3. Algebraické struktury (grupy, okruhy, obory integrity a tělesa, svazy a Booleovy algebry, univerzální algebry)

Klasifikace založená na grupách

Algebra $(A,\cdot)$ typu (2) se nazývá **grupoid**.

Grupoid $(H,\cdot)$ se nazývá **pologrupa** právě tehdy, když je $\cdot$ asociativní.

Pologrupa $(H,\cdot)/(H,\cdot,e)$ se nazývá **monoid** typu (2)/(2, 0), pokud e je neutrální prvek. Monoid je tedy asociativní algebra s neutrálním prvkem.

Monoid $(G,\cdot)$ / $(G,\cdot,e,{}^{-1})$se nazývá **grupa** typu (2)/(2, 0, 1)$\Leftrightarrow\forall x\in G$ je invertibilní, tj. $\forall x\in G\exists x^{-1}\in G{:}xx^{-1}=e$. Grupoid je tedy algebra, která je asociativní, má neutrální prvek a všechny prvky jsou invertibilní. Grupa, která je navíc i komutativní se nazývá **abelovská grupa**.

Algebra $(R,+,\cdot)$ / $(R,+,0,-,\cdot)$ se nazývá **okruh** typu (2, 2)/(2, 0, 1, 2) právě když je to vůči $(R,+)$ abelovksá grupou, vůči $(R,\cdot)$ pologrupa a operace $\cdot$ je distributivní nad $+$. Prvek 0 nazýváme **nulovým prvkem** okruhu vzhledem k $+$.

Okruh s jednotkovým prvek je algebra $(R,+,0,-,\cdot,1)$ typu (2, 0, 1, 2, 0), kde $(R,+,0,-,\cdot)$ je okruh a 1 je neutrální prvek vzhledem k $\cdot$, který nazýváme **jednotkovým prvkem** k násobení. Okruh s vlastností komutativity se nazývá **komutativní okruh**.

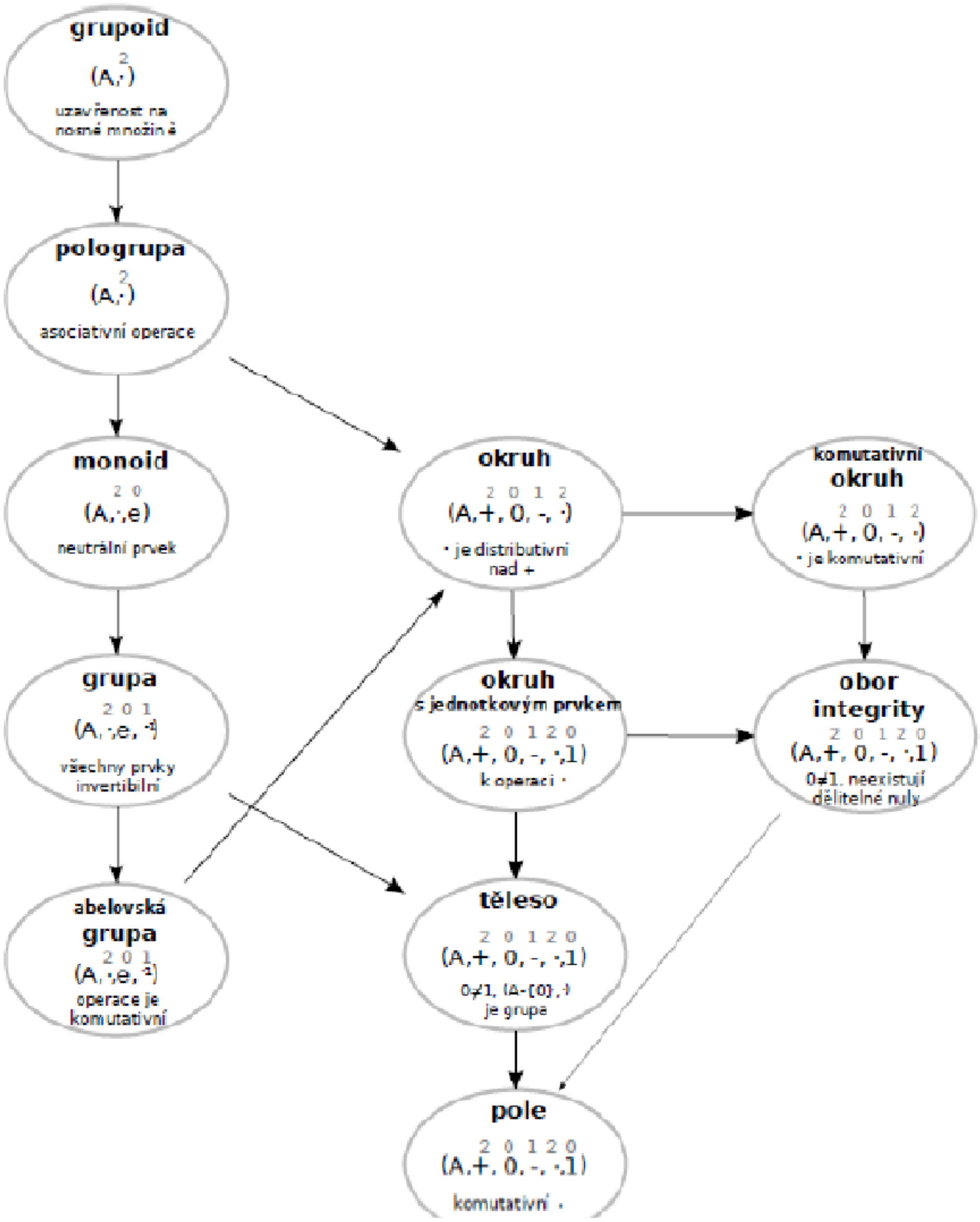
Komutativní okruh s jednotkovým prvkem se nazývá **obor integrity** $\Leftrightarrow$:

