Algebraické struktury

Grupy

Pro danou množinu G je *binární operace* na množině G zobrazení $f : G \times G \to G$. Binární operaci budeme obvykle značit symbolem $\cdot$ (další používané symboly jsou $+$, $\circ$) a psát „infixově“ místo „prefixově“, tj. budeme psát $a \cdot b$ místo $\cdot(a, b)$, nebo dokonce pouze ab.

Příklady binárních operací jsou sčítání, odčítání, násobení na množinách $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Pro dané $n \in \mathbb{N}_0$ hovoříme obecněji o *n-ární operaci* $f : G^n \to G$; toto n se nazývá *arita* operace f. Obvykle se f nazývá operace, místo přesnějšího n-ární operace, zvláště pokud je arita známá z kontextu.

Pro konečnou množinu G lze každou binární operaci $\cdot$ zadat tabulkou (tzv. *multiplikativní tabulka* operace), kde do políčka obsaženého v řádku označeném prvkem a a v slopci označeném prvkem b píšeme prvek $a \cdot b \in G$.

Operace $\cdot$ na množině G se nazývá *komutativní* pokud platí

$$(\forall a, b \in G)(\ a \cdot b = b \cdot a\ ),$$

nazývá se *asociativní* pokud

$$(\forall a, b, c \in G)(\ (a \cdot b) \cdot c = a \cdot (b \cdot c)\ ).$$

Poznamenejme, že pro asociativní operaci píšeme součiny více prvků $a_1 \cdot a_2 \cdot a_3 \cdots a_n$ bez závorek, neboť výsledek je vždy stejný prvek jakkoli jsou v součinu prvky „uzávorkovány“. Prvek $e \in G$ se nazývá *neutrální*, pokud

$$(\forall a \in G)(\ a \cdot e = e \cdot a = a\ ).$$

Neutrální prvek je vždy nejvýše jeden a obvykle se značí 1, případně 1_G. Dvojice $(G, \cdot)$ se nazývá *monoid*, pokud $\cdot$ je asociativní operace na množině G taková, že existuje neutrální prvek $1 \in G$.

Příkladem monoidu je $(A^A, \circ)$, kde A^A je množina všech zobrazení z množiny A do sebe a $\circ$ je skládání zobrazení, neutrální prvek v $(A^A, \circ)$ je identické zobrazení. Dalším příkladem monoidu je $(A^*, \cdot)$, kde A^* je množina všech slov nad abecedou A a $\cdot$ je operace zřetězení; neutrální prvek v $(A^*, \cdot)$ je prázdné slovo.

Pro prvek a monoidu $(G, \cdot)$ říkáme, že prvek b je k němu *inverzní* pokud $a \cdot b = b \cdot a = 1$. Pokud inverzní prvek (pro dané a) existuje, je určen jednoznačně a obvykle se značí a^{-1}. V tom případě říkáme, že prvek a je *invertibilní*. Všimněme si, že pokud prvek a je invertibilní, pak a^{-1} je také invertibilní, protože inverzní prvek k prvku a^{-1} je prvek a, tj. $(a^{-1})^{-1} = a$. Monoid kde je každý prvek invertibilní se nazývá *grupa*. Pokud je navíc operace komutativní, hovoříme o *komutativní grupě*.

Příklady grup: $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$, $(S(A), \circ)$ — množina všech bijekcí z množiny A do sebe s operací skládání zobrazení $\circ$.

Některé z těchto grup lze obdržet následující konstrukcí:

Věta Buď $(G, \cdot)$ monoid a G^* označme množinu všech invertibilních prvků z G. Pak $(G^*, \cdot)$ je grupa. (Přesněji $(G^*, \cdot|_{G^* \times G^*})$, kde $\cdot|_{G^* \times G^*}$ je zúžení zobrazení $\cdot : G \times G \to G$ na množinu $G^* \times G^*$.)

V předchozích příkladach $\mathbb{Q} - \{0\} = \mathbb{Q}^*$, $S(A) = (A^A)^*$.

