$G$ grupa $(G, \cdot)$

asoc., jedn. $e$, $\forall a \in G \; \exists \bar{a}^{-1} \in G$

$(a \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot a = e)$

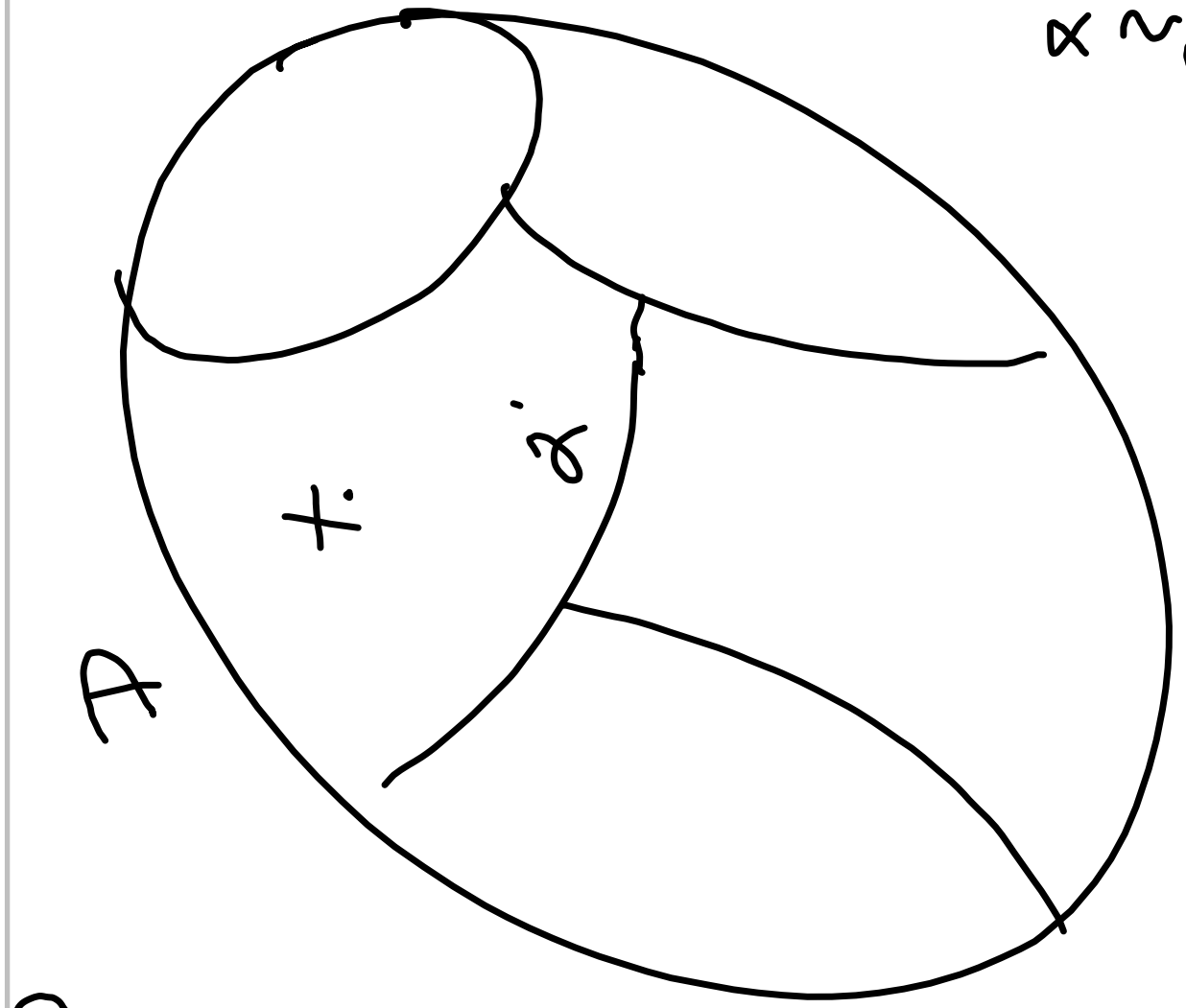
$H$ podgrupa

$H \subseteq G$ a $H$ je grupou

$e \in H$, $\forall a, b \in H : a \cdot b \in H$

$\forall a \in H : \bar{a}^{-1} \in H$

$\left[ \forall a, b \in H : a \cdot \bar{b}^{-1} \in H \right]$




$x \sim_{\mathcal{R}} y$

$\bigcup A_i = A$

$\forall i,j, i \neq j$

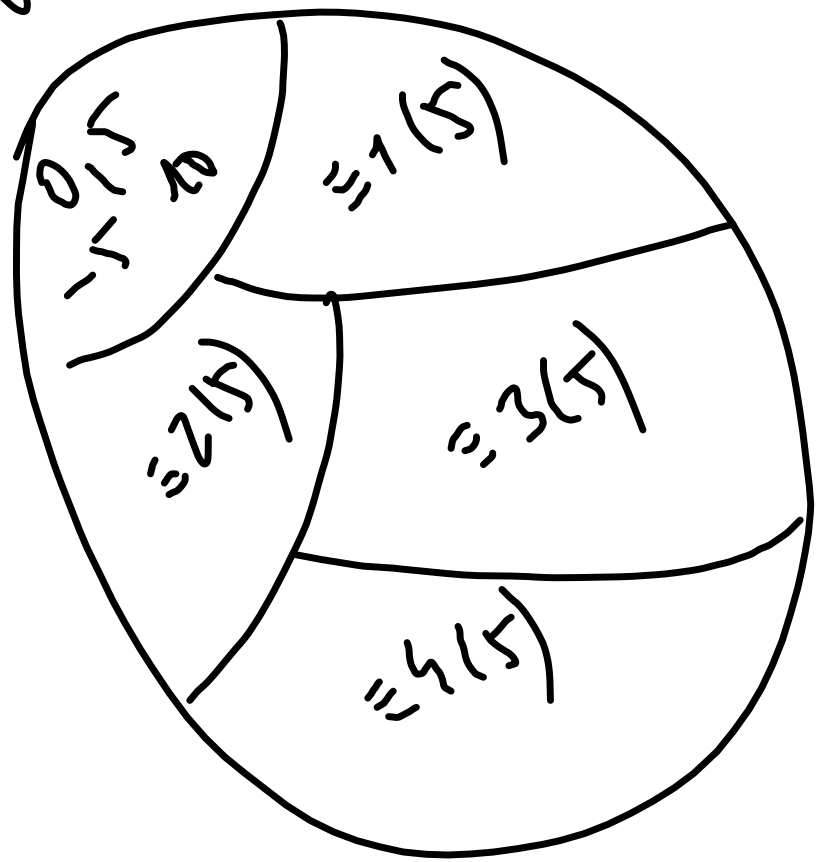
