

Okruhy 2

Úvod a riešené príklady

a) Homomorfizmy na okruhoch

Homomorfizmus z okruhu do okruhu musí rešpektovať obidve operácie.

Majme zobrazenie $h: (R_1, \oplus_1, \otimes_1) \rightarrow (R_2, \oplus_2, \otimes_2)$. Ak platí:

$$h(x \oplus_1 y) = h(x) \oplus_2 h(y)$$

$$h(x \otimes_1 y) = h(x) \otimes_2 h(y)$$

ide o homomorfizmus. Jeho jadro, teda $\{x \in R_1, h(x) = 0_2\}$, je obojstranný *ideál* (cf. ďalej).

Príklad a1

Je dané zobrazenie $h: (2\mathbb{Z}, +, *) \rightarrow (3\mathbb{Z}, +, *)$, $h(x) = (3/2)*x$.

Zistite, či je h homomorfizmus.

Riešenie:

Poznámka: $(2\mathbb{Z}, +, *)$ aj $(3\mathbb{Z}, +, *)$, sú okruhy bez jednotky (pseudookruhy), lebo číslo 1 (iné sa ku $*$ nehodí) tu nie je prítomné.

$$+: \quad h(x+y) = 3/2*(x+y) = 3/2*x + 3/2*y = h(x)+h(y) \quad \checkmark$$

$$*: \quad \begin{aligned} h(x*y) &= 3/2*(x*y) \\ h(x)*h(y) &= 3/2*x * 3/2*y \quad \neq h(x*y) \end{aligned}$$

Záver: **Nie je** to okruhový homomorfizmus.

Príklad a2

Je dané zobrazenie $h: (C(-1,1), +, *) \rightarrow (\mathbb{R}, +, *)$, $h(f) = f(0)$.

Označenie $C(-1,1)$ predstavuje spojité funkcie na intervale $(-1,1)$.

Zistite, či je h homomorfizmus.

Riešenie:

$$h(f+g) = (f+g)(0) = f(0)+g(0) = h(f)+h(g) \quad \checkmark$$

$$h(f*g) = (f*g)(0) = f(0)*g(0) = h(f)*h(g) \quad \checkmark$$

Záver: **Je** to homomorfizmus. Pri riešení sme využili základné pravidlá o sčítaní a násobení funkcií. Jeho jadro $\{f \in C(-1,1), f(0)=0\}$ je ideál.

Príklad a3

Nech $(G, \circ)$ je cyklická grupa rádu n s generátorom a .

Definujeme operácie:

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

Definujeme zobrazenie $h: (G, \oplus, \otimes) \rightarrow (\mathbb{Z}_n, +, *)$, $h(a^k) = k$. Zistite, či je h homomorfizmus.

Riešenie:

Obidve štruktúry sú polia – bolo to riešené na predošlom cvičení.

$$\begin{aligned}h(a^i \oplus a^j) &= h(a^{i+j \bmod n}) = i+j \bmod n \\h(a^i) + h(a^j) \bmod n &= i+j \bmod n\end{aligned}\quad \checkmark$$

$$\begin{aligned}h(a^i \otimes a^j) &= h(a^{i*j \bmod n}) = i*j \bmod n \\h(a^i) * h(a^j) \bmod n &= i*j \bmod n\end{aligned}\quad \checkmark$$

Podmienky sú splnené, je to homomorfizmus. A nielen to – h je tiež bijekcia, ide teda o izomorfizmus. Obe polia sú z hľadiska svojej štruktúry, teda z pohľadu algebry, rovnaké. Jadro tohto zobrazenia je triviálne (iba neutrálny a^0).

Príklad a4

Je dané zobrazenie $h: (\mathbb{R}, +, *) \rightarrow (\mathbb{R}_+, \oplus, \odot)$, kde $x \oplus y = x * y$ a $x \odot y = \exp(\ln(x) * \ln(y))$, s predpisom

$$h(x) = \exp(x) = e^x. \quad \text{Zistite, či } h \text{ je homomorfizmus.}$$

Riešenie:

$$h(x+y) = \exp(x+y) = \exp(x) * \exp(y) = h(x) \oplus h(y) \quad \checkmark$$

$$\begin{aligned}h(x*y) &= \exp(x*y) \\h(x) \odot h(y) &= \exp(x) \odot \exp(y) = \exp(x*y)\end{aligned}\quad \checkmark$$

Zobrazenie h je bijekcia, ide teda o izomorfizmus. (Opäť teda žiadne zaujímavé jadro)

Príklad a5

Je dané zobrazenie $h: (\mathbb{Z}, +, *) \rightarrow (\mathbb{Z}_n, +, *)$, $h(x) = x \bmod n$. Overte, že h je homomorfizmus a nájdite jeho jadro.

