

Okruhy

Úvod

Kategorizácia štruktúr s dvoma operáciami.

Reč bude o množinách s dvoma operáciami $(R, \oplus, \otimes)$. Písmeno R je od slova ring (okruh). Nech sú obe operácie prakticky definované akokoľvek, formálne budeme prvú považovať za aditívnu a druhú za multiplikatívnu. Označenie $+ a *$ v krúžku však naznačuje, že nemusí ísť o klasické $+ a *$.

Podobne ako pri štruktúrach s jednou operáciou, aj tu budeme rozlišovať rozličné typy/názvy štruktúr podľa toho, aké vlastnosti operácie $\otimes$ sa nám podarí dokázať. Operácia $\oplus$ musí svoje vlastnosti spĺňať vždy v plnej miere.

a) Nutný základ I. – $(R, \oplus)$

$(R, \oplus)$ musí byť **abelovská grupa**, tj. operácia $\oplus$ musí byť operácia na R , asociatívna, komutatívna, musí existovať neutrálny prvok e_0 ("nula", $\ominus$) a každý prvok x z R musí mať inverzného kamaráta $-x$ (kde "-" nie je nutne klasické mínus, ale "opak" ku $\oplus$).

b) Nutný základ II. – distributívny zákon

Vzájomný vzťah operácií $\oplus, \otimes$ musí byť harmonický – musí platiť distributívny zákon "roznásobovania":

$$\begin{aligned} a \otimes (b \oplus c) &= (a \otimes b) \oplus (a \otimes c) \\ (b \oplus c) \otimes a &= (b \otimes a) \oplus (c \otimes a) \end{aligned}$$

c) Nutný základ III. – $(R, \otimes)$

Operácia $\otimes$ musí byť operáciou na R , tj. $(R, \otimes)$ musí byť grupoid.

Splnenie predpokladov a,b,c samo osebe ešte nedáva nárok na žiadne tituly, ale je ich nutným základom a východiskom. Ak a,b,c nie sú splnené alebo sú splnené len čiastočne, ide o štruktúry, ktorými sa v tomto semestri nebudeme zaoberať.

d) Kategorizácia podľa vlastností $(R, \otimes)$

– Ak je $\otimes$ asociatívna, teda $(R, \otimes)$ je pologrupa, štruktúra $(R, \oplus, \otimes)$ sa nazýva **pseudookruh, okruh bez jednotky, rng (ring bez i)**
/ Ak je $\otimes$ komutatívna, ide o **komutatívny pseudookruh (kom. okruh bez jednotky)**.

– Ak navyše pre $\otimes$ existuje neutrálny prvok e_1 ("jednotka", $\mathbb{1}$), teda $(R, \otimes)$ je monoid, tak $(R, \oplus, \otimes)$ sa nazýva: **okruh, okruh s jednotkou, ring**
/ Ak je $\otimes$ komutatívna, ide o **komutatívny okruh (kom. okruh s jednotkou)**.

– Ak navyše platí $a \otimes b = \ominus \Rightarrow a = \ominus \vee b = \ominus$, štruktúra $(R, \oplus, \otimes)$ sa nazýva **okruh bez deliteľov "nuly"**
/ Ak je $\otimes$ komutatívna, ide o **obor integrity**.

Táto vlastnosť je slabším odvarom existencie inverzných prvkov a nemusíme ju overovať, ak dokážeme platnosť nasledujúceho bodu.

– Ak pri $\otimes$ existujú inverzné prvky x^{-1} pre všetky prvky x z R okrem "nuly", teda $(R \setminus \{\ominus\}, \otimes)$ je grupa, tak štruktúra $(R, \oplus, \otimes)$ sa nazýva **teleso**.
/ Ak je $\otimes$ komutatívna, ide o **pole**.

Riešené príklady

Príklad 1

Kategorizujme štruktúru $(2\mathbb{Z}, +, *)$, teda množinu párnych čísel a klasické plus, krát.

Riešenie:

a) $(2\mathbb{Z}, +)$

Operácia $+$ je operáciou aj na výlučne párnych číslach.

