Algebraické struktury

ZPRACUJE: Mystik

Operace

Operace

Zobrazení $A^n \longrightarrow A$ se nazývá n-nární operace (0-nární operace = konstanta)

Parciální operace

Zobrazení není definováno pro všechny možné hodnoty operandů (např.: dělění je parciální operace, protože není definováno dělění nulou)

Cayleyova tabulka

Způsob zápisu definice binárních operací s konečným definičním oborem (sloupce jsou hodnoty prvního operandu, řádky hodnoty druhého operandu, příslušná buňka je výsledek operace)

Cayleyova tabulka pro binární sčítání

+	0	1
0	0	1
1	1	1

Typy operací

Asociativní

$$(x \circ y) \circ z = x \circ (y \circ z)$$

Komutativní

$$x \circ y = y \circ x$$

Distributivní (* distributivní nad +)

$x(y + z) = xy + xz$

$(y + z)x = yx + zx$

Operace s dělením

$$\forall (a,b) \in A, \exists (x,y) \in A : a \circ x = b \wedge y \circ a = b$$

Pokud A není prázdná tak ○ je operace s dělěním pokud je asociativní, existuje neutrální prvek a každý prvek A je invertibilní

Operace s krácením

$$a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2$$
$$x_1 \circ a = x_2 \circ a \Rightarrow x_1 = x_2$$

Rovnice $a \circ x = b$ a $y \circ a = b$ mají v operaci s krácením maximálně jendno řešení. Pokud je operace i asociativní tak mají práve jendo řešení.

Pro konečnou množinu A platí: ○ je operace s dělením $\Leftrightarrow$ ○ je operace s krácením

Absorbční zákony

(viz Svazy dole)

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

Algebry

Speciální prvky algeber

Neutrální prvek (vzhledem k operaci ○)

Levý neutrální prvek $e \circ x = x$

Pravý neutrální prvek $x \circ e = x$

Neutrální prvek $e \circ x = x \circ e = x$

- Existuje nejvýše jeden neutrální prvek pro každou operaci
- V multiplikativním značení (pro operace značené jako násobení) jej nazýváme jednotkový prvek (1)
- V aditivním značení (pro operace značené jako sčítání) jej nazýváme nulový prvek (0)

Inverzní prvek (k prvku x vzhledem k operaci ○)

Levý inverzní prvek $y \circ x = e$
Pravý inverzní prvek $x \circ y = e$
Inverzní prvek $y \circ x = x \circ y = e$

- Pokud existuje inverzní prvek k y, tak y nazýváme **invertibilní**
- Pokud je operace asociativní existuje nejvýče jeden inverzní prvek
- V multiplikativním značení jej značíme x^{-1}
- V aditivním značení jej značíme $-x$

Univerzální algebra

$U := (A, (\omega_i)_{i \in I})$ (množina hodnot, operace, operace, ...)

A - množina hodnot, I - množina indexů, ω_i -n_i-nární operace na A pro $i \in I$

Typ algebry

$U := (A, (n_i)_{i \in I})$

Popisuje typy operací v algebře. Např.: (2, 2, 1) je algebra s dvema binárními a jendou unární operací

Grupy

Algebry s jednou binární operací (a případně několika unárními operacemi)

Přehled typů grup

Název	Zápis	Asociativní	Neutrální prvek	Inverzní prvek	Komutativní	Poznámka
Grupoid	$(A, \circ)$	-	-	-	-	
Pologrupa	$(A, \circ)$	Ano	-	-	-	Asociativní grupoid
Monoid	$(A, \circ, e)$	Ano	Ano	-	-	Pologrupa + neutrální prvek
Grupa	$(A, \circ, e, ^{-1})$	Ano	Ano	Ano	-	Monoid + inverzní prvek
Abelovská grupa	$(A, \circ, e, ^{-1})$	Ano	Ano	Ano	Ano	Komutativní grupa

