- $(R, \oplus, \odot)$ je komutativní okruh
jestliže $(R, \oplus)$ je kom. grupa
[$\oplus$ komutativní, asociativní, ex. neutrální a opačné prvky]
a dále $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ dist.
a navíc ex. neutrální prvek vzhledem k násobení $\odot$
- kom. okruh je obor integrity
jestliže $a \odot b = 0 \Rightarrow a = 0 \vee b = 0$

neutrální prvek vzhledem k $\oplus$

[$\mathbb{Z}_4$ není obor integrity neboť $2 \cdot 2 = 4 \equiv 0 \mod 4$]
- těleso: navíc každý prvek (s výjimkou neutrálního prvku vzhledem k $\oplus$) má inverzi

vzhledem k násobení.

9.1 $(R, \oplus, \odot)$

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

$a \odot b = -3$

$(R, \oplus)$ komutativní grupa?

- kom, asoc.
- neutrální prvek vzhledem k $\oplus$ je -3
- opačný prvek k a je b:

$a \oplus b = -3$

$a + b + 3 = -3 \Rightarrow \boxed{b = -a - 6}$

Distr: $a \odot (b \oplus c) = -3$ ok

$(a \odot b) \oplus (a \odot c) = -3 \oplus -3 = -3$

Neutr. vzhledem k násobení:

Uvažme b t. ž. $\forall a \in R$ platí

$a \odot b = a$ $\Rightarrow$ neutr. neex.

$\Rightarrow$ není okruh

(ii) $R = \mathbb{Z}$, $a \oplus b = a + b - 3$

$a \odot b = a \cdot b - 1$

$(R, \oplus)$ komutativní okruh

Distr: $a \odot (b \oplus c) = a \odot (b + c - 3) = a(b + c - 3) - 1$

$(a \odot b) \oplus (a \odot c) =$

$= (ab - 1) \oplus (ac - 1) =$

$= ab - 1 + ac - 1 - 3$

nerovnají se

Není okruh.

(iii) $R = \mathbb{Z}$, $a \oplus b = a + b - 1$

$a \odot b = a + b - ab$

Pozn 1 neutr. prvek

$(R, \oplus)$ je kom. grupa

Distr.: $a \odot (b \oplus c) = a \odot (b+c-1) =$

$= a + (b+c-1) - a(b+c-1)$

$(a \odot b) \oplus (a \odot c) = (a+b-ab) \oplus (a+c-ac)$

$= (a+b-ab) + (a+c-ac) - 1$

$\Rightarrow$ je distributivní

Násobení $\odot$: $a \odot b = a+b-ab$

$\Rightarrow$ neutr. prvek vzhledem k $\odot$ je 0

asociativita násobení

$(a \odot b) \odot c = (a+b-ab) \odot c =$

$= (a+b-ab) + c - c(a+b-ab)$

$= a+b+c-ab-ac-bc+abc$

$a \odot (b \odot c) = \ldots$ ↗ totéž

komutativní okruh

- **je těleso?**

$a \in R$, b jeho inverse

$$a \circ b = 0$$

$$a + b - ab = 0$$

$$b(1-a) = -a$$

$$b = \frac{-a}{1-a}, \quad a \neq 1$$

$$\nexists$$

Z obecně

není těleso

Obor integrity? ANO

$$a \circ b = 1$$

$$a + (b - ab) = 1$$

$$b(1-a) = 1-a$$

$$(b-1)(1-a) = 0 \Rightarrow a = 1 \vee b = 1$$

(iv) $R = \mathbb{Q}$, $a \oplus b = a + b$

$a \odot b = b$

↳ není kom.

není komutativní okruh

(v) $R = \mathbb{Q}$, $a \oplus b = a + b + 1$

$a \odot b = a + b + ab$

$(R, \oplus)$ je komutativní grupa

neutrální prvek vzhledem k $\oplus$ je -1

<u>Distr.</u>: • $a \odot (b \oplus c) = a \odot (b + c + 1)$

$= \underline{\underline{a}} + (\underline{b} + \underline{c} + 1) + a(\underline{b} + \underline{c} + \underline{\underline{1}})$

• $(a \odot b) \oplus (a \odot c) = (a + b + ab) \oplus (a + c + ac)$

$= (\underline{\underline{a}} + \underline{b} + \underline{ab}) + (\underline{\underline{a}} + \underline{c} + \underline{ac}) + 1$ <u>OK</u>

Násobení $\odot$: komutativní

$$a\odot(b\odot c) = a\odot(b+c+bc)$$
$$= a + (b+c+bc) + a(b+c+bc)$$

$$(a\odot b)\odot c = (a+b+ab)\odot c$$
$$= (a+b+ab) + c + c(a+b+ab)$$

$\Rightarrow$ je asociativní

- neutrální prvek je 0
- inverzní prvky:

a zadané, chceme b t. ž.

$$a\odot b = 0$$
$$a+b+ab = 0$$
$$b(1+a) = -a$$
$$b = \frac{-a}{1+a} \in \mathbb{Q}$$

těleso

$$\forall a \neq -1$$

DÚ 9.2:

$$\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

$r_1, r_2 \in \mathbb{Z}[i]$

- $\left.\begin{array}{l} r_1 + r_2 \in \mathbb{Z}[i] \\ r_1 \cdot r_2 \in \mathbb{Z}[i] \end{array}\right\}$ zřejmé
- $\left.\begin{array}{l} 0 = 0 + 0 \cdot i \\ 1 = 1 + 0 \cdot i \end{array}\right\} \in \mathbb{Z}[i]$
- $(\underbrace{\mathbb{Z}[i], +}_{\text{kom. grupa}}, \cdot)$ $\to$ kom., asoc., distr.