Grupa zbytkových tříd Pro pevně zvolené přirozené číslo $n \in \mathbb{N}$ je relace ρ definovaná vztahy

$$a \rho b \iff a \equiv b\,(\bmod n) \iff n \mid a - b \iff a, b \text{ dávají stejný zbytek po dělení } n$$

relací ekvivalence na množině $\mathbb{Z}$. Příslušný rozklad $\mathbb{Z}\backslash\rho$ se značí $\mathbb{Z}_n$ a jednotlivé prvky ρ_a se nazývají zbytkové třídy (modulo n) a označují $[a]_n$. Tedy $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$ a rozklad $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$ má n prvků. Vztahy $[a]_n + [b]_n = [a + b]_n$ a $[a]_n \cdot [b]_n = [a \cdot b]_n$ korektně definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_n$, přičemž $(\mathbb{Z}_n, +)$ je komutativní grupa a $(\mathbb{Z}_n, \cdot)$ grupa není.

Všimněme si, že na přiřazení inverzního prvku lze nahlížet jako na unární (1-ární) operaci, tj. $^{-1} : G \to G$, $a \mapsto a^{-1}$ a podobně výběr neutrálního prvku 1 je 0-ární operace ($1 : G^0 \to G, \emptyset \mapsto 1$, kde $G^0 = \{\emptyset\}$).

V grupách lze také definovat libovolné celočíselné mocniny: pro grupu G a její prvek a definujeme pro libovolné přirozené číslo n mocninu a^n jako součin n kopií prvku a, dále a^0 klademe rovno neutrálnímu prvku 1 a pro záporné celé číslo n pak definujeme $a^n = (a^{-1})^{-n}$, tj. součin $-n$ kopií prvku a^{-1}. Lze ukázat, že všeobecně známé vztahy $a^n \cdot a^m = a^{n+m}$ a $(a^n)^m = a^{nm}$ platí v libovolné grupě.

Podgrupy

Podmnožina K grupy $(G, \cdot)$ se nazývá *podgrupa*, pokud je uzavřena na operace $\cdot, 1, ^{-1}$, přesněji, pokud platí následující podmínky

$$(\forall a, b \in K)(\ a \cdot b \in K\ ) \ \wedge\ (1 \in K) \ \wedge\ (\forall a \in K)(\ a^{-1} \in K\ ).$$

Např: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ jsou podgrupy grupy $(\mathbb{C}, +)$. Pro libovolnou grupu $(G, \cdot)$ jsou G i $\{1\}$ podrupy (tzv. triviální). V grupě $(\mathbb{Z}, +)$ jsou podgrupy právě množiny $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ pro libovolné $n \in \mathbb{N}_0$ — pro $n = 0$ a $n = 1$ dostáváme triviální podgrupy.

Poznamenejme, že průnik libovolného neprázdného systému podgrup dané grupy G je opět podgrupou grupy G. Proto systém všech podgrup grupy G, uspořádaný inkluzí, tvoří úplný svaz.

Homomorfismy a součiny grup

Zobrazení $f : G \to H$ se nazývá *homomorfismus* z grupy $(G, \cdot)$ do grupy $(H, \circ)$ pokud platí:

$$(\forall a, b \in G)(\ f(a \cdot b) = f(a) \circ f(b)\ ).$$

Lze dokázat, že potom taktéž platí $f(1_G) = 1_H$ a pro libovolné $a \in G$ platí $f(a^{-1}) = f(a)^{-1}$ (pozor, zde se inverze počítají v odlišných grupách). Bijektivním homomorfismům říkáme *izomorfismy* a dvě grupy jsou *izomorfní* pokud existuje izomorfismus mezi nimi. (Neformálně lze říci, že dvě grupy jsou izomorfní jestliže jsou stejné až na přejmenování prvků.)

Příklady: pro libovolné $n \in \mathbb{N}$ jsou zobrazení $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = na$, respektive $g : \mathbb{Z} \to \mathbb{Z}_n$, $g(a) = [a]_n$ homomorfismy z grupy $(\mathbb{Z}, +)$ do sebe, repektive do grupy $(\mathbb{Z}_n, +)$. Zobrazení $log : \mathbb{R}^+ \to \mathbb{R}$ je izomorfismus grupy $(\mathbb{R}^+, \cdot)$ všech kladných reálných čísel s násobením do grupy $(\mathbb{R}, +)$ všech reálných čísel se sčítáním.

