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

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

Spousta tvrzení:

① $*$ asociativní $\Rightarrow$ výrazy $a_1 * \dots * a_n$ 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 navíc platí $a \cdot c = b \cdot c$, $c \neq 0 \Rightarrow a = b$

④ Každé těleso je oborem.

⑤ Každý konečný obor je tělesem.

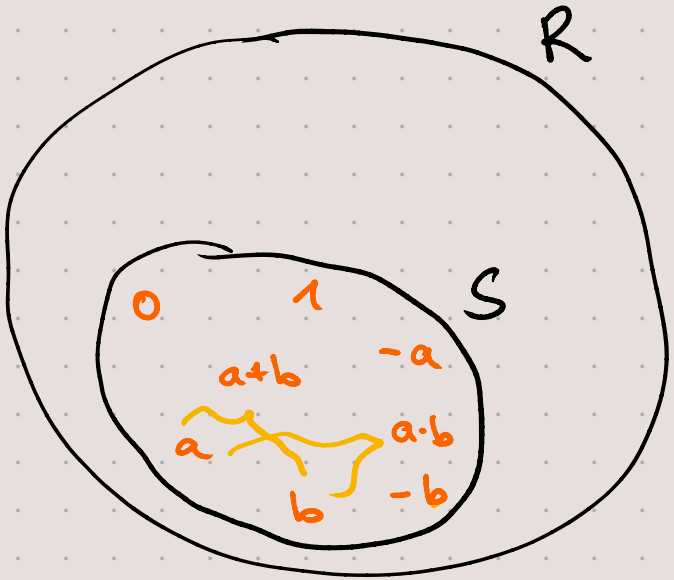
Buď $(R, +, -, \cdot, 0, 1)$ okruh.

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

$a, b \in S \Rightarrow a+b \in S$, $a \cdot b \in S$, $-a \in S$ } S je uzavřená na operace $+, -, \cdot$

Pak $(S, +\restriction_S, -\restriction_S, \cdot\restriction_S, 0, 1)$ nazýváme PODOKRUH okruhu R.

restrikce operací z R na S

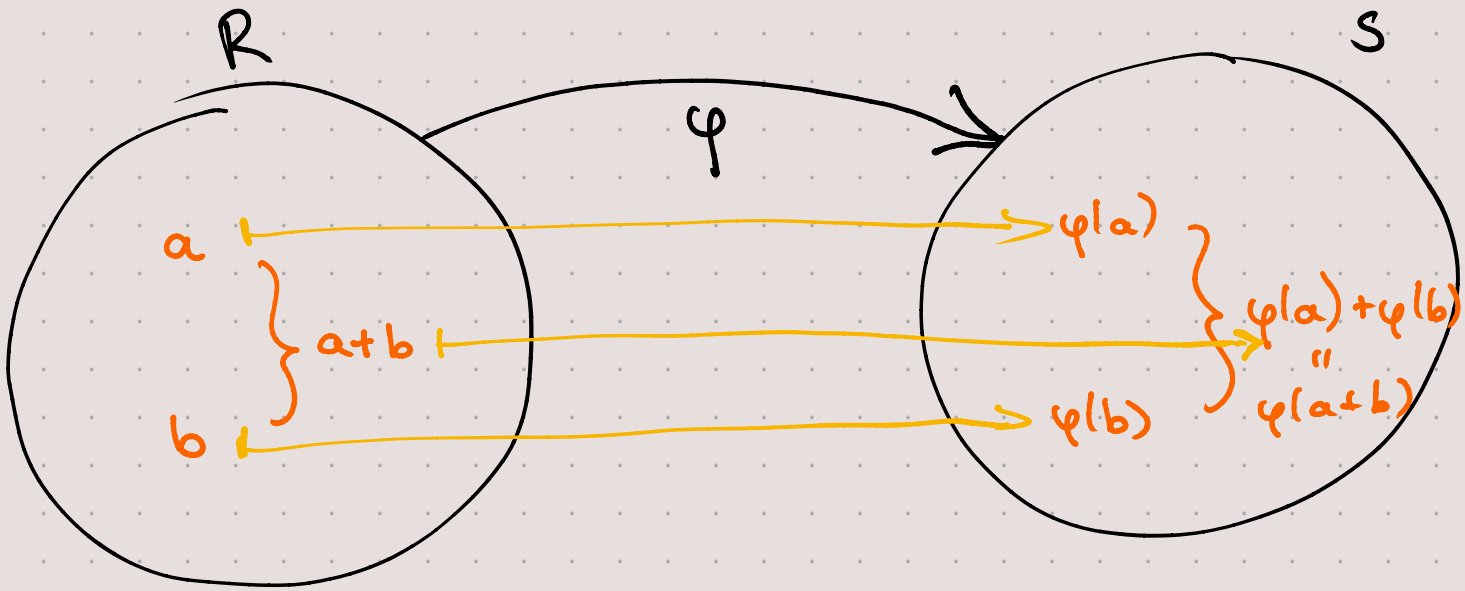


Buď R, S okruhy. Bijektivní zobrazení $\varphi: R \to S$ nazveme

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 $\exists$)



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 $a*b = b*a \quad \forall a,b \in G$.