- je to komutativní okruh
- není těleso

- Je obor integrity neboť

$$\underbrace{(a_1+b_1 i)}_{\in \mathbb{Z}[i]}\underbrace{(a_2+b_2 i)}_{\in \mathbb{Z}[i]} = 0$$

$$\Rightarrow a_1+b_1\cdot i = 0 \vee a_2+b_2 i = 0$$

$\Rightarrow$ obor integrity

Které prvky v $\mathbb{Z}[i]$ mají inverzi?

$$\frac{1}{a+bi} = \frac{a-bi}{\sqrt{a^2+b^2}} = \underbrace{\overbrace{\frac{a}{\sqrt{a^2+b^2}}}^{x}}_{\in \mathbb{Z}} - \underbrace{\overbrace{\frac{b}{\sqrt{a^2+b^2}}}^{y}}_{\in \mathbb{Z}} i$$

$\cap\, \mathbb{Z}[i]$

$$x^2+y^2=1$$

$$\Rightarrow (x,y) \in \{(\pm 1,0),(0,\pm 1)\}$$

$\Rightarrow$ inverzi mají prvky

± 1 a $\pm i$

$$\underline{9.3}: \quad A := \underbrace{\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}}_{\text{T: podokruh}} \subseteq \underbrace{Mat_{2,2}(\mathbb{R})}_{\text{je okruh}}$$

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & -(b_1+b_2) \\ b_1+b_2 & a_1+a_2 \end{pmatrix}$$

$$A \ni$$

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 & -a_1 b_2 - a_2 b_1 \\ a_1 b_2 + a_2 b_1 & a_1 a_2 - b_1 b_2 \end{pmatrix}$$

$$\begin{array}{ccc} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \begin{array}{c} \longmapsto \\ \longleftarrow\!\!\mid \end{array} & a + ib \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ A & & \mathbb{C} \end{array}$$

$$\underset{T}{\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix}} \underset{T}{\begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix}} = \underset{T}{\begin{pmatrix} a_1 a_2 - b_1 b_2 & -(a_1 b_2 + a_2 b_1) \\ a_1 b_2 + a_2 b_1 & a_1 a_2 - b_1 b_2 \end{pmatrix}}$$

$(a_1+ib_1)\cdot(a_2+ib_2) = (a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i$

<u>9.4</u>: Nechť $\varphi: \mathbb{R}\to\mathbb{R}$ je automorfismus tělesa $(\mathbb{R},+,\cdot)$. Ukažte, že $\varphi = id$.

- $\varphi(0)=0, \quad \varphi(1)=1$
- $\varphi(n) = \varphi(\underbrace{1+1+\ldots+1}_{n}) = \underbrace{\varphi(1)+\ldots+\varphi(1)}_{n} = \underbrace{1+\ldots+1}_{n} = n \qquad (n\in\mathbb{N})$
- $\varphi(-n) = \varphi(-1\cdot n) = \varphi(-1)\cdot\varphi(n) = -n \qquad (n\in\mathbb{N})$

$1+(-1)=0 \quad /\ \varphi$

$\varphi(1)+\varphi(-1)=\varphi(0) \Rightarrow 1+\varphi(-1)=0 \Rightarrow \varphi(-1)=-1$

- $p \in \mathbb{Z},\ q \in \mathbb{Z} \setminus \{0\}$

$$p = \varphi(p) = \varphi\left(q \cdot \frac{p}{q}\right) = \varphi(q) \cdot \varphi\left(\frac{p}{q}\right) = \underbrace{q \cdot \varphi\left(\frac{p}{q}\right) = p}$$

$$\varphi\left(\frac{p}{q}\right) = \frac{p}{q}$$

$$\Rightarrow \varphi\big|_{\mathbb{Q}} = id\big|_{\mathbb{Q}}$$

- $x \geq 0 \Rightarrow \varphi((\sqrt{x})^2) = \varphi(x)$

$$\varphi((\sqrt{x})^2) = \varphi(\sqrt{x})^2 \Rightarrow \varphi(x) \geq 0$$

- $0 < x < y \quad \Rightarrow 0 < \varphi(x) < \varphi(y)$

$$\underbrace{y}_{\geq 0} = \underbrace{x}_{\geq 0} + \underbrace{(y-x)}_{\geq 0} \quad \Big|\ \varphi$$

$$\varphi(y) = \varphi(x) + \underbrace{\varphi(y-x)}_{\geq 0}$$

- Spunem prin RAP, fie $x \neq \varphi(x)$

pro nějaké $x \in \mathbb{R}$

$\rightsquigarrow x \in \mathbb{R}_+$

Pak $0 < x < \varphi(x)$ nebo $0 < \varphi(x) < x$

$\rightsquigarrow$ existuje $r \in \mathbb{Q}$ t.ž.

$0 < x < r < \varphi(x)$ $/ \varphi$

$0 < \varphi(x) < \varphi(r) = r$

} SPOR

$\square$