$\Rightarrow A_i \cap A_j$

Rozklad množiny $A_i, i \in I$

Př. ekvivalence $(\mathbb{Z}, S, T)$

kongruence mod $m \in \mathbb{N}$ na $\mathbb{Z}$

$m=5$



$H \leq G \quad (H < G)$

$a \sim_H b :\Leftrightarrow b^{-1} \cdot a \in H$

$b^{-1} \cdot a \in H \Rightarrow (b^{-1} \cdot a)^{-1} = a^{-1} \cdot (b^{-1})^{-1} = a^{-1} b \in H$

T: $a \sim_H b \wedge b \sim_H c$

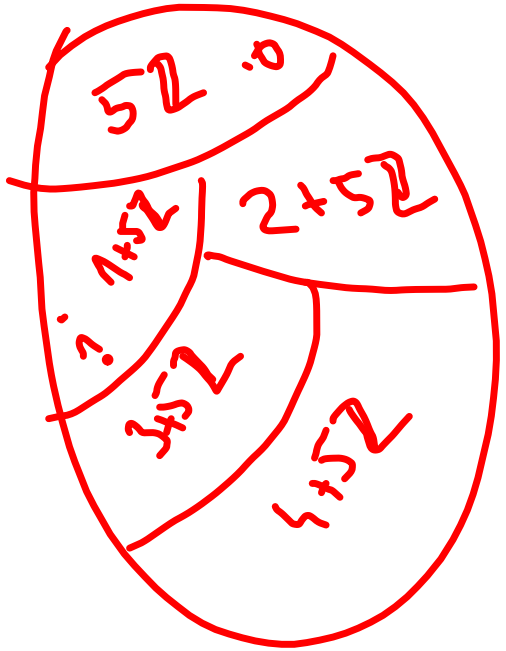
$b^{-1} a \in H \quad c^{-1} b \in H \Rightarrow c^{-1} a \in H \Rightarrow$

