Od grupoidů ke grupám

Martina Vaváčková

Abstrakt. Příspěvek představuje grupoidy, neboli množiny s jednou binární operací. Seznamuje s různými typy grupoidů a uvádí množství příkladů, kde se s těmito strukturami můžeme setkat.

Grupoid je množina, na níž je zavedena jedna binární operace, tedy zobrazení, které každé dvojici prvků přiřazuje nějaký třetí prvek. Podle vlastností této operace lze grupoidy dále dělit – základní dělení si na přednášce představíme a osaháme.

Ačkoliv se nám (obzvlášť některé) grupoidy mohou na první pohled zdát podivné, uvidíme, že jsou vlastně docela přirozené a narážíme na ně i v běžném životě.

Formální definice a vlastnosti

Definice. (Grupoid) Množina G spolu s binární operací $\cdot : G \times G \to G$ se nazývá *grupoid* a značí se $(G, \cdot)$.

Cvičení. Určete, zda je a) $(\mathbb{N}, +)$, b) $(\mathbb{N}, -)$ grupoid.

Cvičení. Kolik existuje grupoidů na množině $\{1, 2\}$?

Má-li množina G konečně mnoho prvků, lze na ní zadat binární operaci pomocí tabulky výsledků – tzv. *Cayleyho tabulky.*

Příklad. Uvažujme množinu $\{0, 1, 2\}$ s operací sčítání modulo 3. Příslušná Cayleyho tabulka je:

$$\begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$$

Definice. (Některé základní vlastnosti grupoidů)

(i) Grupoid $(G, \cdot)$ je *asociativní*, jestliže pro všechna $a, b, c \in G$ platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

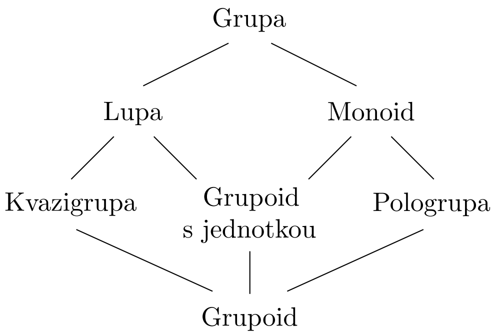
(ii) Grupoid $(G, \cdot)$ má *latinskou vlastnost*, jestliže pro všechna $a, b \in G$ existuje právě jedno x takové, že $a \cdot x = b$, a právě jedno y takové, že $y \cdot a = b$. Ekvivalentně, Cayleho tabulka operace $\cdot$ tvoří latinský čtverec.

(iii) Grupoid $(G, \cdot)$ má *jednotku*, jestliže existuje $e \in G$ takové, že pro všechna $a \in G$ platí $a \cdot e = e \cdot a = a$.
(iv) Grupoid $(G, \cdot)$ je *komutativní*, jestliže pro všechna $a, b, c \in G$ platí $a \cdot b = b \cdot a$.
(v) Prvek $a \in G$ je *idempotentní*, jestliže $a \cdot a = a$. Grupoid $(G, \cdot)$ je *idempotentní*, jestliže pro všechna $a \in G$ platí $a \cdot a = a$.

Cvičení. Ukažte, že každý grupoid má nejvýše jednu jednotku.

Hierarchie grupoidů

Asociativní grupoid se nazývá *pologrupa*. Pokud má navíc jednotku, jedná se o *monoid*. Grupoid s latinskou vlastností je *kvazigrupa*, a pokud má jednotku, nazývá se *lupa*. Asociativní grupoid s latinskou vlastností a jednotkou je *grupa*.[1]



Motivační příklady

Příklad. (Maximum) Množina $\mathbb{R}$ spolu s operací maxima, která každé dvojici čísel $a, b \in \mathbb{R}$ přiřadí to větší z nich, je komutativní idempotentní pologrupa.

Příklad. (Slova) Množina všech konečných posloupností znaků anglické abecedy spolu s operací „zřetězení" je monoid. Jednotkou je prázdná posloupnost.

Příklad. (Relativistické sčítání rychlostí) Množina všech reálných čísel z intervalu $(-c, c)$ spolu s operací $\oplus$ definovanou jako

$$u \oplus v = \frac{u + v}{1 + \frac{uv}{c^2}}$$

je komutativní lupa s jednotkou 0.

