Okruh

Def. (Okruh): Uspořádanou trojici $(R, +, \cdot)$, kde R je neprázdná množina a $+$ a $\cdot$ jsou zobrazení definovaná na $R \times R$, nazveme okruhem právě tehdy, když

1.) $\forall a, b \in R : \quad a + b \in R$
2.) $\forall a, b, c \in R : \quad a + (b + c) = (a + b) + c$
3.) $\exists 0 \in R \; \forall x \in R : \quad 0 + x = x + 0 = x$
4.) $\forall x \in R \; \exists -x \in R : \quad x + (-x) = (-x) + x = 0$
5.) $\forall a, b \in R : \quad a + b = b + a$

} $(R, +)$ je komutativní grupa

6.) $\forall a, b \in R : \quad a \cdot b \in R$
7.) $\forall a, b, c \in R : \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$

} $(R, \cdot)$ je pologrupa

(nemusí existovat jedničke, ani inverze při násobení, násobení nemusí být komutativní)

8.) $\forall a, b, c \in R : \quad a(b + c) = ab + ac$
9.) $\forall a, b, c \in R : \quad (a + b) \cdot c = ac + bc$

} násobení je distributivní vzhledem ke sčítání

Př: Příkladem okruhu může být:

1.) $(\mathbb{Z}, +, \cdot)$ ... okruh celých čísel
2.) $(\mathbb{Z}_n, +, \cdot)$ ... okruh zbytkových tříd modulo n ($+$ a $\cdot$ je sčítání a násobení „modulo n")
3.) $(\mathbb{R}, +, \cdot)$ ... okruh reálných čísel
4.) $(\mathbb{M}_{m,m}, +, \cdot)$ ... okruh reálných matic typu (m, m) ($+$ a $\cdot$ je jejich obvyklé sčítání a násobení)

Poznámka: Jestliže $(R,+,\cdot)$ je okruh, pak neutrální prvek vzhledem ke sčítání (musí existovat) budeme značit 0 a nazývat nulou v okruhu $(R,+,\cdot)$ a prvek neutrální vzhledem k násobení (nemusí existovat) budeme značit 1 a nazývat jedničkou v okruhu $(R,+,\cdot)$

Dříve jsme ukázali, že v pologrupě, pokud existuje, je jediný neutrální prvek

$(R,+)$ je grupa $\Rightarrow$ 0 existuje a je jediná.

$(R,\cdot)$ je pologrupa $\Rightarrow$ pokud 1 existuje, je jediná

Dále víme, že v monoidu (pologrupa s neutrálním prvkem), pokud existuje, existuje k danému prvku jediný prvek inverzní.
V okruhu $(R,+,\cdot)$ budeme prvek inverzní k prvku $a \in R$ vzhledem ke sčítání značit $-a$ a vzhledem k násobení a^{-1}.

$(R,+)$ je grupa $\Rightarrow$ $\forall a \in R \quad \exists -a$

$(R,\cdot)$ je pologrupa $\Rightarrow$ $\forall a \in R$:
- 1 neexistuje $\Rightarrow$ a^{-1} neexistuje (nemohlo by vyjít $a \cdot a^{-1} = 1$)
- 1 existuje $\Rightarrow$ pokud a^{-1} existuje, pak je jediný

Označení: Jestliže $(R,+,\cdot)$ je okruh, pak $\forall a \in R$ $\forall n \in \mathbb{N}$ budeme značit:

$$\underbrace{a+a+\ldots+a}_{n\text{- krát}} = n \cdot a$$

(toto není násobení v okruhu!)

Základní vlastnosti sčítání a násobení v okruhu popisuje následující věta.