Uvažujme monoid $(\mathbb{Z}_7, \cdot)$ a v něm podmnožinu invertibilních prvků $\mathbb{Z}_7^* = \mathbb{Z}_7 - \{[0]_7\}$. Potom zobrazení $f : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ dané předpisem $f([a]_6) = [3]_7^a$ je izomorfismus grup. Poznamenejme, že ne vždy podobný předpis korektně definuje zobrazení. Zde například je definice zobrazení korektní: pokud $[a]_6 = [b]_6$, pak existuje $k \in \mathbb{Z}$ tak, že $a = b + 6k$ a proto $[3]_7^a = [3]_7^{b+6k} = [3]_7^b \cdot ([3]_7^6)^k = [3]_7^b \cdot [1]_7^k = [3]_7^b$, tedy obraz prvku $[a]_6$ nezávisí na volbě reprezentanta v třídě $[a]_6$. Naopak, předpis $f : \mathbb{Z}_5 \to \mathbb{Z}_7^*$, $f([a]_5) = [3]_7^a$ nedefinuje korektně zobrazení, protože $[1]_5 = [6]_5$, přičemž $[3]_7^1 = [3]_7 \neq [1]_7 = [3]_7^6$ a není tedy jednoznačně určen obraz prvku $[1]_5 = [6]_5$. Připomeňme, že stejným způsobem se ověřuje korektnost definice sčítání a násobení na $\mathbb{Z}_n$, tj. $[a]_n = [c]_n, [b]_n = [d]_n \implies [a + b]_n = [c + d]_n, [a \cdot b]_n = [c \cdot d]_n$.

Pro libovolnou grupu $(G, \cdot)$ je identické zobrazení izomorfismus a zobrazení definované předpisem $f(a) = 1_H$, pro libovolné $a \in G$, homomorfismus do libovolné grupy $(H, \circ)$.

Jádro homomorfismu $f : G \to H$ je množina $Ker(f) = \{a \in G \mid f(a) = 1_H\}$. (Pozor, připomeňme, že jádro zobrazení je relace na množině G, kdežto jádro homomorfismu grup je podmnožina G. Snadno se nahlédne, že

$$(a, b) \in J_f \iff f(a) = f(b) \iff f(ab^{-1}) = 1_H \iff ab^{-1} \in Ker(f),$$

což vysvětluje, proč se v teorii grup pracuje s Ker(f), neboť relace J_f je touto množinou již plnně popsána.) Jádro je podgrupa grupy G. *Obraz homomorfismu* $f : G \to H$ je množina $Im(f) = \{f(a) \mid a \in G\}$. Obraz je podgrupa grupy H.

Součin grup $(G, \cdot)$ a $(H, \circ)$ je množina $G \times H$ společně s operací $*$ definovanou předpisem $(a, b) * (c, d) = (a \cdot c, b \circ d)$ pro $a, c \in G, b, d \in H$. Poznamenejme, že zobrazení projekce $p_1 : G \times H \to G, p_1((a, b)) = a$ je homomorfismus grup. Grupy $G \times H$ a $H \times G$ jsou izomorfní

Grupa komplexních čísel $(\mathbb{C}, +)$ je izomorfní grupě $(\mathbb{R}, +) \times (\mathbb{R}, +)$. Grupa $(\mathbb{R}^*, \cdot)$ je izomorfní grupě $(\{1, -1\}, \cdot) \times (\mathbb{R}^+, \cdot)$.

V elementární teori grup lze například ukázat, že počet prvků konečné grupy je násobkem počtu prvků libovolné její podgrupy. Dále lze ukázat, že libovolná konečná komutativní grupa je izomorfní jistému součinu grup $\mathbb{Z}_{n_i}$. Tyto poznatky jsou obsahem kurzu Algebra I.

