3.4. Okruhy

Definice 3.4.1:

Okruh je algebraický systém <A;+,.> se dvěma základními binárními operacemi a s následujícími vlastnostmi:

- <A;+> je Abelova grupa, tzv. ***aditivní grupa okruhu***,
- <A;.> je grupoid, tzv. ***multiplikativní grupoid okruhu***,

operace + a . splňují distributivní zákony /násobení vzhledem k sčítání/:

$$a.(b+c)=a.b+a.c, \quad (a+b).c=a.c+b.c$$

/přijímáme konvenci podle které má násobení prioritu před sčítáním/.

Asociativní okruh je okruh s asociativním násobením.

Komutativní okruh je okruh s komutativním násobením.

Okruh s jednotkovým prvkem je asociativní okruh s jednotkovým prvkem vzhledem k násobení.

Příklady 3.4.1:

<I;+,.>, <R;+,.>, <C;+,.> ... okruh celých, reálných a komplexních čísel - asociativní a komutativní okruhy s jednotkovým prvkem

- $<Z_m;+,.>$ ... okruh zbytkových tříd modulo m - asociativní a komutativní okruh s jednotkovým prvkem
- $<R_{nn};+,.>$ ... okruh reálných čtvercových matic n-tého řádu - asociativní okruh s jednotkovým prvkem, nekomutativní

Věta 3.4.1:

Jednotkový prvek aditivní grupy okruhu je nulovým prvkem jeho multiplikativního grupoidu. Tento prvek nazýváme ***nulovým prvkem okruhu*** a označujeme 0.

Důkaz:

$$a.a = a.(a+0) = a.a+a.0 \Rightarrow a.0=0 ,$$
$$a.a = (a+0).a = a.a+0.a \Rightarrow 0.a=0 .$$

Definice 3.4.2:

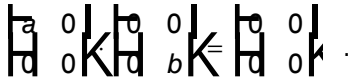
Dělitelé nuly jsou dva nenulové prvky okruhu, jejichž součin je roven nule, tj. prvky a,b pro které platí:

$$a\neq 0 \ \wedge \ b\neq 0 \ \wedge \ a.b=0.$$

Obor integrity je asociativní a komutativní okruh /s aspoň dvěma prvky/ ve kterém neexistují dělitelé nuly.

Příklady 3.4.2:

Okruh čtvercových matic n-tého řádu obsahuje dělitele nuly. Tak např. v $<R_{22};+,.>$ máme



- V okruhu $\langle Z_4;+,.\rangle$ platí **2.2=0** , tj. tento okruh obsahuje dělitele nuly.
- Okruhy $\langle I;+,.\rangle$, $\langle R;+,.\rangle$, $\langle C;+,.\rangle$ jsou obory integrity.

Věta 3.4.2:

Okruh $\langle A;+,.\rangle$ je oborem integrity právě tehdy, když lze v okruhu krátit nenulovým prvkem, tj. když pro $a\neq 0$ platí:

$$a.b=a.c \Rightarrow b=c, \quad b.a=c.a \Rightarrow b=c .$$

Důkaz:

1. Nechť $\langle A;+,.\rangle$ nemá dělitele nuly. Potom pro $a\neq 0$ platí:
   $$a.b=a.c \Rightarrow a.b-a.c=0 \Rightarrow a.(b-c)=0 \Rightarrow b-c=0 \Rightarrow b=c$$
   a tedy lze krátit nenulovým prvkem.
2. Nechť $\langle A;+,.\rangle$ má dělitele nuly, tj. existují prvky $a\neq 0$, $b\neq 0$ takové, že $a.b=0$. Potom krácením platného vztahu $a.b=a.0$ /neboť $a.0=0$/ dostaneme $b=0$, což je spor s předpokladem $b\neq 0$. Krátit tedy nesmíme.

Věta 3.4.3:

Okruh $\langle Z_p;+,.\rangle$ je oborem integrity právě tehdy, když p je prvočíslo.