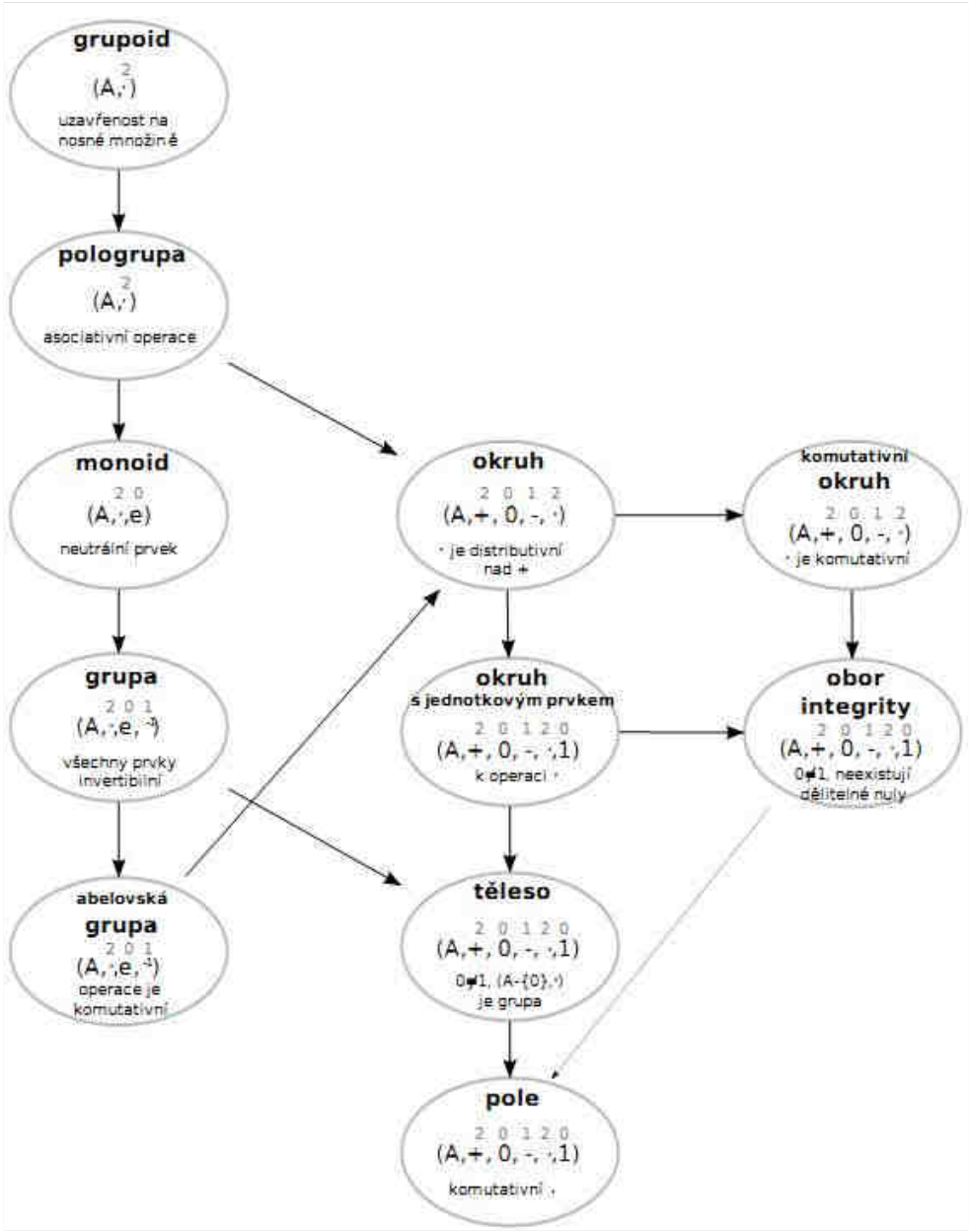
Okruhy, obory integrity, tělesa, pole

Algebry s dvěma binárními operacemi + a * (a případně několika unárními operacemi)

- Operace + tvoří abelovskou grupu
- nulový prvek = 0 = neutrální prvek pro operaci +
- jednotkový prvek = 1 = neutrální prvek pro operaci *
- Operace * je distributivní nad +