Věta: Nechť $(R,+,\cdot)$ je okruh. Potom pro každé $a,b,c \in R$ platí:

1.) $a \cdot 0 = 0 \cdot a = 0$

2.) $a(-b) = (-a)b = -(a \cdot b)$

3.) $(-a)(-b) = a \cdot b$

4.) $a(b-c) = ab - ac \quad \wedge \quad (a-b)c = ac - bc$

Navíc, jestliže v okruhu $(R,+,\cdot)$ existuje neutrální prvek vzhledem k násobení, budeme jej značit 1 (jednička v okruhu) a platí:

5.) $(-1) \cdot a = -a$

6.) $(-1)(-1) = 1$

Důkaz: 1.) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = 0$ (plní úlohu 0 $\Rightarrow$ je to 0 (je v okruhu jediná))

$0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a \Rightarrow 0 \cdot a = 0$

2.) $a(-b) + a \cdot b = a \cdot (-b+b) = a \cdot 0 = 0 \Rightarrow a(-b) = -(a \cdot b)$ (plní úlohu $-(a \cdot b)$ $\Rightarrow$ je to $-(a \cdot b)$)

$(-a)b + a \cdot b = (-a+a)b = 0 \cdot b = 0 \Rightarrow (-a)b = -(a \cdot b)$

3.) $(-a)(-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$

(= podle 2.) (= podle 2.) (= vyuzedefinice inverzního prvku)

4.) $a(b-c) = ab + a(-c) = ab - ac \quad \wedge \quad (a-b)c = ac + (-b)c = ac - bc$

5.) $(-1)a + a = (-1)a + 1 \cdot a = (-1+1)a = 0 \cdot a = 0 \Rightarrow (-1)a = -a$

6.) $(-1)(-1) \overset{\text{podle 5.}}{=} -(-1) = 1$ □

Def (Podokruh): Nechť $(R, +, \cdot)$ je okruh. Uspořádanou trojici $(H, +', \cdot')$ nazveme podokruhem okruhu $(R, +, \cdot)$ právě když:

1.) $H \subseteq R$

2.) $+'$ je restrikce $+$ na H a $\cdot'$ je restrikce $\cdot$ na H

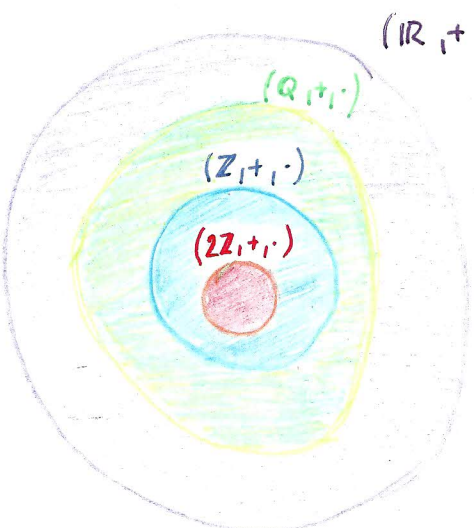
3.) $(H, +', \cdot')$ je okruh

Úmluva: Nebudeme rozlišovat operace na okruhu a jeho podokruhu. Budeme tedy hovořit o podokruhu $(H, +, \cdot)$ okruhu $(R, +, \cdot)$.

Poznámka: „Nejmenším" podokruhem okruhu $(R, +, \cdot)$ je $(\{0\}, +, \cdot)$

„Největším" podokruhem okruhu $(R, +, \cdot)$ je $(R, +, \cdot)$

Př.: Podokruhem okruhu reálných čísel $(\mathbb{R}, +, \cdot)$ je okruh racionálních čísel a jeho podokruhem je okruh celých čísel a jeho podokruhem je okruh sudých celých čísel.



Jak poznáme v okruhu podokruh?

Věta: Nechť $S \subseteq R$, $S \neq \emptyset$. Potom $(S, +, \cdot)$ je podokruh okruhu $(R, +, \cdot)$ právě tehdy, když:

1.) $\forall a, b \in S : a - b \in S$

2.) $\forall a, b \in S : a \cdot b \in S$

Důkaz:

$\Rightarrow$ Pokud je $(S, +, \cdot)$ podokruh, je dle definice okruhem $\Rightarrow$
$(S, +)$ je grupa $\Rightarrow$ $+$ je operace uzavřená na $S \Rightarrow \forall a, b \in S : a, b \in S \Rightarrow a + (-b) \in S$
$(S, \cdot)$ je pologrupa $\Rightarrow$ $\cdot$ je operace uzavřená na S.

