Monoidy, grupy, okruhy, tělesa

Grupoidy

Buď G množina. Uvažme libovolné zobrazení kartézské mocniny $G \times G$ do G. O takovém zobrazení říkáme, že je to **binární operace** na množině G. Je-li taková binární operace pevně zadána, pak jsou-li $a, b \in G$ libovolné prvky a je-li prvek $c \in G$ obrazem uspořádané dvojice (a, b) při tomto zobrazení, píšeme to zpravidla ve tvaru $c = a \cdot b$ a mluvíme o binární operaci $\cdot$. Podle okolností užíváme pro označení binárních operací i jiné zavedené symboly, například $+$, $*$, $\circ$ a podobně.

Je-li na množině G zadána binární operace $\cdot$, pak říkáme, že jde o **grupoid** a zapisujeme ho jako dvojici $(G, \cdot)$.

Příklady. Nechť $\mathbb{N} = \{1, 2, \dots\}$, $\mathbb{Z}$ a $\mathbb{Q}$ jsou množiny všech přirozených, celých a racionálních čísel. Pak dvojice $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, -)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q} - \{0\}, :)$, kde $+$, $-$, $\cdot$, $:$ jsou obvyklé operace sčítaní, odečítání, násobení a dělení v rámci číselných množin, jsou grupoidy.

Pro libovolnou množinu X jsme symbolem X^X označili množinu všech zobrazení množiny X do X a symbolem $\circ$ jsme značili skládání zobrazení. Pak dvojice $(X^X, \circ)$ je grupoid. Z následujícího odstavce vyplyne, že je to dokonce pologrupa.

Pologrupy

Nechť $(G, \cdot)$ je grupoid. Je-li pro každá $a, b, c \in G$ splněno

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

pak o operaci $\cdot$ říkáme, že je to **asociativní** operace, a o grupoidu $(G, \cdot)$ mluvíme jako o asociativním grupoidu, anebo častěji říkáme, že $(G, \cdot)$ je **pologrupa**.

Nechť znovu $(G, \cdot)$ je grupoid. Je-li pro každá $a, b \in G$ splněno

$$a \cdot b = b \cdot a,$$

pak o operaci $\cdot$ říkáme, že je to **komutativní** operace, a o grupoidu $(G, \cdot)$ mluvíme jako o komutativním grupoidu.

Příklady. Dvojice $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$ jsou komutativní pologrupy.

Tvrzení. Buď $(G, \cdot)$ pologrupa. Pak pro libovolné přirozené číslo n a pro libovolná $a_1, a_2, \ldots, a_n \in G$ výsledek součinu prvků $a_1, a_2, \ldots, a_n$ v dané pologrupě v uvedeném pořadí nezávisí na jejich uzávorkování.

Poznámka. Proto pak takový součin zapisujeme ve tvaru

$$a_1 \cdot a_2 \cdot \ \ldots \ \cdot a_n.$$

Důkaz se provede indukcí vzhledem k počtu prvků n.

Podobně lze dokázat také následující fakt.

Tvrzení. Buď $(G, \cdot)$ komutativní pologrupa. Pak pro libovolné přirozené číslo n a pro libovolná $a_1, a_2, \ldots, a_n \in G$ výsledek součinu prvků $a_1, a_2, \ldots, a_n$ nezávisí na jejich pořadí ani na uzávorkování.

Monoidy

Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** nebo též **jednotkový prvek** grupoidu $(G, \cdot)$, je-li pro každý prvek $a \in G$ splněno

$$e \cdot a = a = a \cdot e.$$

Tvrzení. V libovolném grupoidu $(G, \cdot)$ existuje nejvýše jeden jednotkový prvek.

Důkaz. Nechť $e, f \in G$ jsou jednotkové prvky grupoidu $(G, \cdot)$. Pak dostáváme

$$e = e \cdot f = f,$$

kde první rovnost plyne z toho, že f jednotkový prvek, a druhá rovnost plyne z toho, že e je jednotkový prvek. Takže $e = f$.

Z uvedeného tvrzení plyne, že má-li grupoid jednotkový prvek, je tento prvek jednoznačně určen. Proto se pro něj mnohdy používá speciální symbol, zpravidla je to symbol $\mathtt{1}$.

Je-li $(G, \cdot)$ pologrupa, která obsahuje jednotkový prvek $\mathtt{1}$, říkáme, že $(G, \cdot)$ je **monoid**.

Příklady. Dvojice $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$ jsou komutativní monoidy.

Znovu zopakujme, že pro libovolnou množinu X jsme symbolem X^X označili množinu všech zobrazení množiny X do X a symbolem $\circ$ jsme značili skládání zobrazení. Pak dvojice $(X^X, \circ)$ je monoid, neboť skládání zobrazení je asociativní operace na množině X^X a identické zobrazení id_X zde hraje roli jednotkového prvku. Tento monoid obecně není komutativní.