Riešenie:

$$\begin{aligned}h(x+y) &= (x+y) \bmod n = (x \bmod n + y \bmod n) \bmod n = (h(x) + h(y)) \bmod n \\h(x*y) &= (x*y) \bmod n = (x \bmod n * y \bmod n) \bmod n = (h(x) * h(y)) \bmod n\end{aligned}$$

Je to homomorfizmus. Jeho jadrom je množina násobkov čísla n, teda $n\mathbb{Z}$. Je to ideál, čo podrobnejšie overíme nižšie.

Príklad a6

Je daný okruh $(R_x, +, *)$, kde R_x je množina všetkých polynómov s reálnymi koeficientami, a okruh komplexných čísel $(\mathbb{C}, +, *)$.

Zobrazenie $h: (R_x, +, *) \rightarrow (\mathbb{C}, +, *)$ je určené predpisom $h(p(x)) = p(i)$, tj. polynóm zobrazíme do jeho funkčnej hodnoty v imaginárnej jednotke i.

Overte, že h je homomorfizmus a nájdite jeho jadro.

Riešenie:

$$\begin{aligned}h(p+q) &= (p+q)(i) = p(i) + q(i) = h(p) + h(q) \\h(p*q) &= (p*q)(i) = p(i) * q(i) = h(p) * h(q)\end{aligned}$$

Zobrazenie je homomorfizmus. Jeho jadrom sú všetky polynómy, ktoré po dosadení hodnoty i dajú nulu. Keďže ide o polynómy s reálnymi koeficientami, v ich rozklade na súčin elementárnych členov musí byť prítomný (x^2+1) . Jadrom sú teda všetky polynómy deliteľné členom (x^2+1) . Ide o ideál.

b) Ideály

V bežnom živote ideály postupne strácame, tu v algebre ich naopak niekoľko nájdeme. Začnime definíciou:

Nech je daná štruktúra $(R, \oplus, \otimes)$. Ideálom sa nazýva množina I , pre ktorú platí:

1. $(I, \oplus) \subset (R, \oplus)$ – tj. pri aditívnej operácii je I podgrupou R

2a. $\forall a \in I, x \in R : a \otimes x = ax \in I$

2b. $\forall a \in I, x \in R : x \otimes a = xa \in I$

Ak platí len 2a, ide o pravý ideál, ak 2b, ide o ľavý ideál. Pri komutatívnych operáciách samozrejme rozlišovanie pravého a ľavého ideálu nie je potrebné.

Multiplikatívnu operáciu $\otimes$ budeme "nepísať" podobne ako pri bežnom násobení.

Hrubšie povedané, má platiť absorpcia:

2a. $\forall a \in I : aR \in I$, resp. $IR \subseteq I$

2b. $\forall a \in I : Ra \in I$, resp. $RI \subseteq I$

Zmysel podmienok 2a, 2b spočíva v tom, že ideál I má fungovať po faktorizácii ako neutrálny prvok (ľavý, pravý alebo plný).¹

Platí: Prienik, súčet a súčin dvoch ideálov je ideál.

Hlavný ideál je taký ideál, ktorý sa dá generovať jediným svojím prvkom a ,

tj. existuje $a \in I$ také, že $I = Ra$ (ľavý), $I = aR$ (pravý), $I = RaR$ (obojsstranný).

Ideál sa nazýva **prvoideál** (prostý ideál, *prime ideal*), ak pre všetky $a, b \in R$ také, že $a \otimes b \in I$, platí $a \in I$ alebo $b \in I$. (Táto vlastnosť súvisí s deliteľmi nuly).

Ideál I sa nazýva **maximálny**, ak je vlastný (nie je rovný R) a pre každý iný vlastný ideál J platí, že ak $I \subseteq J$, tak $I = J$. (Tj. neexistuje už nič medzi I a R). Okruh môže mať viacero maximálnych ideálov. Maximálny ideál je zároveň prvoideál.

Ideál I sa nazýva **nilpotentný** (= nihil + potens), ak existuje prirodzené k také, že $I^k = \mathbf{0}$, tj. súčin ľubovoľných k prvkov z I sa rovná aditívnemu neutrálnemu prvku ("nule").

Podľa ideálov je možné rozkladať okruhy na triedy.

Faktorizácia okruhu podľa ideálu je opäť okruh.

Faktorizácia okruhu podľa maximálneho ideálu pri komutatívnej $\otimes$ je pole.

Faktorizácia okruhu podľa prvoideálu pri komutatívnej $\otimes$ je obor integrity.

¹ Pozor na poradie – ľavý ideál sa podobá pravému neutrálnemu prvku a pravý ideál ľavému neutr. prvku.

Príklad b1.