 $R\backslash\{0\} \neq \emptyset$ (tj. $0\neq1$ je netriviální, nosná množina obsahuje aspoň dva prvky);

 $\forall x,y \in R : x \neq 0 \land y \neq 0 \Rightarrow xy \neq 0$ (tj. neexistují dělitelé 0).

Okruh s jednotkovým prvkem $(R,+,0,-,\cdot,1)$ se nazývá **těleso**, pokud je netriviální a neobsahuje dělitele nuly.

Komutativní těleso se nazývá **pole** $\Leftrightarrow 0 \neq 1 \land$ $(R\backslash 0 ,\cdot)$ je abelovská grupa. Každé pole je tak obor integrity.



Vlastnosti grup

Základní vlastnosti, které vnímáme na množině reálných čísel, jako součin, pravidla pro počítání s mocninami.

Buď $G,\cdot,e,{-1}$ je grupa a $a\in G$. Potom **kardiální číslo (řád prvku)** je množství různých mocnin a:

$$\mathrm{o}\,(a) = |\{a^0{=}e, a^1, a^{-1}, a^2, a^{-2}, \ldots\}| = |\{a^k | k\in\mathbb{Z}\}|$$

Řádem grupy rozumíme $|G|$ mohutnost nosné množiny, kdy $\forall a\in G\colon \mathrm{o}(a)\leq G$.

Klasifikace založená na svazech

Svaz je algebra $(V,\cap,\cup)$ typu (2, 2), kde platí, že $\cap,\cup$ jsou komutativní i asociativní a platí **absorpční zákony** $X\cap(X\cup Y)=X$ a $X\cup(X\cap Y)=X$. Obecně nazýváme $\cap$ průsekem a $\cup$ spojením.

U svazů platí princip duality kdy svaz je $(V,\cap,\cup)$, právě když $(V,\cup,\cap)$ je svaz.

Svaz je **distributivním svazem**, když platí distributivní zákon svazů, kde je $\cup$ distributivní nad $\cap$, ale i $\cap$ je distributivní nad $\cup$:

$$a\cap(b\cup c)=(a\cap b)\cup(a\cap c) \text{ a } a\cup(b\cap c)=(a\cup b)\cap(a\cup c)$$

Prvek $0\in V$ se nazývá **nulový prvek svazu *V*** (neutrální k $\cup$)$\Leftrightarrow\forall a\in V: a\cup 0=a$ a prvek $1\in V$ se nazývá **jednotkový prvek svazu *V*** (neutrální k $\cap$)$\Leftrightarrow\forall a\in V: a\cap 1=a$. Svaz, který má oba tyto prvky, se nazývá **ohraničený svaz**.

