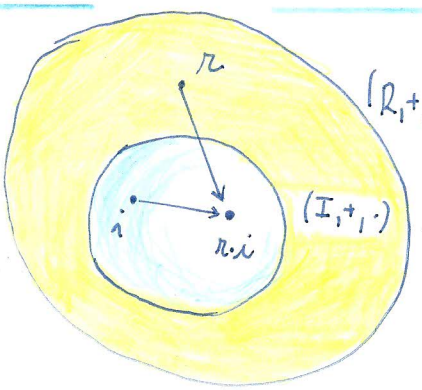
Ideál

Def (Ideál): Nechť $(R,+,\cdot)$ je okruh. Jeho podokruh $(I,+,\cdot)$ nazveme ideálem v okruhu $(R,+,\cdot)$ (oboustranným) právě když

$$\forall r \in R \ \forall i \in I: \quad r \cdot i \in I$$
$$i \cdot r \in I$$

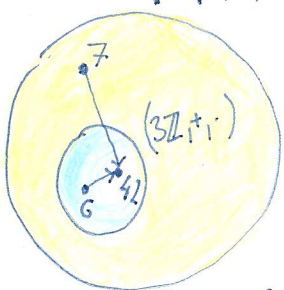


„Ideál funguje jako černá díra. Při násobení vše vtaženo do sebe."

Příklad: 1.) $(3\mathbb{Z},+,\cdot)$, kde $3\mathbb{Z} = \{3.k \mid k \in \mathbb{Z}\}$ je podokruh okruhu $(\mathbb{Z},+,\cdot)$. Navíc je to ideál!

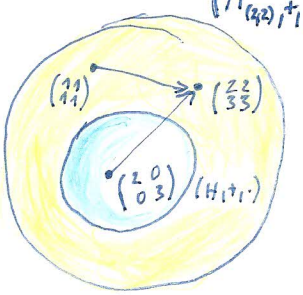
$$\forall r \in \mathbb{Z} \ \forall 3k \in 3\mathbb{Z}: \quad r \cdot 3k = 3 \cdot (r \cdot k) \in 3\mathbb{Z}$$

$(\mathbb{Z},+,\cdot)$



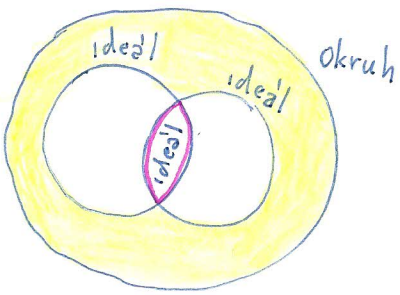
2.) $(H,+,\cdot)$, kde $H = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a,b \in \mathbb{R}\right\}$ je podokruh okruhu $(M_{(2,2)},+,\cdot)$, kde $M_{(2,2)} = \left\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mid a_{ij} \in \mathbb{R}\right\}$, ale není to ideál!

$(M_{(2,2)},+,\cdot)$



$$\underset{\in H}{\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}} \underset{\in M_{(2,2)}}{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}} = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \notin H$$

Věta: Nechť $(I_1, +, \cdot)$ a $(I_2, +, \cdot)$ jsou ideály v okruhu $(R, +, \cdot)$. Potom $(I_1 \cap I_2, +, \cdot)$ je ideál v okruhu $(R, +, \cdot)$.



Důkaz: Průnik dvou podokruhů je podokruh. Proto $(I_1 \cap I_2, +, \cdot)$ je podokruhem okruhu $(R, +, \cdot)$. Navíc

$$\forall r \in R \ \forall i \in I_1 \cap I_2 : \left.\begin{array}{l} i \in I_1 \Rightarrow r \cdot i \in I_1 \ \wedge \ i \cdot r \in I_1 \\ i \in I_2 \Rightarrow r \cdot i \in I_2 \ \wedge \ i \cdot r \in I_2 \end{array}\right\} \Rightarrow \begin{array}{l} r \cdot i \in I_1 \cap I_2 \\ i \cdot r \in I_1 \cap I_2 \end{array}$$

$\Rightarrow (I_1 \cap I_2, +, \cdot)$ je ideál v $(R, +, \cdot)$. □

Věta: Nechť $(R, +, \cdot)$ je okruh. $(I, +, \cdot)$, kde $I \subseteq R$, $I \neq \emptyset$ je idealem v okruhu $(R, +, \cdot)$ právě tehdy, když

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

2.) $\forall r \in R \ \forall i \in I : \ r \cdot i \in I \ \wedge \ i \cdot r \in I$

Důkaz: ⇒

$$(I, +, \cdot) \text{ je ideál} \Rightarrow \begin{array}{ll} \text{je to podokruh} & \Rightarrow 1.) \ \forall a, b \in I : \ a - b \in I \\ \text{je ideál} & \Rightarrow 2.) \ \forall r \in R \ \forall i \in I : \ r \cdot i \in I \ \wedge \ i \cdot r \in I \end{array}$$

⇐

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

2.) $\forall r \in R \ \forall i \in I : \ r \cdot i \in I \ \wedge \ i \cdot r \in I$

$\Rightarrow$ 1.) $\forall a, b \in I : \ a - b \in I$, 2.) $\forall r, i \in I : \ r \cdot i \in I$ $\Rightarrow (I, +, \cdot)$ je podokruh splňující

$\Rightarrow (I, +, \cdot)$ je ideál

□

Faktorový okruh

Věta: Nechť I je oboustranný ideál v okruhu $(R,+,\cdot)$.
Potom $(I,+)$ je normální podgrupa grupy $(R,+)$.