Grupy

Než definujeme pojem grupy, uvedeme několik přípravných poznatků.

Nechť $(G, \cdot)$ je grupoid s jednotkovým prvkem $\mathtt{1}$. Jestliže pro některý prvek $a \in G$ existuje prvek $b \in G$ takový, že platí

$$a \cdot b = \mathtt{1} = b \cdot a,$$

pak prvek a se nazývá **invertibilní prvek** grupoidu $(G, \cdot)$ a prvek b se nazývá **inverzní prvek** k prvku a v tomto grupoidu.

Tvrzení. V libovolném monoidu $(G, \cdot)$ existuje ke každému prvku $a \in G$ nejvýše jeden inverzní prvek.

Důkaz. Označme $\mathtt{1}$ jednotkový prvek monoidu $(G, \cdot)$. Nechť $b, c \in G$ jsou inverzní prvky k danému prvku $a \in G$, takže platí $a \cdot b = \mathtt{1} = b \cdot a$ a $a \cdot c = \mathtt{1} = c \cdot a$. Pak máme

$$b = b \cdot \mathtt{1} = b \cdot (a \cdot c) = (b \cdot a) \cdot c = \mathtt{1} \cdot c = c,$$

takže $b = c$.

Z uvedeného tvrzení plyne, že existuje-li v monoidu $(G, \cdot)$ k prvku $a \in G$ inverzní prvek, je tento prvek jediný a můžeme pro něj proto užít zvláštní označení. Zpravidla se tento inverzní prvek značí symbolem a^{-1}.

Tvrzení. Nechť $(G, \cdot)$ je monoid a nechť $\mathtt{1}$ je jeho jednotkový prvek. Nechť n je přirozené číslo a nechť $a, a_1, a_2, \ldots, a_n \in G$ jsou libovolné invertibilní prvky monoidu $(G, \cdot)$. Pak $\mathtt{1}$, a^{-1} a $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ jsou rovněž invertibilní prvky a platí rovnosti

$$\begin{aligned} \mathtt{1}^{-1} &= \mathtt{1}, \\ (a^{-1})^{-1} &= a, \\ (a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} &= a_n^{-1} \cdot \ldots \cdot a_2^{-1} \cdot a_1^{-1}. \end{aligned}$$

Důkaz. Toto tvrzení plyne z již dokázané jednoznačnosti inverzních prvků a z faktů, že $\mathtt{1}$ je inverzním prvkem k $\mathtt{1}$, a je inverzním prvkem k a^{-1} a $a_n^{-1} \cdot \ldots \cdot a_2^{-1} \cdot a_1^{-1}$ je očividně inverzním prvkem k $a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Nyní můžeme definovat výše avizovaný pojem grupy. Monoid $(G, \cdot)$, v němž ke každému prvku existuje prvek inverzní, to znamená monoid, jehož všechny prvky jsou invertibilní, se nazývá **grupa**.

Příklady. Dvojice $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$ jsou komutativní grupy.

Vezměme opět libovolnou množinu X a uvažujme dále libovolné bijekce $f : X \to X$. Takovým bijekcím jsme v minulé kapitole říkali permutace množiny X. Množinu všech permutací množiny X jsme označili $S(X)$. Pak skládání zobrazení $\circ$ je operací též na množině $S(X)$, takže dvojice $(S(X), \circ)$ je monoid, a je to dokonce grupa, neboť pro každou permutaci $f : X \to X$ je inverzní zobrazení $f^{-1} : X \to X$ permutací, která je k ní inverzním prvkem. Uvedená grupa se nazývá **grupa permutací** množiny X. Jde o grupu, která obecně není komutativní.

Z posledního tvrzení tohoto odstavce bezprostředně plyne ještě následující fakt.

Důsledek. Nechť $(G, \cdot)$ je monoid a nechť $H \subseteq G$ je množina všech invertibilních prvků monoidu $(G, \cdot)$. Pak množina H je uzavřená vzhledem k operaci $\cdot$, čili tato operace je operací i na množině H, a přitom dvojice $(H, \cdot)$ je grupa.

Okruhy

Budeme se dále zabývat strukturami se dvěma binárními operacemi. Mějme tedy množinu R, na níž jsou zadány dvě binární operace $+$ a $\cdot$. Takovou strukturu zapisujeme jako trojici $(R, +, \cdot)$. Předpokládejme navíc, že tato struktura splňuje následující podmínky:

$(R, +)$ je komutativní grupa,

$(R, \cdot)$ je monoid,

platí následující **distributivní** zákony:
pro každá $a, b, c \in R$ je splněno
$a \cdot (b + c) = a{\cdot}b + a{\cdot}c$ a $(a + b) \cdot c = a{\cdot}c + b{\cdot}c$.