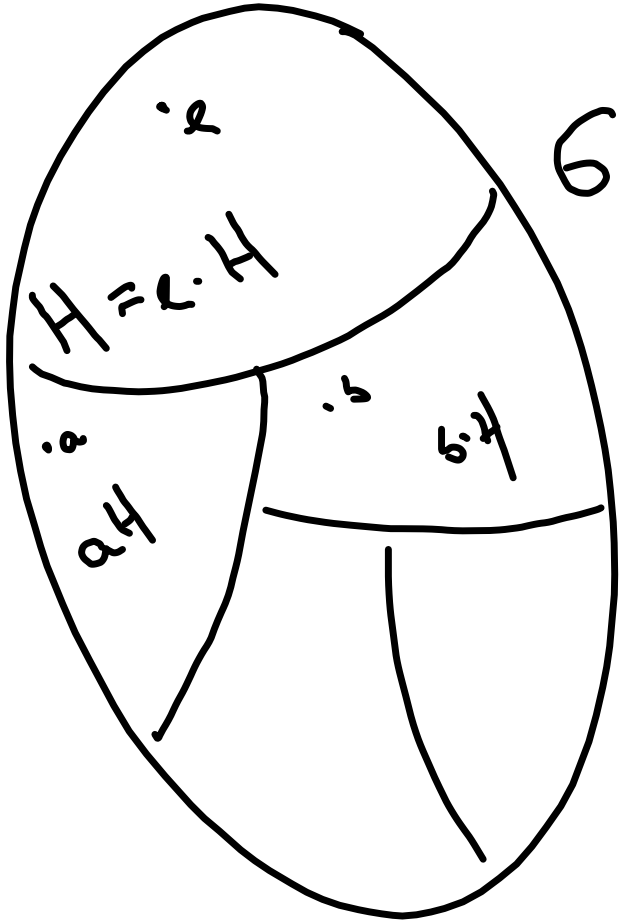
$a \sim_H c$

Př: Kongruence mod 5

$G = (\mathbb{Z}, +)$

$H = (5\mathbb{Z}, +)$




$G/H$

$a \cdot H = b \cdot H \Leftrightarrow \forall h_1 \in H \exists h_2 \in H : a \cdot h_1 = b \cdot h_2 \quad / \cdot b^{-1}$

$b^{-1} \cdot a \cdot h_1 = h_2 \quad / \cdot h_1^{-1}$

$b^{-1} \cdot a = h_2 h_1^{-1} \in H$

$\forall a:\ a \cdot H = H \cdot a$

$\forall h \in H\ \exists h' \in H:\ a \cdot h = h' a \quad / \cdot a^{-1}$

$a \cdot h \cdot a^{-1} = h' \in H$

---

$H$ má stejnou mohutnost (stejně prvků)

jako $a \cdot H$ $(\forall a \in G)$

$\varphi : H \longrightarrow a \cdot H$

$h \mapsto a \cdot h \in a \cdot H$

injektivní:

$a \cdot h_1 = a \cdot h_2 \quad / \cdot a^{-1}$

$h_1 = h_2$

surjektivní

$\forall y \in a \cdot H\ \exists x:\ \varphi(x) = y$

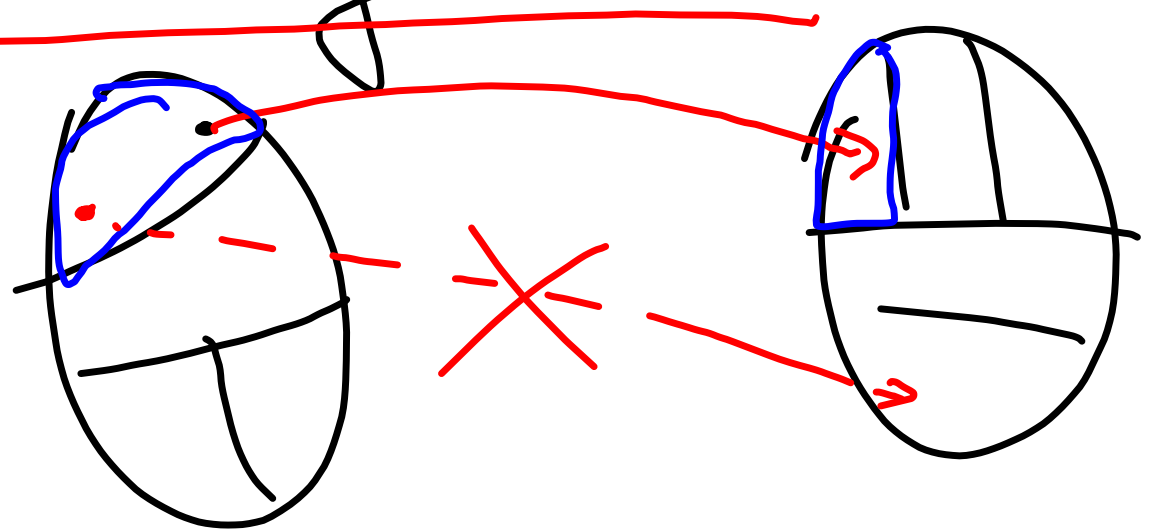
$\exists h \in H:\ y = a \cdot h \Rightarrow x = a^{-1} \cdot y$