$+$ je asociatívna aj komutatívna, neutrálny prvok je 0, inverzný ku x je $-x$. ✓

b) Distributívny zákon pre $+$, $*$ platí. ✓

c) $(2\mathbb{Z}, *)$

Operácia $*$ je operáciou aj na výlučne párnych číslach.

$*$ je asociatívna aj komutatívna.

Neutrálny prvok by mal byť 1, ale ten sa v definičnom obore nenachádza.

Záver: **Komutatívny okruh bez jednotky (pseudookruh)**

Príklad 2

Kategorizujme štruktúru $(\mathbb{R}^2, +, *)$, teda množinu dvojíc reálnych čísel a klasické plus, krát aplikované "po zložkách".

Riešenie:

a) $(\mathbb{R}^2, +)$

Operácia $+$ je operáciou aj na dvojiciach čísel.

$+$ je asociatívna aj komutatívna, neutrálny prvok je $\textcircled{0} = [0,0]$, inverzný ku $[x,y]$ je $[-x,-y]$. ✓

b) Distributívny zákon pre $+$, $*$ platí. ✓

Platí na každej zložke osobitne a to stačí, lebo zložky sa navzájom neovplyvňujú.

c) $(\mathbb{R}^2, *)$

Operácia $*$ je operáciou aj na dvojiciach čísel.

$*$ je asociatívna aj komutatívna.

Neutrálny prvok je $\textcircled{1} = [1,1]$.

Delitele "nuly" – existujú, napr.: $[x,0] * [0,y] = [0,0]$

Záver: **Komutatívny okruh s jednotkou (ale už nie "bez deliteľov nuly")**

Príklad 3

Kategorizujme štruktúru $(\mathbb{Z}_v, +, *)$, kde $\mathbb{Z}_v = \{a+b\sqrt{2}; a,b \in \mathbb{Z}\}$.

Riešenie:

a) $(\mathbb{Z}_v, +)$

Operácia $+$ je operáciou na $\mathbb{Z}_v$: $a+b\sqrt{2} + c+d\sqrt{2} = (a+c)+(b+d)\sqrt{2}$

$+$ je asociatívna aj komutatívna, neutrálny prvok $0 = 0+0\sqrt{2}$, inverzný ku $a+b\sqrt{2}$ je $-a-b\sqrt{2}$. ✓

b) Distributívny zákon pre $+$, $*$ platí. ✓

c) $(\mathbb{Z}_v, *)$

Operácia $*$ je operáciou aj na $\mathbb{Z}_v$.

$$(a+b\sqrt{2}) * (c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$$

$*$ je asociatívna aj komutatívna (nezáleží na tom, na akej množine).

Neutrálny prvok je $1 = 1+0\sqrt{2}$.

Delitele "nuly" – neexistujú. Označme $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$. x a y sú reálne čísla a určite platí, že $xy=0$ len ak $x=0$ alebo $y=0$.

Inverzné prvky majú problém, napr. pre $2 = 2+0\sqrt{2}$ je inverzným $1/2$, čo ale nepatrí do $\mathbb{Z}_v$.

Záver: **Obor integrity** (ale nie teleso)

Príklad 4

Kategorizujme štruktúru $(\mathbb{Z}_n, +, *)$, kde $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ a $+$, $*$ predstavujú sčítanie a násobenie modulo n .

Riešenie:

a) $(\mathbb{Z}_n, +)$

Je to abelovská grupa (už sme riešili) ✓

b) Distributívny zákon pre $+$, $*$ platí a modulo n to nemá ako pokaziť. ✓

c) $(\mathbb{Z}_n, *)$

Operácia $*$ je operáciou na $\mathbb{Z}_n$.

$*$ je asociatívna aj komutatívna (aj s modulom).

Neutrálny prvok je 1.

Delitele "nuly": neexistujú, pokiaľ je n prvočíslo – ale toto vyplynie aj z nasledujúceho bodu.