Zápis: typicky
- aditivní $(G, +, -, 0)$
- multiplikativní $(G, \cdot, ^{-1}, 1)$, $(G, \circ, ^{-1}, id)$

Spousta tvrzení:

① $*$ asociativní $\Rightarrow$ výrazy $a_1 * \dots * a_n$ 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) $(a*b)' = b' * a'$

③

④

⋮

} pro okruhy

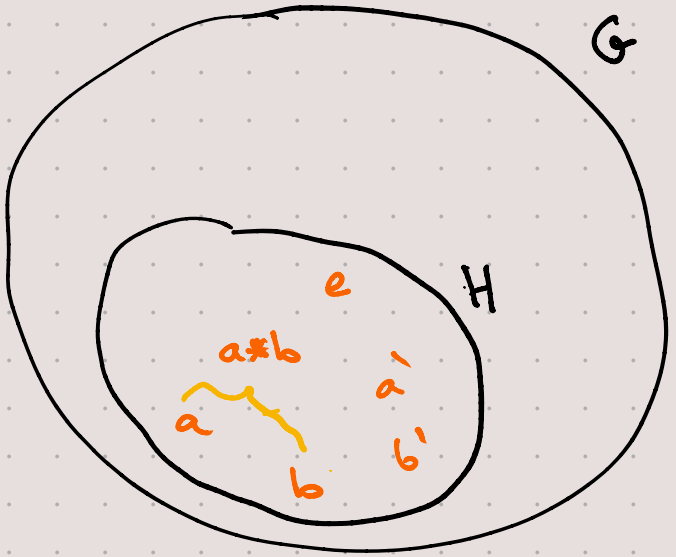
Buď $G = (G, *, ', e)$ grupa.

Buď $H \subseteq G$ podmnožina t.ž. $1 \in H$
$a, b \in H \Rightarrow a * b \in H$
$a \in H \Rightarrow a' \in H$

} je uzavřená na operace $*, '$

Pak $(H, *\restriction_H, '\restriction_H, e)$ nazýváme PODGRUPA grupy G.

$*\restriction_H, '\restriction_H$ ... restrikce operací z G na H



Tvrzení: Průnik podgrup je podgrupa.

def.: Buď $G_i = (G_i, *_i, {}^{-1_i}, e_i)$ grupy, $i = 1, \dots, n$.

Definujeme operace na kartézském součinu $G_1 \times \dots \times G_n$:

$$(a_1, \dots, a_n) * (b_1, \dots, b_n) := (a_1 *_1 b_1, \dots, a_n *_n b_n)$$

$$(a_1, \dots, a_n)' := (a_1^{-1}, \dots, a_n^{-1})$$

$$e := (e_1, \dots, e_n)$$

Pak $(G_1 \times \dots \times G_n, *, {}', e)$ je grupa, říkáme jí

DIREKTNÍ SOUČIN a značíme také $G_1 \times \dots \times G_n$.

Pozn.: pro $G_1 = \dots = G_n = G$ hovoříme o DIREKTNÍ MOCNINĚ G^n

def.: Buď $(G, \cdot, ^{-1}, 1)$ grupa, $a \in G$, $n \in \mathbb{Z}$.

MOCNINA PRVKU:

$$a^n := \begin{cases} \underbrace{a \cdot \ldots \cdot a}_{n\text{-krát}} & \text{pro } n > 0 \\ 1 & \text{pro } n = 0 \\ \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{(-n)\text{-krát}} & \text{pro } n < 0 \end{cases}$$

$a^{k+l} = a^k \cdot a^l$, $a^{k \cdot l} = (a^k)^l = (a^l)^k$, $a \cdot b = b \cdot a \Rightarrow (a \cdot b)^k = a^k \cdot b^k$

Pozn.: v aditivním zápise píšeme ~~a^k~~ $k \cdot a$ a platí

$(k+l)a = k \cdot a + l \cdot a$, $(k \cdot l) \cdot a = k \cdot (l \cdot a) = l \cdot (k \cdot a)$, $a + b = b + a \Rightarrow k \cdot (a+b) = k \cdot a + k \cdot b$

def.: ŘÁD prvku a v grupě G je
- nejmenší $n \in \mathbb{N}$ t.ž. $a^n = 1$ pokud takové existuje
- ∞ — " — ne - " —

$=: \operatorname{ord}_G(a)$

def.: ŘÁD GRUPY G je $|G|$.

Pozn.: brzy dokážeme, že $\operatorname{ord}_G(a) = |\langle a \rangle_G|$.