bijekce mezi $G/H$ a $H\backslash G$

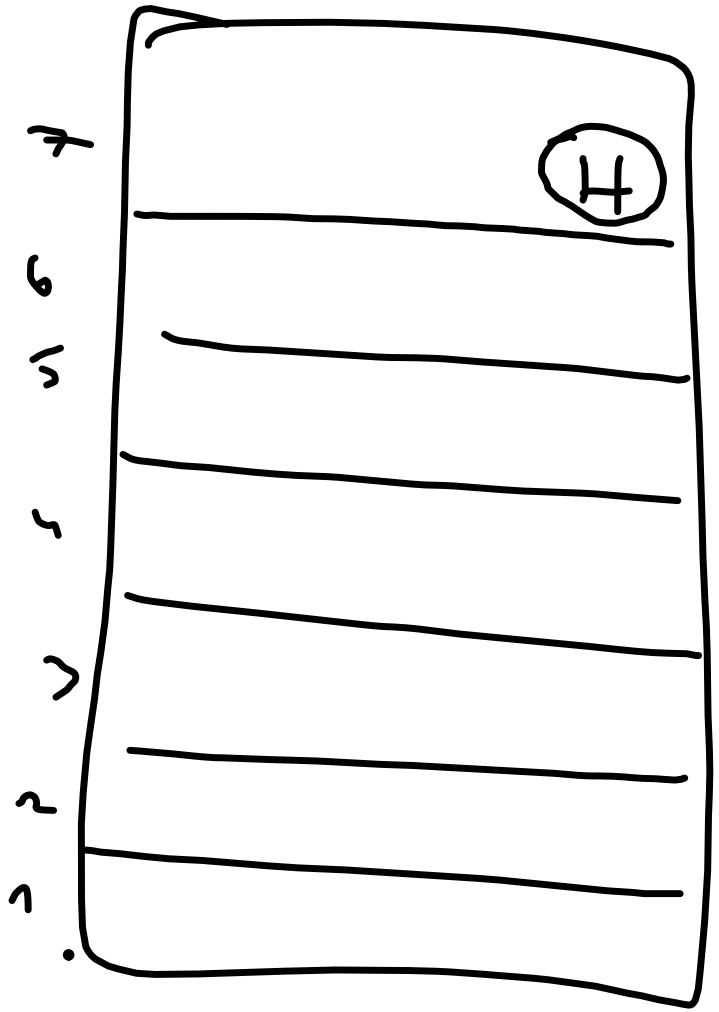
$$a \cdot H \longmapsto H \cdot a^{-1}$$

$\forall a,b \in H: a \cdot H = b \cdot H \Rightarrow H \cdot a^{-1} = H \cdot b^{-1}$

dobře definované zobrazení, bijekce



$aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow a^{-1}b = a^{-1}(b^{-1})^{-1} \in H \Leftrightarrow H \cdot a^{-1} = Hb^{-1}$




$n = |G|$

řád grupy

Pak:

$|G/H| = 7$

$|G| = 7 \cdot |H|$

$\langle a \rangle = \{e, a, a \cdot a = a^2, a \cdot a \cdot a = a^3, \ldots, a^k = e, \ldots\}$