Máme okruh $(\mathbb{Z}, +, *)$ a množinu $2\mathbb{Z}$. Zistite, či ide o ideál. Ak áno, urobte rozklad okruhu.

Riešenie:

1. Je zrejmé, že $(2\mathbb{Z}, +) \subset (\mathbb{Z}, +)$ – je to podgrupa.

2. $\forall a=2k \in 2\mathbb{Z}, \forall x \in \mathbb{Z} : ax=2kx \in 2\mathbb{Z}$

Ľudovo povedané, ak párnym číslom vynásobíme akékoľvek celé číslo, výsledkom bude opäť párne číslo (absorpcia). Podobne to funguje pre násobky 3, 4, ...

Ideál $I=2\mathbb{Z}$ je hlavný, ako totiž vidno už z uvedeného zápisu, dá sa generovať číslom 2.

Ideál $I=2\mathbb{Z}$ je prvoideál, lebo ak ab je párne, iste je aspoň jedno z čísel a, b párne.

Ideál $I=2\mathbb{Z}$ je maximálny ideál, nie je totiž už možné nájsť nič medzi $2\mathbb{Z}$ a $\mathbb{Z}$.

Rozklad $(\mathbb{Z}, +, *)$ podľa $I=2\mathbb{Z}$:

- a) Najprv spravíme rozklad $(\mathbb{Z}, +)/(I, +)$ ako pri grupách.
Výsledkom sú triedy $T_0=2\mathbb{Z}, T_1=2\mathbb{Z}+1$. Vieme z dávnejších cvičení, že operácia $+$ sa tu dá aplikovať blokovo na celé triedy.
- b) Získané triedy "preskúšame" s operáciou $*$ (či je to kongruencia):
 $T_0 * T_0 = T_0$ (súčin 2 párných čísel je vždy párne číslo)
 $T_0 * T_1 = T_0$ (súčin párneho a nepárneho čísla je vždy párne číslo)
 $T_1 * T_1 = T_1$ (súčin 2 nepárnych čísel je vždy nepárne číslo)

Aby bol rozklad v poriadku, musia platiť oba body a, b. To, že I je ideál, túto platnosť zaručuje – náš postup v a, b bol len overením, že je to v poriadku.

Rozklad $\{T_0, T_1\}$, ktorý sa dá reprezentovať štruktúrou $(\mathbb{Z}_2, +, *)$, je pole – ako inak, veď sme rozkladali podľa maximálneho ideálu.

Príklad b2.

Máme pole $(\mathbb{Z}_{12}, +, *)$. Nájdime všetky jeho hlavné ideály a rozklady podľa nich.

Riešenie:

Postup sa podobá hľadaniu podgrúp $(\mathbb{Z}_{12}, +)$ a rozkladaniu podľa nich. Pripomenieme si, čo sme už dávnejšie zistili:

Podgrupa $(2\mathbb{Z}_6, +)$ – párne čísla. Platí, že súčin párneho čísla s celým je opäť párne číslo, ide o ideál.

Rozklad $(\mathbb{Z}_{12}, +)/(2\mathbb{Z}_6, +) \rightarrow T_0=2\mathbb{Z}_6, T_1=2\mathbb{Z}_6+1$. Ideál je hlavný, dá sa generovať 2-kou.

Je to prvoideál a maximálny ideál.

Podgrupa $(3\mathbb{Z}_4, +)$ – násobky 3. Platí, že súčin násobku 3 s celým je opäť násobok 3, ide o ideál.

Rozklad $(\mathbb{Z}_{12}, +)/(3\mathbb{Z}_4, +) \rightarrow T_0=3\mathbb{Z}_4, T_1=3\mathbb{Z}_4+1, T_2=3\mathbb{Z}_4+2$.

Ideál je hlavný, dá sa generovať 3-kou. Je zároveň prvoideál a maximálny ideál (stále nie je nič medzi $3\mathbb{Z}_4$ a $\mathbb{Z}_{12}$).

Podgrupa $(4\mathbb{Z}_3, +)$ – násobky 4. ...

Ide o hlavný ideál, ale nie je to prvoideál (napr. číslo 4 zo $4\mathbb{Z}_3$ viem získať ako súčin $2*2$, ale 2 nepatrí do $4\mathbb{Z}_3$), a nie je to ani maximálny ideál – medzi $4\mathbb{Z}_3$ a $\mathbb{Z}_{12}$ leží $2\mathbb{Z}_6$.

Podgrupa $(6\mathbb{Z}_2, +)$ – násobky 6. ... Ide o hlavný ideál, ale nie je to prvoideál a nie je to ani maximálny ideál.

Keďže spomenuté podgrupy sú ideály, rozklady podľa nich sú možné a výsledky faktorizácie budú okruhy.

