def.: GRUPA je čtveřice $(G, *, ', e)$ kde G je množina (tzv. nosná množina)

$*: G^2 \to G$, $': G \to G$ zobrazení ("násobení", inverz)

$e \in G$ (jednotka)

splňující axiomy:

$$\left.\begin{aligned} a*(b*c) &= (a*b)*c \\ a*e &= e*a = a \\ a*a' &= a'*a = e \end{aligned}\right\} \forall a,b,c \in G$$

Grupa se nazývá abelovská pokud $a*b = b*a \quad \forall a,b \in G$.

def.: OKRUH je šestice $(R, +, -, \cdot, 0, 1)$ kde R je množina

$+, \cdot : R^2 \to R$, $-: R \to R$

$0, 1 \in R$

splňující axiomy:

$(R, +, -, 0)$ je abelovská grupa

$$\left.\begin{aligned} a\cdot(b\cdot c) &= (a\cdot b)\cdot c \\ a\cdot 1 &= 1\cdot a = a \\ a\cdot(b+c) &= a\cdot b + a\cdot c, \quad (b+c)\cdot a = b\cdot a + c\cdot a \end{aligned}\right\} \forall a,b,c \in R$$

Okruh se nazývá komutativní pokud $a\cdot b = b\cdot a \quad \forall a,b \in R$.

Buď R komutativní okruh.

def: Buď $a \in R$. Pokud $\exists b \in R$ t.ž. $a \cdot b = 1$, říkáme, že a je invertibilní a značíme $a^{-1} = b$.

R nazveme OBOR pokud $\forall a, b \neq 0 \quad a \cdot b \neq 0$

R nazveme TĚLESO pokud $\forall a \neq 0$ je invertibilní

👁 a, b invertibilní $\Rightarrow$ $a \cdot b$ invertibilní, a^{-1} invertibilní

$\rightsquigarrow \quad R^* := (\{a \in R : a \text{ inv.}\}, \cdot, ^{-1}, 1)$ je grupa, tzv. multiplikativní grupa okruhu R

Created by Notein

Spousta tvrzení:

1. $*$ asociativní $\Rightarrow$ výrazy $a_1 * \ldots * a_n$ nezávisí na uzávorkování

2. $(G, *, ', e)$ grupa, $a, b, c \in G \Rightarrow$

   (a) $a * c = b * c \Rightarrow a = b$

   (b) $a * u = u * a = e \Rightarrow u = a'$

   (c) $a'' = a$

   (d) $(a * b)' = b' * a'$

Pozn.: $(R, +, -, \cdot, 0, 1)$ okruh $\Rightarrow$ lze vztáhnout na aditivní grupu $(R, +, -, 0)$ i na mult. gp. $(R^*, \cdot, ^{-1}, 1)$

3. $(R, +, -, \cdot, 0, 1)$ komut. okruh, $a, b, c \in R \Rightarrow$

   (a) $a \cdot 0 = 0$

   (b) $-(a \cdot b) = a \cdot (-b) = (-a) \cdot b$, $(-a) \cdot (-b) = a \cdot b$

   (c) pro obory rovnic platí $a \cdot c = b \cdot c$, $c \neq 0 \Rightarrow a = b$

4. Každé těleso je oborem.

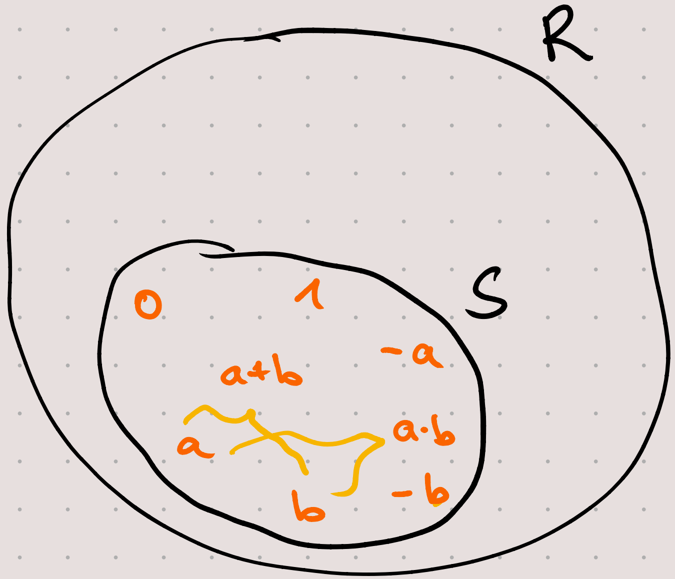
5. Každý konečný obor je tělesem.