$a \in G$

podgrupa $G$ generovaná prvkem $a$

má $k$ prvků

$\Rightarrow k \mid |G|$

Př. $\nu\ (\mathbb{Z}, +)$

$\langle 2 \rangle = 2\mathbb{Z}$ ... sudá čísla

$\nu\ (\mathbb{Z}_8, +)$

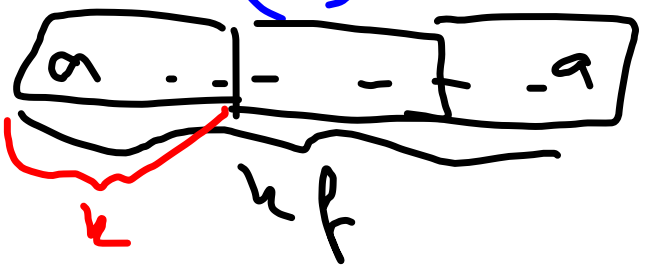
$\langle [2]_8 \rangle = \{[2], [4], [6], [8] = [0]\}$

řád $[2]_8$ je roven 4

$a \in G$

$\text{řád } a = \min\{k \in \mathbb{N} : a^k = e\}$

$k \mid n \Rightarrow a^n = a^{k \cdot l} = (a^k)^l = e^l = e$

$n = k \cdot l$ $\quad \underbrace{a \cdots a}_{n} =$ 


Důk. 5 $\quad |G| = p$

$a \in G \Rightarrow$ řád $a$ dělí $p$

$\Rightarrow$ řád $a$ je 1 nebo $p$

$\exists g \in G$ řádu $p$: $G = \langle e, g, g^2, \dots, g^{p-1} \rangle \cong (\mathbb{Z}_p, +)$

izomorfismus $G \longrightarrow \mathbb{Z}_p$

$g \longmapsto [1]_p$

(celkem $g^2 \longmapsto [2]_p$

$g^3 \longmapsto [3]_p$

$\vdots$

$e = g^p \longmapsto [0]_p$

M.F.V. pta  p prvočíslo

$$a^{p-1} \equiv 1 \pmod{p}$$

$$G = (\mathbb{Z}_p^\times, \cdot)$$

$$\mathbb{Z}_p^\times = \{[1]_p, [2]_p, [3]_p, \dots, [p-1]_p\}$$

$e$

$|\mathbb{Z}_p^\times|$

$\forall [a] \in \mathbb{Z}_p^\times: \quad [a]^{p-1} = e = [1]$

$[a^{p-1}]_p = [1]_p \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$

$m \in \mathbb{N}$

$(\mathbb{Z}_m^\times, \cdot)$ grupa invertibilních zbytkových tříd modulo $m$

$|\mathbb{Z}_m^\times| = \varphi(m)$

Tj. v $(\mathbb{Z}_m, \cdot)$ jsou invertibilní $[a]$ pro které $(a, m) = 1$ [ $\exists x: a \cdot x \equiv 1 \ (m)$ ]