Důkaz: 1.) $(I,+,\cdot)$ je podokruh okruhu $(R,+,\cdot) \Rightarrow (I,+)$ je podgrupa $(R,+)$
2.) $(R,+)$ je komutativní grupa $\Rightarrow$

$$\forall x \in R: \quad x+I = \{x+i \mid i \in I\} = \{i+x \mid i \in I\} = I+x$$

$\Rightarrow (I,+)$ je normální podgrupa grupy $(R,+)$.

Věta: Nechť I je oboustranný ideál v okruhu $(R,+,\cdot)$.
Definujme množinu $R/I = \{x+I \mid x \in R\}$ a operace $\oplus$ a $\odot$ na R/I:

$$\forall x,y \in R: \quad (x+I) \oplus (y+I) = (x+y)+I$$

$$(x+I) \odot (y+I) = (x \cdot y)+I$$

Potom $(R/I, \oplus, \odot)$ je okruh.

Poznámka: Okruh $(R/I, \oplus, \odot)$ budeme nazývat faktorovým okruhem okruhu $(R,+,\cdot)$ podle ideálu I. Nebudeme rozlišovat značení operací na R/I od značení operací na R. Tj. budeme hovořit o faktorovém okruhu $(R/I,+,\cdot)$ okruhu $(R,+,\cdot)$.

Důkaz: 1.) Víme, že $(I,+)$ je normální podgrupa komutativní grupy $(R,+)$. Proto

$(R/I,+)$ je komutativní grupa

(je to faktorová grupa grupy $(R,+)$ podle normální podgrupy $(I,+)$.)

2.) Musíme ověřit korektnost definice operace $\odot$

Předpokládejme $x_1+I = x_2+I$ a $y_1+I = y_2+I$

$x_1+I = x_2+I \Rightarrow (-x_2+x_1)+I = I \Rightarrow -x_2+x_1 \in I \Rightarrow \exists i\in I: x_1 = x_2+i$

$y_1+I = y_2+I \Rightarrow \ldots \Rightarrow \exists j\in I: y_1 = y_2+j$

$$\Rightarrow (x_1+I)\odot(y_1+I) = (x_1\cdot y_1)+I = (x_2+i)(y_2+j)+I =$$

$$= (x_2y_2 + \underbrace{iy_2}_{\in I} + \underbrace{jx_2}_{\in I} + \underbrace{ij}_{\in I}) + I = (x_2y_2 + \underbrace{i^*}_{\in I})I =$$

protože I je ideál $\in I$ protože $(I,+)$ je grupa

$$= (x_2y_2)+I) \oplus (\underbrace{i^*+I}_{=I=0+I}) = x_2y_2+I =$$

$$= (x_2+I)\odot(y_2+I)$$

3.) $\odot$ je asociativní: $\forall a,b,c\in R$:

$$(a+I)\odot[(b+I)\odot(c+I)] = (a+I)\odot[(b\cdot c)+I] = a\cdot(b\cdot c)+I = (a\cdot b)\cdot c+I =$$
$$= (a\cdot b+I)\odot(c+I) = [(a+I)\odot(b+I)]\odot(c+I)$$

4.) $\forall a,b,c\in R$:

$$(a+I)\odot[(b+I)\oplus(c+I)] = (a+I)\odot(b+c)+I = a(b+c)+I = (ab+ac)+I =$$
$$= (ab+I)\oplus(ac+I) = (a+I)\odot(b+I) \oplus (a+I)(c+I)$$

$$[(a+I)\oplus(b+I)]\odot(c+I) = \ldots \text{analogicky} = (a+I)\odot(c+I) \oplus (b+I)\odot(c+I) \quad \square$$

Příklad: $(\mathbb{Z}, +, \cdot)$, kde $\mathbb{Z}$ je množina celých čísel a $+a\cdot$ je jejich obvyklé sčítání a násobení je okruh. $(3\mathbb{Z}, +, \cdot)$ je ideál v okruhu $(\mathbb{Z}, +, \cdot)$. A tak platí:

$$\mathbb{Z}/3\mathbb{Z} = \{ x + 3\mathbb{Z} \mid x \in \mathbb{Z} \}$$

viz dříve:

... rozklad grupy $(\mathbb{Z}, +)$ podle $(3\mathbb{Z}, +)$ $= \mathbb{Z}_3$

obsahuje zbytkové třídy modulo 3: $a + 3\mathbb{Z} = \bar{a}_3$

Jestliže na $\mathbb{Z}$ definujeme sčítání $\oplus$ předpisem:

$$(a + 3\mathbb{Z}) \oplus (b + 3\mathbb{Z}) = (a+b) + 3\mathbb{Z}$$

(jinak zapsáno: $\bar{a}_3 \oplus \bar{b}_3 = \overline{a+b}_3$). Jestliže navíc definujeme násobení $\odot$:

$$(a + 3\mathbb{Z}) \odot (b + 3\mathbb{Z}) = (a \cdot b) + 3\mathbb{Z}$$

(jinak zapsáno: $\bar{a}_3 \odot \bar{b}_3 = \overline{a \cdot b}_3$). Potom víme, že

$(\mathbb{Z}_3, \oplus, \odot)$ je okruh

to jest, víme, že $(\mathbb{Z}_3, \oplus)$ je komutativní grupa a $(\mathbb{Z}_3, \odot)$ je pologrupa.