Buď $(R,+,-,\cdot,0,1)$ okruh.

Buď $S \subseteq R$ podmnožina t.ž. $0,1 \in S$

$$\left.\begin{array}{l} 0,1 \in S \\ a,b \in S \Rightarrow a+b \in S \\ \qquad\qquad\;\; a\cdot b \in S \\ \qquad\qquad\;\; -a \in S \end{array}\right\} \text{S je \underline{uzavřená} na operace } +,-,\cdot$$

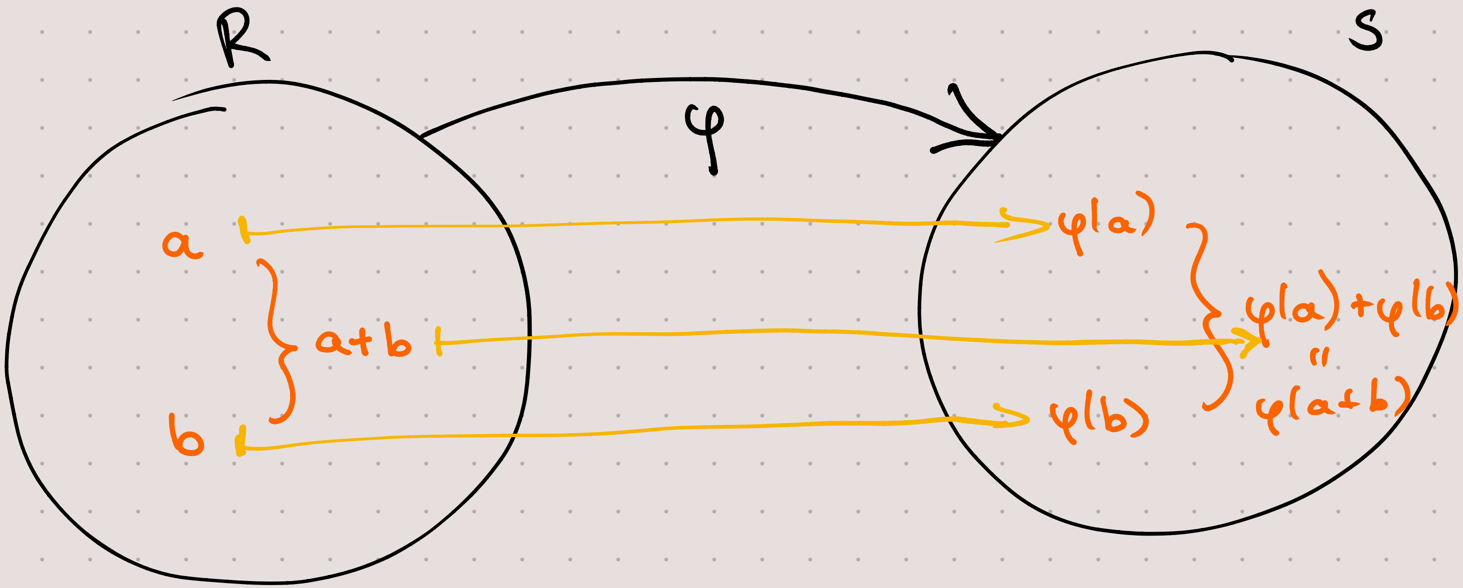
Pak $(S, \underbrace{+\restriction_S, -\restriction_S, \cdot\restriction_S}_{\text{restrikce operací z } R \text{ na } S}, 0, 1)$ nazýváme **PODOKRUH** okruhu R.



Buď R, S okruhy. Bijektivní zobrazení $\varphi: R \to S$ nazveme **IZOMORFISMEM** pokud $\forall a, b \in R$

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

(pak taky $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(-a) = -\varphi(a)$, $\varphi(a^{-1}) = \varphi(a)^{-1}$ pokud $\exists$)



Created by Notein