Okruhy

Množina R spolu s dvěmi operacemi $+$ a $\cdot$ se nazývá *okruh* pokud $(R, +)$ je komutativní grupa, $(R, \cdot)$ je monoid a pro operace $+$ a $\cdot$ platí tzv. *distributivní zákony*, tj. platí

$$(\forall a, b, c, \in R)(\ a \cdot (b + c) = a \cdot b + a \cdot c \ \wedge\ (b + c) \cdot a = b \cdot a + c \cdot a\ ).$$

Příklady okruhů jsou $(\mathbb{Z}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, dále okruhy čtvercových matic $n \times n$ nad daným okruhem (např. $\mathbb{Z}$) a také okruhy polynomů nad daným okruhem (např. $\mathbb{R}$). Pro libovolné přirozené číslo n je $(\mathbb{Z}_n, +, \cdot)$ okruh.

Abychom odlišili dvě operace, užíváme pro první z nich výhradně aditivní notaci (tj. symbol $+$, neutrální prvek 0, inverze $-$) a pro druhý notaci multiplikativní (tj. symbol $\cdot$, neutrální prvek 1, případná inverze $^{-1}$).

Pokud je operace $\cdot$ komutativní, hovoříme o *komutativním okruhu*.

Pokud má okruh pouze jeden prvek, pak hovoříme o *triviálním* okruhu. V opačném případě se jedná o okruh *netriviální*. Poznamenejme, že v netriviálním okruhu vždy $0 \neq 1$.

Lze ukázat, že prvek 0 je tzv. *nulový prvek* vzhledem k násobení, tj. $0 \cdot a = a \cdot 0 = 0$ pro libovolné $a \in R$ a proto neexistuje k prvku 0 prvek inverzní.

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení se nazývá *těleso*. Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou tělesy. Okruh $(\mathbb{Z}, +, \cdot)$ těleso není. Okruh $(\mathbb{Z}_n, +, \cdot)$ je těleso právě tehdy, když n je prvočíslo.

Netriviální komutativní okruh $(R, +, \cdot)$ se nazývá *obor integrity*, pokud pro libovolné nenulové prvky $a, b \in R$ platí $a \cdot b \neq 0$. Každé těleso je oborem integrity. Naopak lze dokázat, že každý konečný obor integrity je těleso. Příklady oborů integrity, které nejsou tělesy jsou $(\mathbb{Z}, +, \cdot)$, nebo okruhy polynomů nad obory integrity.

Podokruhy a homomorfismy okruhů

Podmnožina M okruhu $(R, +, \cdot)$ se nazývá *podokruh* pokud je uzavřena na všechny operace, přesněji pokud platí

$$(\forall a, b \in M)(\ a + b, 0, -a, a \cdot b, 1 \in M\ ).$$

Všimněme si, že podokruh okruhu je opět okruhem, podokruh oboru integrity je obor integrity, ale podokruh tělesa nemusí být těleso.

Důležité příklady okruhů tedy vznikají jako podokruhy okruhu $(\mathbb{C}, +, \cdot)$. Například podokruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ nebo podokruh $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{3}i \mid a, b \in \mathbb{Z}\}$ či podokruh okruhu reálných čísel $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

Zobrazení $f : R \to S$ se nazývá homomorfismus okruhů $(R, +, \cdot)$ a $(S, +, \cdot)$ pokud platí:

$$(\forall a, b \in R)(\ f(a + b) = f(a) + f(b)\ ) \ \wedge\ (\forall a, b \in G)(\ f(a \cdot b) = f(a) \cdot f(b)\ ) \ \wedge\ f(1_R) = 1_S.$$

Bijektivním homomorfismům říkáme izomorfismy a dva okruhy jsou izomorfní pokud existuje izomorfismus mezi nimi.

Příkladem homomorfismu je komplexní konjugovanost, tj. $f : \mathbb{C} \to \mathbb{C}$, $f(a + bi) = a - bi$ je izomorfismus okruhu $(\mathbb{C}, +, \cdot)$ na sebe. Dále $g : \mathbb{Z} \to \mathbb{Z}_n$, $g(a) = [a]_n$ je homomorfismus okruhu $(\mathbb{Z}, +, \cdot)$ do okruhu $(\mathbb{Z}_n, +, \cdot)$.

Jádro homomorfismu se definuje podobně jako pro grupy: $Ker(f) = \{a \in R \mid f(a) = 0\}$.