Takových tříd je $\varphi(m)$

$[a]_m^{\varphi(m)} = [1]$

$a^{\varphi(m)} \equiv 1 \ (m)$

---

Př: $(\mathbb{Z}_6, \cdot)$ $[2] \cdot [a] = [1]$

$\nexists a$

$\forall a \in G \quad \forall h \in H:$

$a \cdot h a^{-1} \in H$

$\exists h': \; a \cdot h a^{-1} = h' \qquad / \cdot a$

$a \cdot h = h' \cdot a$

$^{c}a \cdot H \subseteq {}^{c}H \cdot a$

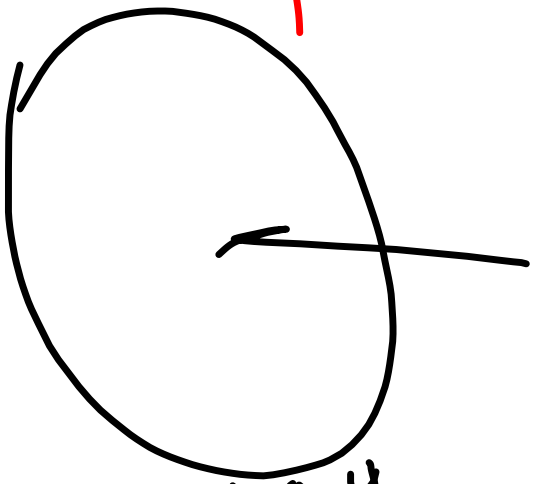
podle 2

$H \trianglelefteq G$

$\{1\} = \{e\} \trianglelefteq G$

Př. $G/G$ $\quad a \sim_G b \Leftrightarrow b^{-1}a \in G$

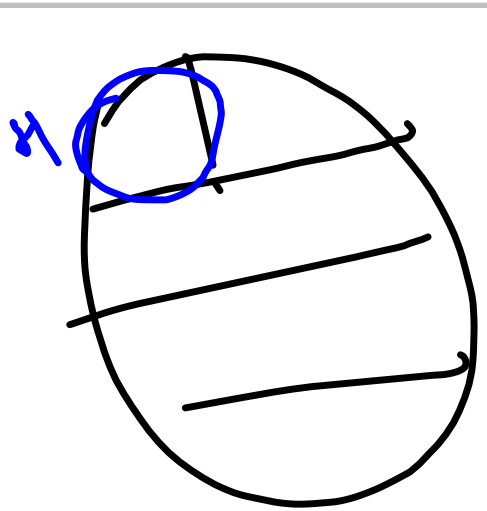
platí kdykoliv



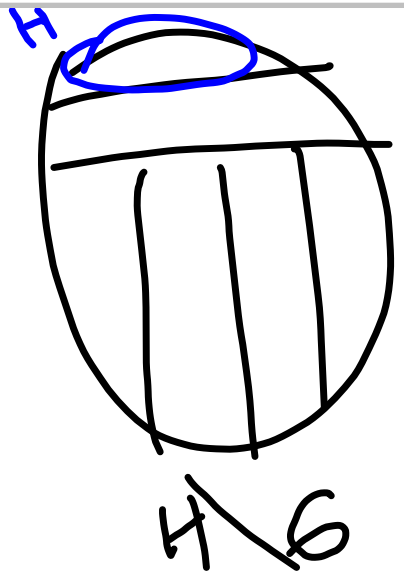
jediná třída

Př. $G$ komut. $\quad a \cdot h \cdot a^{-1} = a \cdot a^{-1} \cdot h =$

$= e \cdot h = h \in H$




$G/H$



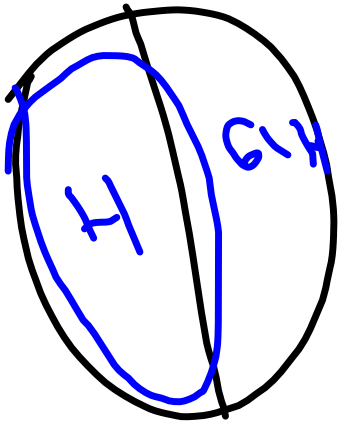

$H \backslash G$

$|H| = \frac{|G|}{2}$

$G/H$


$=$

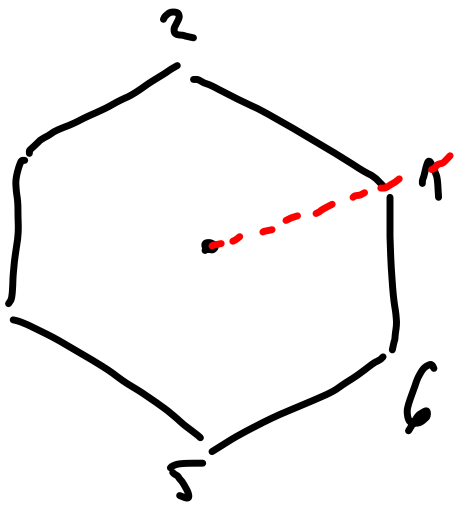
$H \backslash G$




$\Rightarrow$ H normální v G

$D_{2n}$ ... grupa symetrií pravidelného $n$-úhelníka

$\langle r, s \mid r^n = id,\ s^2 = id,\ sr = r^{-1}s \rangle$




$sr = (1,6)(2,5)$
$(3,4)$

$r^{-1}s = (1,6)(2,5)$
$(3,4)$

$r$ ... rotace o $60° \left( \sigma \frac{2\pi}{n} \right)$ $= (1,2,3,4,5,6)$

$r^6 = id$ $\quad r^n = id$

$s$ ... Symetrie podle přímky $\quad s^2 = id$

$r \; s \; r^3 \; s \; r^2 \; s \; r^{-2} \; s$

$r \; r^{-3} \; s \quad \ldots$

$r^{-2} \; s \; s \; r^2 \; s \; r^{-2} \; s$

$r^{-2} \; r^2 \; s \; r^{-2} \; s$

$s \; r^{-2} \; s$

$r^2 \cdot s \cdot s$

$r^2$

$$D_{2n}/\langle r\rangle = \{\{r, r^2, \dots, r^{n-1}, e\},\ \{s, rs, r^2s, \dots, r^{n-1}s\}\}$$