Důkaz:

Jest $Z_p=\{0,1,2,...,p-1\}$, $\mathbf{m},\mathbf{n}\in Z_p \Leftrightarrow m,n\in\{0,1,2,...p-1\}$.

1. Nechť p je prvočíslo. Tedy neexistují čísla $m,n\in\{0,1,2,...p-1\}$ taková, že $m.n=p$ a tedy ani třídy $\mathbf{m},\mathbf{n}\in Z_p$ takové, $\mathbf{m.n}=\mathbf{0}$. Neexistují tedy dělitelé nuly.
2. Nechť p není prvočíslo. Tedy existují čísla $m,n\in\{0,1,2,...p-1\}$ taková, že $m.n=p$ a tedy také třídy $\mathbf{m},\mathbf{n}\in Z_p$, $\mathbf{m},\mathbf{n}\neq\mathbf{0}$ takové, $\mathbf{m.n}=\mathbf{0}$. Existují tedy dělitelé nuly.

Definice 3.4.3:

Těleso je asociativní okruh, jehož nenulové prvky tvoří grupu vzhledem k násobení.

Pole je komutativní těleso.

Příklady 3.4.3:

: $\langle R;+,.\rangle$, $\langle C;+,.\rangle$ jsou komutativní tělesa, neboli pole.

Následující tabulka definuje konečný okruh $\langle Z_3;+,*\rangle$ /asociativní, komutativní a s jednotkovým prvkem/, který je oborem integrity, tělesem i polem.

+	0	1	2	*	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

Prvek 0 je jednotkou aditivní grupy okruhu, nulou multiplikativního grupoidu okruhu a nulou okruhu. Prvek 1 je jednotkou multiplikativního grupoidu a jednotkou okruhu. Množina nenulových prvků okruhu {1,2} tvoří grupu vzhledem k násobení

- Následující tabulka definuje konečný okruh $\langle Z_4;+,*\rangle$ /asociativní, komutativní a s jednotkovým prvkem/, který není oborem integrity.

+	0	1	2	3	*	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	2	3	0	1	0	1	2	3
2	2	3	0	1	2	0	2	0	2
3	3	0	1	2	3	0	3	2	1

Platí **2*2=0**, prvek **2** je tedy dělitelem nuly.

- $\langle I;+,.\rangle$ není tělesem a tedy ani polem.
- Množina regulárních čtvercových matic je tělesem, ale nikoliv polem.

Věta 3.4.4:

Těleso neobsahuje dělitele nuly.

Důkaz:

Sporem. Nechť existují $a\neq 0$, $b\neq 0$ takové, že $a.b=0$. Potom platí:

$$b=1.b=(a^{-1}.a).b=a^{-1}.(a.b)=a^{-1}.0=0,$$

což je spor s předpokladem $b\neq 0$.

Věta 3.4.5:

Každý konečný obor integrity je těleso a to dokonce komutativní /pole/.

Konečná tělesa se nazyvají ***Galoisovými tělesy***.

Důkaz:

Obtížný.

Příklady 3.4.4:

Okruh $\langle Z_p;+,.\rangle$, kde p je prvočíslo je konečným oborem integrity a tedy i Galoisovým tělesem.

- *Věta*:

$\langle 2^A;\oplus,\cap\rangle$, kde A je libovolná množina, $\oplus$ je operace symetrického rozdílu a $\cap$ operace průniku, je okruh /asociativní, komutativní a s jednotkovým prvkem. Tento okruh není oborem integrity.