Príklad b3.

Je daný okruh $(\mathbb{Q}, +, *)$ a jeho podokruh $(\mathbb{Z}, +, *)$. Je tento podokruh ideálom?

Riešenie:

Podmienka a) je splnená, avšak b) nie. Ideál to teda nie je.

Príklad b4.

Je daný okruh $(M_n, +, *)$, kde M_n je množina všetkých matíc $n \times n$ a jeho podokruh $(M_{n0}, +, *)$, kde M_{n0} je množina všetkých matíc $n \times n$ s nulovým posledným riadkom.

Je tento podokruh ideálom?

Riešenie:

Nech N je matica z podokruhu M_{n0} a M je ľubovoľná matica z M_n .

Platí $N * M \in M_{n0}$, ale zároveň $M * N \notin M_{n0}$. Tj. M_{n0} je pravý ideál, ale nie ľavý.

Príklad b5.

Máme pole $(\mathbb{Z}_{64}, +, *)$. Nájdite všetky jeho nilpotentné ideály.

Riešenie:

Vieme, že $(\mathbb{Z}_{64}, +)$ je cyklická grupa, čo znamená, že všetky jej podgrupy budú tiež cyklické (generované jedným prvkom). Z doterajších skúseností vieme, že všetky netriviálne podgrupy budú tieto:

$$[2] = 2\mathbb{Z}_{32}$$

$$[4] = 4\mathbb{Z}_{16}$$

$$[8] = 8\mathbb{Z}_8$$

$$[16] = 16\mathbb{Z}_4$$

$$[32] = 32\mathbb{Z}_2$$

Ľahko overíme, že vo všetkých spomenutých prípadoch sú $((64/r) \mathbb{Z}_r, +, *)$ ideály.

Všetky sú aj nilpotentné. V $2\mathbb{Z}_{32}$ súčin ľubovoľných 32 prvkov $\mid \text{mod } 64$ dá nulu,

v $4\mathbb{Z}_{16}$ súčin ľubovoľných 16 prvkov $\mid \text{mod } 64$ dá nulu, atď.

Neriešené príklady

A

1. Nech $D = [0, 2]$ je reálny interval, $P = \{0, 1, 2\}$ je množina bodov a R je množina spojitých funkcií na D . Definujeme zobrazenie

$$h(f) = f(P) = (f(0), f(1), f(2)).$$

Zistite, či $h: (R, +, *) \rightarrow (\mathbb{R}_3, +, *)$ je homomorfizmus.

(operácie $+$ a $*$ v cieľovej štruktúre fungujú „po zložkách“)

Nájdite jadro tohto homomorfizmu a overte, že je to ideál.

2. Nech $h: (\mathbb{R}^2, +, *) \rightarrow (\mathbb{R}, +, *)$ je definované predpisom $h(x_1, x_2) = x_1$. Operácie $+$, $*$ vo východiskovej štruktúre fungujú „po zložkách“. Je h homomorfizmus?

Nájdite jeho jadro a overte, že je to ideál.

3. Nech $h: (\mathbb{Z}, +, *) \rightarrow (\mathbb{Z}^n, +, *)$ je definované predpisom $h(x) = m * x \mid \text{mod } n$.

Pre aké dvojice m, n je h homomorfizmus? (skúste konkrétne príklady a potom zovšeobecnite).

4. Je daný okruh $(R_x, +, *)$, kde R_x je množina všetkých polynómov s reálnymi koeficientami, a okruh reálnych čísel $(\mathbb{R}, +, *)$.

Zobrazenie $h: (R_x, +, *) \rightarrow (\mathbb{R}, +, *)$ je určené predpisom $h(p(x)) = p(1)$, tj. polynóm zobrazíme do jeho funkčnej hodnoty v jednotke.

Overte, že h je homomorfizmus a nájdite jeho jadro.

B

1. Nech $(C(\mathbb{R}), +, *)$ sú spojité reálne funkcie a $I = \{f \in C(\mathbb{R}); \exists m \in \mathbb{R}^+, \forall x, |x| \geq m: f(x) = 0\}$. Zistite či I je ideál v $C(\mathbb{R})$.

2. Máme okruh $(\mathbb{Z}, +, *)$ a množinu $3\mathbb{Z}$. Zistite, či ide o ideál. Ak áno, urobte rozklad okruhu.

3. Overte (podľa definície ideálu), že jadro homomorfizmu z príkladu a6 je ideál.

4. Je daný okruh $(M_n, +, *)$, kde M_n je množina všetkých matic $n \times n$ a jeho podokruh $(M_{n0}, +, *)$, kde M_{n0} je množina všetkých matic $n \times n$ s nulovým posledným stĺpcom.

Je tento podokruh ideálom?