Pologrupy, monoidy, grupy

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. 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.

Buď A libovolná množina a buď $\mathcal{P}(A)$ potenční množina množiny A. Pak dvojice $(\mathcal{P}(A), \cup)$, $(\mathcal{P}(A), \cap)$, $(\mathcal{P}(A), -)$, kde $\cup$, $\cap$ a $-$ jsou obvyklé operace sjednocení, průniku a rozdílu 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.

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.

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. Postupujeme indukcí vzhledem k n. Pro $n = 1$ a $n = 2$ není co dokazovat a pro $n = 3$ je tento fakt dán asociativitou operace $\cdot$. Nechť dále $n > 3$. Předpokládejme, že tvrzení platí pro všechny hodnoty $1, 2, 3, \ldots, n-1$ a dokažme, že pak platí také pro n. Zvolme libovolné uzávorkování součinu prvků $a_1, a_2, \ldots, a_n$ v tomto pořadí a označme a výsledek tohoto součinu. Pak existuje $k \in \{1, 2, 3, \ldots, n-1\}$ takové, že $a = b \cdot c$, kde b je součin prvků $a_1, a_2, \ldots, a_k$ a c je součin prvků $a_{k+1}, \ldots, n$, obojí při jistých uzávorkováních uvedených prvků. Ovšem podle indukčního předpokladu součin prvků $a_1, a_2, \ldots, a_k$ nezávisí na způsobu uzávorkování, takže lze psát $b = a_1 \cdot d$, kde d je součin prvků $a_2, \ldots, a_k$ při nějakém uzávorkování. Vzhledem k asociativitě operace $\cdot$ pak můžeme psát $a = (a_1 \cdot d) \cdot c = a_1 \cdot (d \cdot c)$, kde $d \cdot c$ je součinem prvků $a_2, \ldots, a_n$ při jistém uzávorkování. Ovšem opět podle indukčního předpokladu výsledek tohoto součinu zase nezávisí na způsobu uzávorkování. Máme tedy $a = a_1 \cdot (d \cdot c)$, kde prvek $d \cdot c$ nijak nezávisí na původně zvoleném uzávorkování součinu prvků $a_1, a_2, \ldots, a_n$. Tím je tvrzení dokázáno.

Podobně jednoduše 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 uzávorkování.

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.

Buď opět A libovolná množina a buď $\mathcal{P}(A)$ potenční množina množiny A. Pak dvojice $(\mathcal{P}(A), \cup)$, resp. $(\mathcal{P}(A), \cap)$ jsou komutativní monoidy, v nichž neutrálními prvky jsou podmnožiny $\emptyset$, resp. A.

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.

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 ústřední pojem této kapitoly. 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.

Buď ještě jednou A libovolná množina a buď $\mathcal{P}(A)$ potenční množina množiny A. Definujeme na množině $\mathcal{P}(A)$ binární operaci $\div$ **symetrické diference** následujícím předpisem. Pro libovolné dvě podmnožiny $B, C \subseteq A$ klademe

$$B \div C = (B \cup C) - (B \cap C) = (B - C) \cup (C - B).$$

Lze se přesvědčit o tom, že tato operace je asociativní na $\mathcal{P}(A)$ a že dvojice $(\mathcal{P}(A), \div)$ je komutativní grupa, neboť jednotkovým prvkem je zde prázdná podmnožina $\emptyset$ a každá podmnožina $B \subseteq A$ je zde inverzním prvkem sama k sobě.

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 této kapitoly 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.