$r^n = s$

---

$$D_8 = \{id, r, r^2, r^3, s, rs, r^2s, r^3s,\ s = r^4s\}$$

$(1,3)(2,4)$

$\langle r^2\rangle$

$H = \langle r^2 \rangle = \{id, r^2\}$

$G = D_8$

$(rH) \circ (rsH) = r^2 sH = sH$

$(r^3H) \circ (rsH) = r^4 sH = sH$

$id \cdot H = H$

$r \cdot H = \{r, r^3\}$

$r^2 \cdot H = \{r^2, id\} = H$

$r^3 \cdot H = \{r^3, r\} = r \cdot H$

$sH = \{s, sr^2 = r^{-2} \cdot s = r^2 s\}$

$rsH = \{r \cdot s, rsr^2 = r \cdot r^{-2} \cdot s = r^{-1} \cdot s = r^3 \cdot s\}$

$r^2 sH = \{r^2 \cdot s, r^2 s r^2 = r^2 \cdot r^2 \cdot s = s\}$

$r^3 sH = \{r^3 \cdot s, r^3 \cdot s \cdot r^2 = r^5 \cdot s = r \cdot s\}$

$a \cdot h \cdot b \cdot h' = a \cdot b \, b^{-1} h b h' \in ab \cdot H$

$a \cdot h \in aH$ $\quad b \cdot h' \in bH$

$b^{-1} h b \in H$

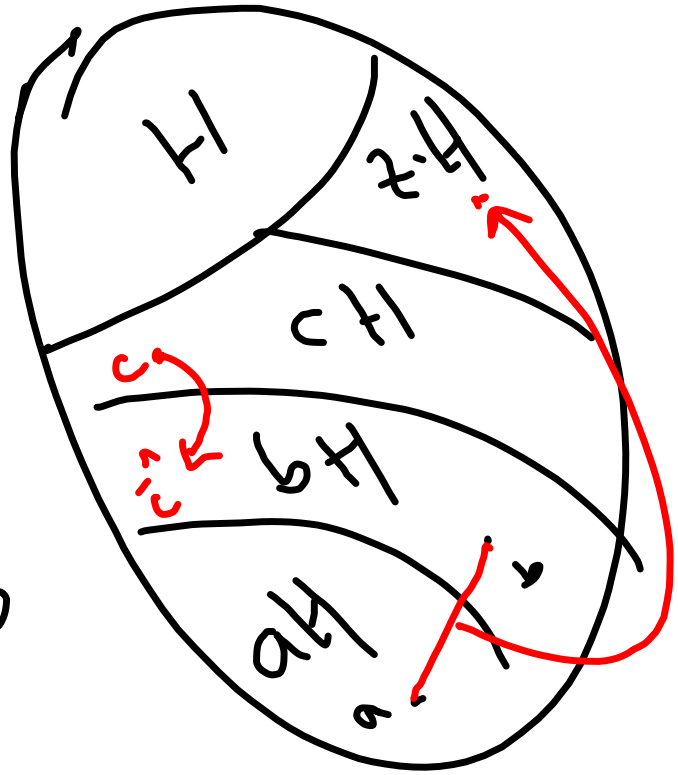
$b^{-1} h b h' \in H$

---

$(G/H, \circ)$ je grupa

jednotka $G/H$ je $H$ $\left[ \begin{array}{l} H = e \cdot H \\ (e \cdot H) \circ (a \cdot H) = (e \cdot a) H = aH \\ (aH)(eH) = (a \cdot e) H = a \cdot H \end{array} \right.$