Důkaz:

Připomeňme definici symetrického rozdílu:

$$x\oplus y = x\cup y - x\cap y = x\cap y' \cup x'\cap y.$$

Nejprve se přesvědčme, že $\langle 2^A;\oplus\rangle$ je Abelova grupa, tj. že pro operaci $\oplus$ platí axiómy UN,AS,JE,IN,KO. Platnost axiómů AN,KO je evidentní, jednotkovým prvkem je prázdná množina $\emptyset$ a inverzním prvkem k prvku x je prvek x sám /o platnosti axiómů JE a IN se přesvědčíme dosazením těchto prvků do definiční rovnosti symetrického rozdílu/. Platnost axiómu AS ověříme na množinovém obrázku 3.4.1. Systém množin {a,b,c,d,e,f,g} tvoří rozklad množiny $x\cup y\cup z$. Platí:

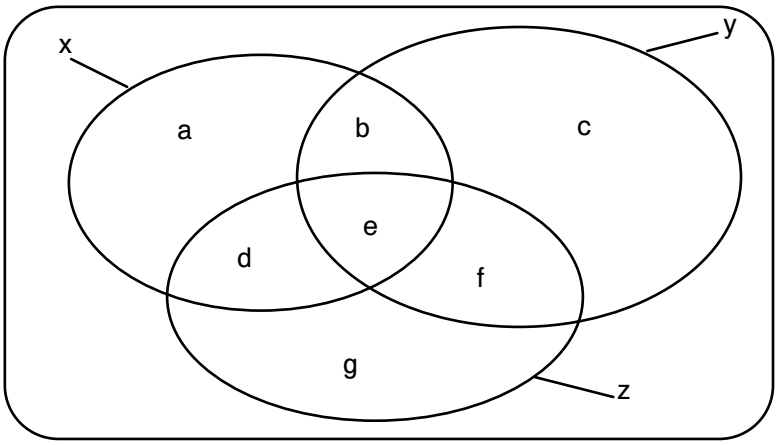
$$x = a\cup b\cup d\cup e,\quad y = b\cup c\cup e\cup f,\quad z = d\cup e\cup f\cup g,$$

$$x\oplus y = a\cup d\cup c\cup f,\quad y\oplus z = b\cup c\cup d\cup g,$$

$$(x\oplus y)\oplus z = a\cup c\cup e\cup g = x\oplus(y\oplus z).$$

Dále se přesvědčíme, že $\langle 2^A;\cap\rangle$ je komutativní, asociativní grupoid s jednotkovým prvkem, tj. že pro operaci $\cap$

platí axiómy UN,AS,KO,JE. Platnost axiómů je evidentní, jednotkovým prvkem je množina A.



Obr. 3.4.1

Zbývá dokázat platnost distributivních zákonů. Vzhledem ke kumutativitě operace průniku stačí dokazat pouze jeden distributivní zákon, např. levý:

$$z \cap (x \oplus y) = (z \cap x) \oplus (z \cap y).$$

Tento axióm můžeme prověřit na množinovém obrázku 3.4.1 stejným způsobem jakým jsme ověřili asociativitu symetrického rozdílu.

Každé dvě disjunktní podmnožiny množiny A jsou děltelé nuly okruhu /prázdná množina je nulovým prvkem okruhu/. Okruh $\langle 2^A; \oplus, \cap \rangle$ tedy není oborem integrity.

- *Věta*:

  Nechť $\oplus$, $\otimes$ jsou binární operace na množině celých čísel I definované takto:

  $x \oplus y = x + y + 1$, $x \otimes y = x.y + x + y$.

  Potom $\langle I; \oplus, \otimes \rangle$ je komutativní a asociativní okruh s jednotkovým prvkem.

  Důkaz:

  Snadno dokážeme, že $\langle I; \oplus \rangle$ je Abelova grupa. Jednotkovým prvkem aditivní grupy /a nulovým prvkem okruhu/ je číslo -1 a inverzním prvkem prvkem k číslu x je číslo -x-2. Stejně jednoduché je i ověření axiómů AN,AS,KO,JE pro operaci $\otimes$. Jednotkovým prvkem multiplikativního grupoidu je číslo 0.

  Zbývá ověření distributivního zákona:

$$z \otimes (x \oplus y) = z \otimes (x+y-1) = z.(x+y-1)+z+(x+y-1) = z.x+z.y+x+y-1 =$$
$$= (z.x+z+y) + (z.y+z+y) -1 = (z.x+z+y) \oplus (z.y+z+y) = (z \otimes x) \oplus (z \otimes y).$$