částečného uspořádání $\leq$
- uspořádání je relace která je:
  - reflexivní – $\forall a \in A: aRa$ – každý prvek je v relaci sám se sebou
  - tranzitivní – $\forall a,b,c \in A: aRb \wedge bRc \rightarrow aRc$
  - antisymetrická (slabá) $\forall a,b \in A: aRb \wedge bRa \rightarrow a = b$

Př.: $(N, \leq)$, $(P(\{1,2,3\}), \subseteq)$ – pokud by to byla silná tak to je $\forall a,b \in A: aRb \rightarrow \neg(bRa)$

Lineárně uspořádaná množina (úplně, řetězec)

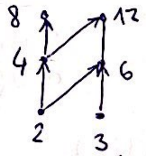
- je to částečně uspořádaná množina pro kterou platí že pro každé dva prvky lze určit který je větší (jsou porovnatelné) – reflexivní, antisymetrická, tranzitivní, trichotomická



Hasseův diagram – jde pro jakoukoliv relaci na konečné množině

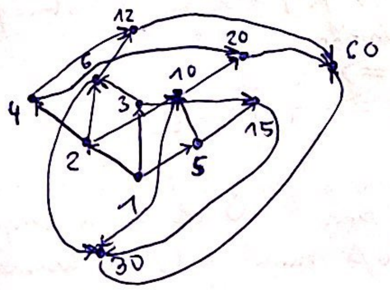
- používá se pro zobrazení konečné částečně uspořádané množiny $(S, \leq)$
- každý prvek $s \in S$ reprezentuje vrchol grafu a každé dva vrcholy propojené hranou říkají že $x \leq y$ a neexistuje žádné z které by bylo mezi nimi
- začíná se zdola a jde se nahoru
- kde jde šipka tam, nesmí jít zpátky → porušila by se antisymetrie

Př.: Uspořádání dělitelností na množině $S = \{2,3,4,6,8,12\}$



- mohla by vést i šipka z 2 do 8 a do 12 ale už mezi nimi je 4 případně 6 a neplatilo by $\leq$

Př.: Uspořádání dělitelnosti na množině $S = \{1,2,3,4,5,6,10,12,15,20,30,60\}$

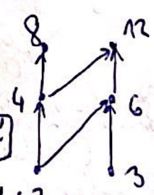


- začínáme od nejmenšího a děláme šipky k následujícím které dělí
- pokud jsme u nějakého prvku a přemýšlíme jestli z něj udělat šipku k dalším tak se nejdříve musíme podívat kam z tohoto prvku u kterého jsme už vedou šipky a jestli nebudou i oni to dělit a pokud ano tak je zkoumáme stejným způsobem a případně uděláme šipku

Nejmenší a největší prvek množiny (jeden)

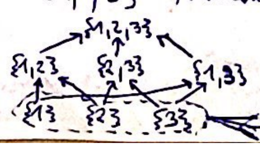
- všechny ostatní prvky množiny jsou větší/menší než tento
- v případě že prvo to není žádný

prvky jsou buď menší/větší nebo nejsou porovnatelné !



Minimální/maximální prvek množiny (více)

- nemusí být největší/nejmenší ale ten nejmenší/největší musí být z minimálních jediný
- minimální – žádný prvek není menší × maximální – žádný prvek není větší
- Př.: množina $\{1,2,3\}$ – vezmeme její potenční množinu bez $\emptyset$



- má největší prvek $\{1,2,3\}$ který je zároveň jediný maximální
- nemá nejmenší prvek ale má tři minimální

Horní/dolní závora množiny M

- množina M je podmnožinou N $M \subseteq N$
- dolní závoru tvoří všechny prvky ~~množiny~~ $\in N$ u kterých platí že žádný prvek množiny M není menší
  - zároveň i nejmenší prvek množiny je dolní závora (pokud jej množina má)
- u horní závory to je analogicky

Infimum/supremum

- největší prvek dolní závory je infimum
- nejmenší prvek horní závory je supremum