Přehled

Název	Zápis	* asociativní	* jednotkový prvek	* inverzní prvek (0 != 1)	* komutativní	Popis operace *	Poznámka
Okruh	$(A, +, 0, -, *)$	Ano	-	-	-	Pologrupa	
Komutativní okruh	$(A, +, 0, -, *)$	Ano	-	-	Ano	Komut. pologrupa	Okruh s komut. operací *
Okruh s jednotkovým prvkem	$(A, +, 0, -, *, 1)$	Ano	Ano	-	-	Monoid	Okruh s neutr. prvkem pro *
Komututativní okruh s jednotkovým prvkem	$(A, +, 0, -, *, 1)$	Ano	Ano	-	Ano	Komut. monoid	Okruh s komut. operací * s neutr. prvkem
Obor integrity	$(A, +, 0, -, *, 1)$	Ano	Ano	-	Ano	Monoid	Komut. okruh s jendn. prvkem, kde **neexistuje dělitel 0**
Těleso	$(A, +, 0, -, *, 1)$	Ano	Ano	Ano	-	Grupa	Okruh s jedn. prvkem a inverzním prvkem
Pole	$(A, +, 0, -, *, 1)$	Ano	Ano	Ano	Ano	Abelovksá grupa	Komutativní okruh



Svazy a Booleovy algebry

Algebry s dvěma binárními operacemi $\cap$ a $\cup$ (a případně několika unárními operacemi)

- Obě operace mají stejné vlastnosti
- nulový prvek = 0 = neutrální prvek pro operaci $\cup$
- jednotkový prvek = 1 = neutrální prvek pro operaci $\cap$
- Komplementární prvky: $a \cap a' = 0$ a $a \cup a' = 1$
- Jednotkový prvek anulový prvek josu komplementární: 0' = 1, 1' = 0

Přehled

Název	Zápis	Asociativní	Komutativní	Absorbční	Distributivní	Neutrální prvky	Komplementární prvky	Poznámka
Svaz	$(V, \cap, \cup)$	Ano	Ano	Ano	-	-	-	
Distributivní svaz	$(V, \cap, \cup)$	Ano	Ano	Ano	Ano	-	-	Svaz, kde operace jsou vzájemně distributivní
Ohraničený svaz	$(V, \cap, \cup, 0, 1)$	Ano	Ano	Ano	-	Ano	-	Svaz s nulovým a jednotkovým prvkem
Komplementární (ohraničený) svaz	$(V, \cap, \cup, 0, 1)$	Ano	Ano	Ano	-	Ano	Ano	Ohraničený svaz s komplementárními prvky

Booleův svaz	$(V, \cap, \cup, 0, 1)$	Ano	Ano	Ano	Ano	Ano	Ano	Distributivní a komplementární svaz (komplement existuje, ale není uveden jako operace)
Booleova algebra	$(V, \cap, \cup, 0, 1, ')$	Ano	Ano	Ano	Ano	Ano	Ano	Booleův svaz, kde je komplemet jako unární operace

Věta o komplementech v Booleově algebře

$(a')' = a$

$(a \cup b)' = a' \cap b', (a \cap b)' = a' \cup b'$ (DeMorganovy zákony)

Relace uspořádání a svazy

(Částečně) uspořádaná množina

množina na které je definována relace (obvykle značíme $\leq$) částečného uspořádání

- každá podmnožina uspořádané množiny je také uspořádaná
- Sousední prvky - prvky a, b mezi nimiž je relace $\leq$ a neexistuje žádná prvek c mezi nimi tj. takový, že $a < c < b$
- Hasseův diagram - graf, kde uzly jsou prvky množiny a hrany jsou mezi prvky, které jsou sousední dle relace $\leq$

Lineárně uspořádaná množina (řetězec)

částečně uspořádaná množina pro kterou platí srovnatelnost (u každých dvou prvků lze rozhodnout, který "je větší")