$\Leftarrow$ Předpokládejme, že $S \subseteq R$, $S \neq \emptyset$. Cílem je dokázat platnost podmínek 1.) až 9.) z definice okruhu (místo množiny R uvažujeme množinu S)

Podmínky 2.), 5.), 7.), 8.) a 9.) platí, neboť $S \subseteq R$.
Zbývá dokázat 1.), 3.), 4.), 6.) :

I.) 3.) $\exists 0 \in S \; \forall x \in S : 0 + x = x + 0 = 0$

Podle předpokladu je $S \neq \emptyset \Rightarrow \exists a \in S$. Dále předpokládáme, že $\forall a, b \in S : a - b \in S$
$\Rightarrow$ $a - a = 0 \in S$

II.) 6.) $\forall a, b \in S : a \cdot b \in S$

Toto tvrzení je jedním z předpokladů při důkazu tohoto směru ekvivalence.

III.) 4.) $\forall x \in S \; \exists -x \in S : x + (-x) = (-x) + (x) = 0$

Podle předpokladu $\forall a, b \in S : a - b \in S$. Víme již, že $0 \in S \Rightarrow$ zvolme $a = 0$, $b = x \Rightarrow$

$\forall x \in R : \quad 0 - x = -x \in S$

IV.) 1.) $\forall a, b \in S : a + b \in S$

$\forall a, b \in S : \quad a, (-b) \in S \Rightarrow a - (-b) \in S \Rightarrow a + b \in S$

□

Př.: Ověřte, zda $(3\mathbb{Z}, +, \cdot)$ je podokruh okruhu $(\mathbb{Z}, +, \cdot)$.

$3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$ ... množina násobků čísla 3 $\neq \emptyset$ a $3\mathbb{Z} \subseteq \mathbb{Z}$

Ověříme platnost podmínek:

1.) $\forall a, b \in 3\mathbb{Z} : a - b \in 3\mathbb{Z}$

$\forall a, b \in 3\mathbb{Z}$: $a = 3k_1$
$b = 3k_2$, kde $k_1, k_2 \in \mathbb{Z}$ $\Rightarrow$ $a - b = 3k_1 - 3k_2 = 3(k_1 - k_2) = 3k$, $k \in \mathbb{Z}$ $\in 3\mathbb{Z}$

$\Rightarrow$ splněno!

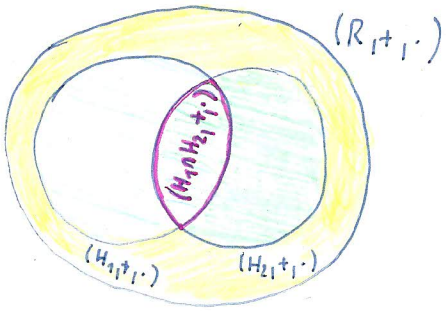
2.) $\forall a, b \in 3\mathbb{Z} : a \cdot b \in 3\mathbb{Z}$

$\forall a, b \in 3\mathbb{Z}$: $a = 3k_1$
$b = 3k_2$, kde $k_1, k_2 \in \mathbb{Z}$ $\Rightarrow$ $a \cdot b = 3(k_1 \cdot 3 \cdot k_2) = 3k$, $k \in \mathbb{Z}$ $\in 3\mathbb{Z}$

$\Rightarrow$ splněno!

$\Rightarrow$ $(3\mathbb{Z}, +, \cdot)$ je podokruh okruhu $(\mathbb{Z}, +, \cdot)$

Věta: Nechť $(H_1, +, \cdot)$ a $(H_2, +, \cdot)$ jsou podokruhy okruhu $(R, +, \cdot)$. Potom $(H_1 \cap H_2, +, \cdot)$ je podokruh okruhu $(R, +, \cdot)$.



Důkaz:

$$\forall a, b \in H_1 \cap H_2 : \begin{cases} a, b \in H_1 \Rightarrow \begin{array}{l} 1.)\ a-b \in H_1 \\ 2.)\ a \cdot b \in H_1 \end{array} \\ a, b \in H_2 \Rightarrow \begin{array}{l} 1.)\ a-b \in H_2 \\ 2.)\ a \cdot b \in H_2 \end{array} \end{cases} \Rightarrow \begin{array}{l} 1.)\ a-b \in H_1 \cap H_2 \\ 2.)\ a \cdot b \in H_1 \cap H_2 \end{array}$$

$\Rightarrow$ $(H_1 \cap H_2, +, \cdot)$ je podokruh okruhu $(R, +, \cdot)$

□