$\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$ ... množina zbytkových tříd modulo 3 $= \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\} = \{\bar{0}_3, \bar{1}_3, \bar{2}_3\}$

$\oplus$ ..... je obvyklé sčítání modulo 3

$\odot$ ..... je obvyklé násobení modulo 3

Obor integrity a těleso

Def (Obor integrity): Okruh $(R,+,\cdot)$ nazveme oborem integrity právě když:

1.) $\exists 1 \in R \ \forall x \in R: \ 1 \cdot x = x \cdot 1 = x$

2.) $1 \neq 0$

3.) $\forall a,b \in R: \ a \cdot b = b \cdot a$

4.) $\forall a,b \in R: \ a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$

Poznámka:

I.) Oborem integrity tedy nazýváme nebiviální (2.) komutativní (3.) okruh s jedničkou (1.) bez dělitelů nuly (4.).

II.) Jestliže $(R,+,\cdot)$ je obor integrity, pak $(R,\cdot)$ je komutativní monoid.

Příklad:

$(\mathbb{Z},+,\cdot)$ je obor integrity, ale

okruh $(\mathbb{Z}_6,+,\cdot)$ není obor integrity:

Je splněno vše, kromě podmínky 4.):

$\bar{2} \cdot \bar{3} = \bar{0}$, ale $\bar{2} \neq \bar{0} \wedge \bar{3} \neq \bar{0}$

Def (Těleso): Okruh $(R, +, \cdot)$ nazveme tělesem právě tehdy, když:

1.) $\exists 1 \in R \quad \forall x \in R: \quad 1 \cdot x = x \cdot 1 = x$

2.) $1 \neq 0$

3.) $\forall a, b \in R: \quad a \cdot b = b \cdot a$

4.) $\forall x \in R - \{0\} \quad \exists \hat{x} \in R \quad : \quad x \cdot \hat{x}^1 = \hat{x}^1 \cdot x = 1$

Poznámka: I.) Tělesem tedy nazýváme netriviální komutativní okruh s jedničkou v němž má každý nenulový prvek prvek inverzní.

II.) Jestliže $(F, +, \cdot)$ je těleso, pak $(F - \{0\}, \cdot)$ je komutativní grupa.
($\hat{x}^1 \neq 0$, jinak by: $x \cdot \hat{x}^1 = 1 \quad \wedge \quad x \cdot \hat{x}^1 = x \cdot 0 = 0 \Rightarrow 1 = 0$ spor!)

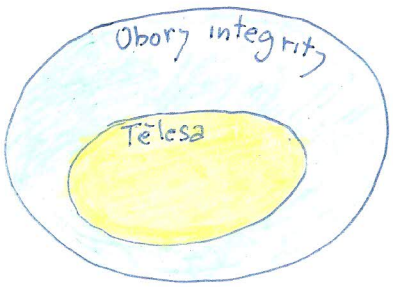
III.) Definice oboru integrity a tělesa se liší pouze v bodu 4.).

Příklad:

$(\mathbb{Q}, +, \cdot)$ je těleso

$(\mathbb{Z}, +, \cdot)$ je obor integrity, ale není to těleso.

Věta: Jestliže $(F,+,\cdot)$ je těleso, pak $(F,+,\cdot)$ je obor integrity.



Důkaz: Definice tělesa a oboru integrity se liší pouze v bodu 4.) :

Těleso: 4.) $\forall x \in F-\{0\} \; \exists \bar{x}^{-1} \in F \; : \; x \cdot \bar{x}^{-1} = \bar{x}^{-1} \cdot x = 1$ (*)

Obor int.: 4.) $\forall a,b \in F \; : \; a \cdot b = 0 \Rightarrow (a=0 \vee b=0)$ (**)

Musíme proto dokázat, že z (*) plyne (**). Předpokládejme proto, že platí (*). Jestliže:

$$a \cdot b = 0 .$$

I.) kde $b \in F-\{0\}$, pak existuje $\bar{b}^{-1}$. Proto

$$a \cdot \underbrace{b \cdot \bar{b}^{-1}}_{=1} = \underbrace{0 \cdot \bar{b}^{-1}}_{=0}$$

Každé těleso je okruhem, proto $0 \cdot \bar{b}^{-1} = 0$. A tak

$$a = 0$$

II.) kde $b = 0$

pak I.) a II.) plyne, že v případě $a \cdot b = 0$ je buď $a=0$, nebo $b=0$.

□