Pak struktura $(R, +, \cdot)$ se nazývá **okruh**. Operace $+$, resp. $\cdot$ se pak nazývají sčítání, resp. násobení. Neutrální prvek grupy

$(R,+)$ se potom nazývá **nulový prvek** daného okruhu a označuje se symbolem 0. Inverzní prvek k prvku $a \in R$ v grupě $(R,+)$ se nazývá **opačný prvek** k prvku a a označuje se symbolem $-a$. Pro libovolné dva prvky $a, b \in R$ budeme symbolem $a - b$ označovat prvek $a + (-b)$. Neutrální prvek monoidu $(R,\cdot)$ se nazývá **jednotkový prvek** daného okruhu a označuje se symbolem 1.

Příklady. Nechť $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ jsou množiny všech celých, racionálních a reálných čísel. Pak trojice $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, kde $+$ a $\cdot$ jsou obvyklé operace sčítání a násobení v rámci číselných množin, jsou okruhy.

Tvrzení. Buď $(R,+,\cdot)$ okruh. Pak pro libovolná $a, b, c \in R$ platí

$$a \cdot 0 = 0 \cdot a = 0,$$
$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b),$$
$$a \cdot (b - c) = a{\cdot}b - a{\cdot}c \quad \text{a} \quad (a - b) \cdot c = a{\cdot}c - b{\cdot}c.$$

Důkaz faktu, že všechny tyto rovnosti plynou z definičních vlastností okruhu, je snadným cvičením.

Buď $R = \{e\}$ jednoprvková množina, na níž jsou definovány binární operace $+$ a $\cdot$ jediným možným způsobem, totiž tak, že $e + e = e$ a $e \cdot e = e$. Pak $(R,+,\cdot)$ je okruh, který se nazývá **triviální okruh**. Platí v něm $0 = e$ a $1 = e$, takže $0 = 1$. Ve skutečnosti platí i obrácené tvrzení, takže celkem máme:

Tvrzení. Buď $(R,+,\cdot)$ okruh. Pak $(R,+,\cdot)$ je triviální okruh právě tehdy, když v něm platí $0 = 1$.

Důkaz. Zbývá ukázat, že platí-li $0 = 1$ v nějakém okruhu $(R,+,\cdot)$, pak $(R,+,\cdot)$ je jednoprvkový, a tedy triviální okruh. Je-li však $0 = 1$, pak pro libovolný prvek $a \in R$ platí, že $a = a \cdot 1 = a \cdot 0 = 0$, takže $R = \{0\}$ a $(R,+,\cdot)$ je opravdu triviální okruh.

V každém netriviálním okruhu $(R,+,\cdot)$ tedy platí $0 \neq 1$.

Buď $(R, +, \cdot)$ okruh. Je-li operace $\cdot$ na R komutativní, tedy je-li $(R, \cdot)$ komutativní monoid, pak okruh $(R, +, \cdot)$ se nazývá **komutativní** okruh. Všechny výše uvedené příklady okruhů byly komutativní okruhy. Příklady nekomutativních okruhů budou uvedeny v následující kapitole.

Tělesa

Buď $(R, +, \cdot)$ netriviální okruh. Pak každý prvek $a \in R$, který je invertibilním prvkem monoidu $(R, \cdot)$, se nazývá **jednotka** okruhu $(R, +, \cdot)$ a prvek k němu inverzní se značí symbolem a^{-1}. Jednou z obecně mnoha jednotek netriviálního okruhu $(R, +, \cdot)$ je jeho jednotkový prvek 1. Podle závěrečného důsledku z odstavce o grupách víme, že množina všech jednotek netriviálního okruhu $(R, +, \cdot)$ je uzavřená vzhledem k operaci $\cdot$ a tvoří vzhledem k této operaci grupu.

Příklad. Jednotkami okruhu $(\mathbb{Z}, +, \cdot)$ všech celých čísel jsou právě čísla 1 a -1. Dvojice $(\{-1, 1\}, \cdot)$ tvoří dvouprvkovou grupu.

Netriviální komutativní okruh $(R, +, \cdot)$, jehož všechny nenulové prvky jsou jednotkami, se nazývá **těleso**. Jinak řečeno, netriviální okruh $(R, +, \cdot)$ je tělesem, jestliže množina $R - \{0\}$ je uzavřená vzhledem k operaci $\cdot$ a přitom $(R - \{0\}, \cdot)$ tvoří komutativní grupu.

Příklady. Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ a $(\mathbb{C}, +, \cdot)$ všech racionálních, reálných a komplexních čísel jsou tělesa. Tato tělesa jsou příklady těles, jimž říkáme **číselná tělesa**.

Existuje množství dalších příkladů těles. Zvláštní oblast tvoří konečná tělesa, o nichž zde není řeč.