Příklad. (Aritmetický průměr) Množina $\mathbb{R}$ spolu s operací $\circ$ definovanou jako $a \circ b = \frac{a+b}{2}$ tvoří komutativní idempotentní kvazigrupu.

[1] Obvykle se grupa definuje jako asociativní grupoid s jednotkou a inverzními prvky, nicméně tato definice je ekvivalentní a pro naše účely výhodnější.

Cvičení a příklady

Cvičení 1. Ukažte, že kdykoliv G je kvazigrupa a pro $a, b, c \in G$ platí $a \cdot b = a \cdot c$ nebo $b \cdot a = c \cdot a$, pak $b = c$.

Cvičení 2. Nechť G je asociativní grupoid s latinskou vlastností. Ukažte, že G je grupa.

Cvičení 3. Nechť G je grupa. Ukažte, že pak ke každému $x \in G$ existuje prvek x^{-1} takový, že $x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzní prvek).

Cvičení 4. Ukažte, že každá idempotentní grupa je už nutně jednoprvková.

V následujících příkladech určete, o jaké struktury se jedná.

Příklad 1. Množina a) $\mathbb{Z}$, b) $\mathbb{Z}\backslash\{0\}$ s násobením.

Příklad 2. Množina $\{e, x, y\}$ spolu s operací $\cdot$ danou následující tabulkou:

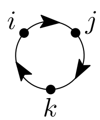
$\cdot$	e	x	y
e	e	x	y
x	y	e	x
y	x	y	e

Příklad 3. Permutace na množině $\{1, 2, 3, 4\}$ se skládáním.

Příklad 4. Komplexní čísla a jejich zobecnění – kvaterniony, oktoniony:

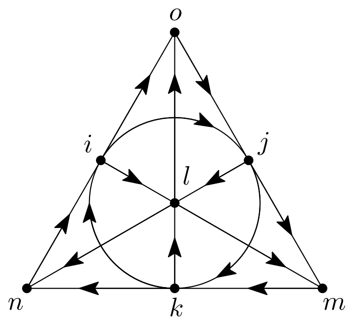
(1) Množina $\{\pm 1, \pm i\}$, kde i je komplexní jednotka splňující $i^2 = -1$, spolu s násobením komplexních čísel.

(2) Množina $\{\pm 1, \pm i, \pm j, \pm k\}$, kde i, j, k jsou komplexní jednotky splňující $i^2 = j^2 = k^2 = -1$, které se mezi sebou násobí dle následujícího schématu:



Kdykoliv $a \neq b$ a vede šipka od a k b, je $a \cdot b = c$ a $b \cdot a = -c$, kde c je třetí jednotka.

(3) Množina $\{\pm 1, \pm i, \pm j, \pm k, \pm l, \pm m, \pm n, \pm o\}$, kde i, j, k, l, m, n, o jsou komplexní jednotky splňující $i^2 = \cdots = o^2 = -1$, které se mezi sebou násobí dle následujícího schématu:



Kdykoliv $a \neq b$ a vede šipka od a k b, je $a \cdot b = c$ a $b \cdot a = -c$, kde c je třetí jednotka na úsečce spojující a a b.

Příklad 5. Množina funkcí $\alpha\colon X \to X$ s operací skládání $\circ$, definovanou jako $\alpha \circ \beta(x) = \alpha(\beta(x))$, $x \in X$.

Příklad 6. *Steinerův systém trojic* je množina X spolu se souborem neuspořádaných trojic T jejích prvků takovým, že pro každé $x, y \in X$ $(x \neq y)$ existuje právě jedno $z \in X$ splňující $\{x, y, z\} \in T$. Na X definujme operaci $\cdot$ následovně:

$$x \cdot y = \begin{cases} z, & \text{pokud } x \neq y \text{ a } \{x, y, z\} \in T, \\ x, & \text{pokud } x = y. \end{cases}$$

Příklad 7. Množina $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{Z} \right\}$ s maticovým násobením.

Příklad 8. Soubor podmnožin dané množiny s operací sjednocení.

Zdroje

Čerpala jsem především z přednášky *Binární systémy* Davida Stanovského na MFF UK, kterému tímto děkuji.