Inverzné prvky – ak n je prvočíslo, $(\mathbb{Z}_n \setminus \{0\}, *)$ je grupa (už sme riešili) ✓

Záver: **Pole**

Príklad 5

Nech $(G, \circ)$ je cyklická grupa rádu n s generátorom a . Vieme, že jej prvky sú:

$$\{e_0, a, a^2, a^3, a^4, \dots, a^{n-1}\}$$

Definujeme operácie:

$$\begin{aligned} a^i \oplus a^j &= a^{i+j \bmod n} & (\text{je to len estetická formalita, } \oplus \text{ je totožná s } \circ) \\ a^i \otimes a^j &= a^{i*j \bmod n} \end{aligned}$$

Kategorizujeme štruktúru $(G, \oplus, \otimes)$.

Riešenie:

a) $(G, \oplus) = (G, \circ)$ je podľa zadania cyklická grupa. Cyklické grupy sú komutatívne. ✓

b) Distributívny zákon pre $+$, $*$ platí:

$$\begin{aligned} a^i \otimes (a^j \oplus a^k) &= a^i \otimes a^{j+k} = a^{i*(j+k)} \\ a^i \otimes a^j \oplus a^i \otimes a^k &= a^{i*j} \oplus a^{i*k} = a^{i*j+i*k} \end{aligned} \quad \checkmark$$

c) $(G, \otimes)$

Operácia $\otimes$ je operáciou na G , je asociatívna aj komutatívna. (Dôkaz – pozriem a vidím)
Neutrálny prvok e_1 – ak existuje – je niektorý z prvkov a^t , pričom t musíme zistiť.

Má platiť $a^i \otimes a^t = a^{i*t} = a^i$ odkiaľ dostaneme $t=1$, teda $e_1 = a$.

Delitele "nuly": $a^i \otimes a^j = a^{i*j \bmod n} = a^0 = e_0$ – neexistujú, pokiaľ je n prvočíslo.

Inverzné prvky – tvrdíme, že ak n je prvočíslo, pre každé i existuje k také, že $i*k \bmod n = 1$.

Dôkaz: ak $i=1$, potom $k=1$ (triviálne). Ak i je medzi 2 a $n-1$,

zoberme postupne $k=1, 2, 3, \dots, n-1$ a počítajme $i*k$. Môže sa stať toto:

– ak by sme našli dve rôzne k_1, k_2 také, že bude $i*k_1 = i*k_2$, potom pre $k_3 = |k_1 - k_2|$ platí $i*k_3 \bmod n = 0$, čo nie je možné, ak je n prvočíslo.

– ak pre všetky k ($n-1$ rôznych hodnôt od 1 po $n-1$) dostaneme odlišné výsledky, musí byť medzi nimi aj 1. A toto sme chceli!

Takže, pre každé a^i existuje také a^k , že $a^i \otimes a^k = a^1 = e_1$

$(G \setminus \{e_0\}, \otimes)$ je grupa. ✓

Záver: **Pole**

Príklad 6

Typickým a veľmi vd'ačným príkladom z témy okruhov sú polynómy. Ich sčítanie je v princípe to isté, ako sčítanie vektorov, ale pri násobení je to už o niečo zaujímavejšie.

Kategorizujme štruktúru $(\mathbb{R}_p(x), +, *)$, kde $\mathbb{R}_p(x)$ sú polynómy s reálnymi koeficientami (PRK).

Riešenie:

a) $(\mathbb{R}_p(x), +)$.

Súčet PRK je opäť PRK. Takže $+$ je operáciou na danej množine.

Komutatívnosť a asociatívnosť patria prirodzene k $+$.

Neutrálny prvok pre $+$ je nula, stačí tu len s úľavou konštatovať, že aj 0 je polynóm.

Inverzný prvok k polynómu $p(x)$ je $-p(x)$.

Komutatívna grupa. ✓

b) Distributívny zákon je operáciám $+, *$ vlastný. Polynómy sú funkcie a pri práci s funkciami na MAT 1-2 sme distributívnosť bez ostychu využívali.

c) $(\mathbb{R}_p(x), *)$

Súčin PRK je opäť PRK, $*$ je operáciou na tejto množine.