Př.: podmnožina reálných čísel interval $(0,1)$
- nemá minimální ani maximální prvky protože vždy najdeme nějaký menší/větší
- nemá ani největší/nejmenší
- má dolní závoru – třeba $0; -1; -0{,}001$ atd..
- má tedy infimum a to 0
- analogicky supremum 1

Svazy a Booleovy algebry

1) Svaz – algebra s dvěma binárními operacemi $\cup$ a $\cap$ přičemž obě dvě mají vždy stejné vlastnosti a označují supremum a infimum dvouprvkové množiny
   - pro každé dva prvky v množině svazu musí existovat supremum a infimum které je zase z toho svazu

$(A, \cup, \cap)$ – $\cap$ a $\cup$ jsou komutativní, asociativní a absorbční a idempotence $a \cap a = a \wedge a \cup a = a$

($\cap$ ↳ průsek, $\cup$ ↳ spojení)

$$a \cap (a \cup b) = a$$
$$a \cup (a \cap b) = a$$

2) Distributivní svaz – svaz a operace $\cap$ a $\cup$ jsou obě navzájem distributivní
   - $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
   - $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$

3) Ohraničený svaz – svaz (nemusí být distributivní) který má neutrální prvky přesně nulový 0 a jednotkový 1 prvek

$(A, \cup, \cap, 0, 1)$ $0 \in A$, $1 \in A$
   - 0 je neutrální pro $\cup \Rightarrow a \cup 0 = a$
   - 1 je neutrální pro $\cap \Rightarrow a \cap 1 = a$

4) Komplementární ohraničený svaz

$(A, \cup, \cap, 0, 1)$

   - má komplementární prvky (něco jako inverzní u okruhů a grup atd..)
   - je to ohraničený svaz
   - každý prvek $a \in A$ musí mít komplementární prvek $a \cap a' = 0 \wedge a \cup a' = 1$
   - zde vidíme že to musí být ohraničený svaz protože bez neutrálních prvků nejsou komplementární prvky

5) Booleův svaz – je to distributivní svaz a zároveň komplementární ohraničený svaz $(A, \cup, \cap, 0, 1)$

6) Booleova algebra – je to booleův svaz kde komplement je unární operace '

$(A, \cup, \cap, 0, 1, ')$
↳ je to tedy šestice

De Morganovy zákony

$(A')' = A$

$(A \cap B)' = A' \cup B'$ $(A \cup B)' = A' \cap B'$

! Otázka: Co vše musí mít Booleova algebra?
- nosnou množinu A, dvě binární operace $\cup$ a $\cap$ kde obě jsou komutativní, distributivní a asociativní a absorbční
- neutrální prvek 0 k operaci $\cup$ a neutr. pr. 1 k operaci $\cap$
- komplementární prvky a' a komplement jako operaci '

Schéma

SVAZ

$[(A,\cap,\cup)]$

– pro každé $a,b \in A$ existuje jejich infimum a supremum

– $\cup$ a $\cap$ jsou obě absorbční komutativní a asociativní

DISTRIBUTIVNÍ SVAZ

$[(A,\cap,\cup)]$

– $\cap,\cup$ jsou i distributivní

OHRANIČENÝ SVAZ

$[(A,\cap,\cup,0,1)]$

– má neutrální prvky

– 0 pro $\cup$: $a \cup 0 = a$

– 1 pro $\cap$: $a \cap 1 = a$

KOMPLEMENTÁRNÍ OHR. SVAZ

$[(A,\cap,\cup,0,1)]$

– pro všechna $a \in A$ platí že mají komplement a'

$a \cap a' = 0$

$a \cup a' = 1$

$0' = 1$ a $1' = 0$ – 0 a 1 jsou komplementy

BOOLEŮV SVAZ

$[(A,\cap,\cup,0,1)]$

– je komplementární ohraničený svaz a je zároveň distributivní

BOOLEOVA ALGEBRA

$[(A,\cap,\cup,0,1,')]$

– je booleův svaz kde komplement je unární operace

neutrální prvky jsou asi nulární operace