$aH \in G/H$ je inverze $a^{-1} H$




6

$(a\cdot H)\circ(b\cdot H) =$

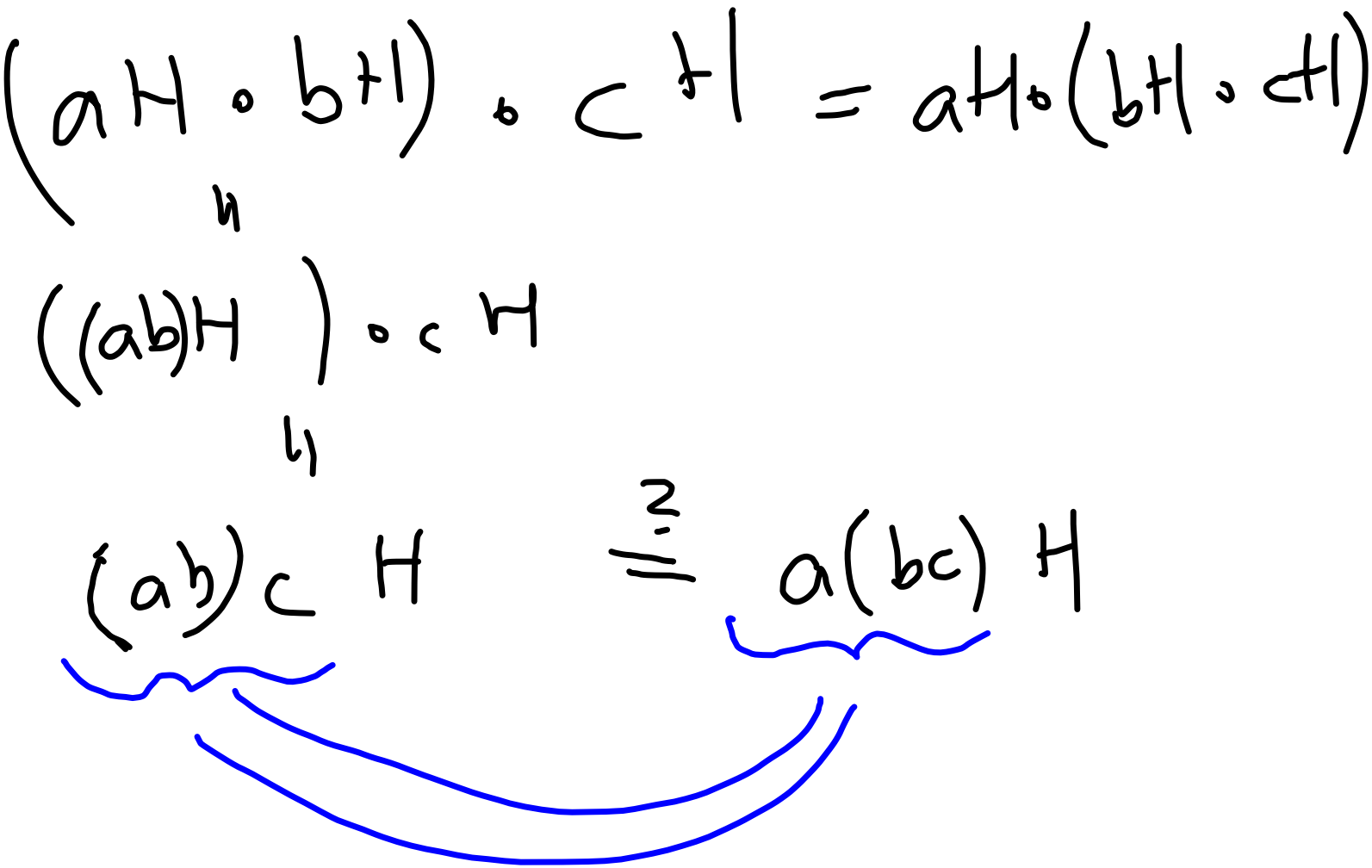
$(a\cdot b)H = zH$

$(cH)^{-1} = c^{-1}H$

inverze

$(cH)\circ(c^{-1}\cdot H) = (c\cdot c^{-1})H = e\cdot H = H$

$e$


(aH · bH) · cH = aH · (bH · cH)
((ab)H) · cH
(ab)c H = a(bc) H

Buď $f: G \to H$ homomorfismus

$$\ker f = \{g \in G;\ f(e) = e_H\}$$

$\ker f \lhd G$

$a, b \in \ker f \Rightarrow ab^{-1} \in \ker f$

$f(a) = f(b) = e_H$

$f(ab^{-1}) = f(a) \cdot f(b)^{-1} = e_H \cdot e_H^{-1} = e_H$

$\ker f$ je normální:

$\forall a \in G\ \forall h \in \ker f:\ aha^{-1} \in \ker f \Leftrightarrow f(aha^{-1}) = e_H$

$$f(aha^{-1}) = f(a)\cdot f(h)\cdot f(a)^{-1} =$$

$h \in \ker f$

$$= f(a)\, e_H\, f(a)^{-1} = f(a)\cdot f(a)^{-1} = e_H$$

$$\Rightarrow aha^{-1} \in \ker f$$

$$p: G \to G/H \qquad \ker p = H$$

$$a \mapsto aH$$