Ohraničený svaz $(V,\cap,\cup,1,0)$ se nazývá **komplementární** $\Leftrightarrow\forall a\in V\exists a'\in V: a\cap a'=0 \wedge a\cup a'=1$. Prvek a' se nazývá **komplementem** a.

Distributivní a komplementární ohraničený svaz $(V,\cap,\cup,1,0)$ se nazývá **Booleův svaz**. Algebra $(B,\cap,\cup,1,0,')$ typu (2, 2, 0, 0, 1) se nazývá **Booleova algebra**.

Univerzální algebry

Buď A množina, $n\in\mathbb{N}_0$, pak zobrazení $\omega: A^n\to A$ nazýváme ***n*-ární operaci** na A. n je četnost (arita) operace.

pro $n\in\mathbb{N}_0$: ω: { $A_n\to A$

$A\times A\times\ldots A\to A$

$(x_1,x_2,\ldots,x_n)\mapsto\omega x_1 x_2\ldots x_n$

pro $n=0$:ω: { $A_0=\{\emptyset\}\to A$

$\emptyset\mapsto\omega\emptyset$

pro $n=2$:ω: { $A_2\to A$

$(x,y)\mapsto\omega xy=:x\omega y$

Buď A množina, $n\in\mathbb{N}_0, D\subseteq A^n$. Potom zobrazení $\omega: D\to A$ se nazývá ***n*-ární parciální operace**. Například dělení je parciální operace na množině $\mathbb{R}$, nelze dělit 0, neexistuje tedy zobrazení s 0 jakožto druhým operandem do $\mathbb{R}$.

Buď A množina, I množina indexů. Pro $i\in I$ buď ω_i n_i-ární operace na A, kde $n_i\in\mathbb{N}_0$. Potom $\mathfrak{A}=(A,(\omega_i)_{i\in I})=(A,\Omega)$ označuje **univerzální algebru** s nosnou množinou A a souborem operací $(\omega_i)_{i\in I}=:\Omega$

Systém arit operace je soubor $n_{i\,i\in I}$ se nazývá **typ** algebry (A,Ω). Algebry téhož typu jsou podobné.

Například $(\mathbb{Z},+,-,0,\cdot,1)$ je algebra typu (2, 1, 0, 2, 0).

Buď A množina, ∘ binární operace na A, pak prvek $e \in A$ se nazývá vzhledem k ∘:

 levý neutrální $\Leftrightarrow \forall x \in A$: $e \circ x = x$;

 pravý neutrální$\Leftrightarrow \forall x \in A$: $x \circ e = x$;

 neutrální$\Leftrightarrow \forall x \in A$: $e \circ \mathrm{x} = x \circ e = x$.

Buď A množina, ∘ binární operace na A, neutrální prvek e a $x \in A$. Potom prvek $y \in A$ se vůči x nazývá:

 levým inverzním$\Leftrightarrow$ $y \circ x = e$;

 pravým inverzním$\Leftrightarrow$ $x \circ y = e$;

 inverzním$\Leftrightarrow$ $y \circ \mathrm{x} = x \circ y = e$;

Ke každé operaci existuje nejvýše jeden neutrální prvek a inverzní prvek. Ke každé operaci inverzní prvek existovat nemusí (prvek není invertibilní), nebo může být prvek inverzní sám k sobě.

Asociativní zákon: Buď A množina, ∘ binární operace na A, pak ∘ se nazývá **asociativní** $\Leftrightarrow \forall x,y,z \in A$: $x \circ\ y \circ z = (x \circ y) \circ z$.

Komutativní zákon: Buď A množina, ∘ binární operace na A, pak ∘ se nazývá **komutativní** $\Leftrightarrow \forall x,y \in A$: $x \circ y = y \circ x$.

Distributivní zákon: Pokud jsou +,· binární operace nad A, potom · je **distributivní** nad + $\Leftrightarrow \forall x,y,z \in A$:

$x \cdot (y+z) = x \cdot y + x \cdot z$

 $\wedge$

$(y+z) \cdot x = y \cdot x + z \cdot x$