Asociatívnosť aj komutatívnosť je zrejmá, sú vlastné operácii $*$.

Neutrálny prvok pre $*$ je 1, čo je nielen číslo, ale aj polynóm (nultého stupňa).

Delitele nuly – dá sa ľahko overiť, že súčin dvoch nenulových polynómov je opäť nenulový polynóm.

Inverzné prvky: napr. k polynómu $p(x) = x$ by mal byť $p' = 1/x$, čo však už polynóm nie je.

Záver: Obor integrity

Príklad 7

Kategorizujeme štruktúru $(\mathbb{R}_r(x), +, *)$, kde $\mathbb{R}_r(x)$ sú racionálne funkcie s reálnymi koeficientami (RaFReK). Na základe našich skúseností z LA a MAT1-2 vieme povedať, že každá racionálna funkcia je súčtom polynómu a niekoľkých (typovo úzko vymedzených) elementárnych zlomkov.

Riešenie:

a) $(\mathbb{R}_r(x), +)$.

Súčet RaFReK je opäť RaFReK. Takže $+$ je operáciou na danej množine.

Komutatívnosť a asociatívnosť patria prirodzene k $+$.

Neutrálny prvok pre $+$ je nula, stačí len konštatovať, že aj 0 je RaFReK.

Inverzný prvok k rac. funkcii $r(x)$ je $-r(x)$.

Komutatívna grupa. ✓

b) Distributívny zákon je operáciám $+, *$ vlastný. Aj racionálne funkcie sú len funkcie a ďalej to už poznáme...

c) $(\mathbb{R}_p(x), *)$

Súčin RaFReK je opäť RaFReK (z estetických dôvodov okrem súčinu treba vždy spraviť novú úpravu/rozklad výsledku na elementárne zlomky), $*$ je teda operáciou na tejto množine.

Asociatívnosť aj komutatívnosť sú zrejmé.

Neutrálny prvok pre $*$ je 1, čo je nielen číslo, ale aj rac. funkcia.

Delitele nuly nebudeme overovať, lebo ich neexistencia vyplynie z nasledujúceho bodu.

Inverzné prvky: k nenulovej rac. funkcii $r(x)$ je inverzným prvkom $1/r(x)$, čo je zase rac. funkcia, ktorá sa samozrejme s trochou námahy dá a musí upraviť na normatívny tvar.

Záver: Pole

Príklad 8

Kategorizujme štruktúru $(2^X, \Delta, \cap)$, teda všetky podmnožiny univerza X s operáciami "symetrická diferencia" a "prienik".

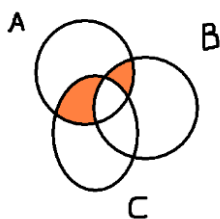
Riešenie:

Pri riešení sa len odvoláme na to, čo už sme v starších cvičeniach zistili.

a) $(2^X, \Delta)$ je komutatívna grupa.

b) distributívny zákon platí, vieme overiť pomocou Vennových diagramov.

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$$



c) $(2^X, \cap)$ je komutatívny monoid.

Záver: $(2^X, \Delta, \cap)$ je komutatívny okruh s jednotkou.

Neriešené príklady

Klasifikujte nasledujúce množiny s dvojicou operácií:

1. $(7\mathbb{Z}, +, *)$, kde $+, *$ sú klasické plus, krát.
2. $(\mathbb{Z}^2, +, *)$
3. $(\mathbb{Q}^2, +, *)$
4. $(C([0,1]), +, *)$ // spojité funkcie na uzavretom intervale $[0,1]$
5. $(\mathbb{Q}_V, +, *)$, kde $\mathbb{Q}_V = \{a+b\sqrt{2}, a,b \in \mathbb{Q}\}$
6. $(\mathbb{R}^+, \oplus, \odot)$, kde $a \oplus b = ab = e^{(\ln a + \ln b)}$, $a \odot b = e^{(\ln a * \ln b)}$
7. $(R, +, *)$, kde R je množina všetkých matic 2×2 a $*$ je maticové násobenie.