Nejmenší/největší prvek množiny

všechny prvky množiny jsou větší/menší než nejmenší/největší prvek množiny

- existuje vždy nejvýše jeden nejmenší/největší prvek

Maximální/minimální prvek množiny

žádný prvek není větší/menší než maximální/minimální prvek

- může jich být více

Dolní/horní závora množiny $M \subset N$

prvek z nad-množiny N, který je menší/větší než všechny prvky podmnožiny M

Infimum *inf(M)*

největší dolní závora

Infimum *sup(M)*

nejmenší horní závora

Svazově uspořádaná množina

Pro každé dva prvky existuje právě jedno společné supremum a infimum

- Pokud je $(V, \cap, \cup)$ svaz pak $(V, \leq)$ je svazově uspořádaná množina pokud platí $a \leq b \Leftrightarrow a \cap b = a$
- Inverzně: $(V, \cap, \cup)$ je svaz pokud definujeme operace jako $a \cap b = sup a, b$ a $a \cup b = inf a, b$

Princip duality

- Je-li $(V, \leq)$ uspořádaná množina pak i $(V, \geq)$ je uspořádaná množina
- Je-li $(V, \leq)$ svazově uspořádaná množina pak i $(V, \geq)$ je svazově uspořádaná množina
- Je-li $(V, \cap, \cup)$ svaz pak i $(V, \cup, \cap)$ je svaz
- Je-li $(V, \cap, \cup, 0, 1, ')$ Booleova algebra pak i $(V, \cup, \cap, 1, 0, ')$ je Booleova algebra

Odkazy

Kategorie Algebraické struktury na Wikipedii (cz) (http://cs.wikipedia.org/wiki/Kategorie:Algebraick%C3%A9_struktury)

Příklady k procvičení

1) Nechť $\mathbb{C}^*$ značí multiplikativní grupu všech nenulových komplexních čísel a G její podgrupu všech komplexních čísel s absolutní hodnotou 1.

Nechť $f : \mathbb{C}^* \to G$ je surjektivní zobrazení dané vztahem $f(z) = \frac{z}{|z|}$. Dokažte, že f je homomorfismus a určete (načrtněte) třídy kongruence dané jádrem zobrazení f.

2) Nechť $\mathbb{C}^*$ značí multiplikativní grupu všech nenulových komplexních čísel a $\mathbb{R}^+$ její podgrupu všech kladných reálných čísel. Nechť $f : \mathbb{C}^* \to \mathbb{R}^+$ je surjektivní zobrazení dané vztahem $f(z) = |z|$. Dokažte, že f je homomorfismus a určete (načrtněte) třídy kongruence dané jádrem zobrazení f.

3) Uvažujme algebru $\mathcal{A} = (\mathbb{Z}, t)$ s jednou unární operací t definovanou pro libovolné $x \in Z$ předpisem $t(x) = x + 1$

(a) Popište všechny podalgebry alegebry $\mathcal{A}$.

(b) Uvažujme rozklad množiny $\mathbb{Z}$, jehož třídy jsou všechny dvouprvkové množiny tvaru $\{2k, 2k + 1\}, k \in \mathbb{Z}$. Je příslušná ekvivalence kongruencí na algebře $\mathcal{A}$?

4) Na množině $\mathbb{C}$ komplexních čísel uvažujme operaci $+$ obvyklého sčítání. Buď $f : \mathbb{C} \to \mathbb{C}$ zobrazení dané předpisem $f(a + ib) = a - ib$. Pak:

(a) $(\mathbb{C}, +)$ není grupa

(b) f je zobrazení grupy $(\mathbb{C}, +)$ do sebe, které není homomorfismem

(c) f je homomorfismus grupy $(\mathbb{C}, +)$ do sebe, který není izomorfismem

(d) f je izomorfismus grupy $(\mathbb{C}, +)$ na sebe (tedy automorfismus)

(e) neplatí žádná z uvedených možností

5) Položme $P = \{f : \mathbb{R} \to \mathbb{R}; \exists a \in \mathbb{R} - \{0\} \forall x \in \mathbb{R} : f(x) = ax\}$. Dokažte, že $(P, \circ)$, kde $\circ$ značí skládání zobrazení, je grupoid. Zjistěte, zda $(P, \circ)$ je dokonce grupa (svůj závěr odůvodněte).

Kategorie: Matematické struktury v informatice | Státnice MAT | Státnice 2011

Stránka byla naposledy editována 25. 5. 2011 v 20:30.