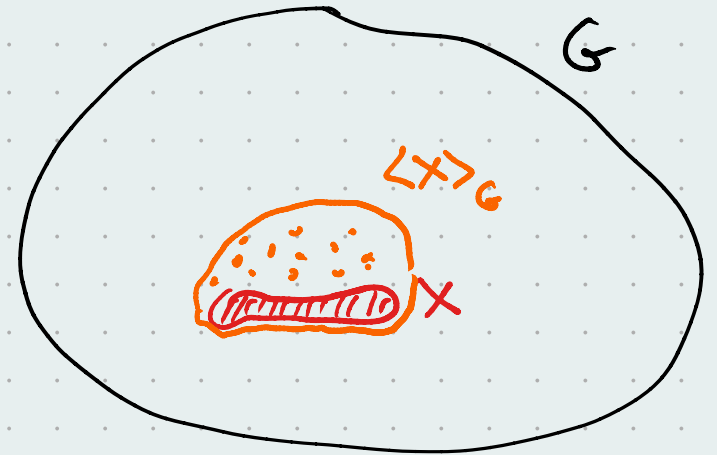


Bnd' G grupa, $X \subseteq G$. Podgrupa generovaná množinou X v G , ozn. $\langle X \rangle_G$,
je nejmenší podgrupa G obsahující X .

☺ existuje, $\langle X \rangle_G = \bigcap_{X \subseteq H \leq G} H$



Tvrzení: G grupa, $\emptyset \neq X \subseteq G \Rightarrow$

$$\langle X \rangle_G = \{ a_1^{k_1} \cdots a_n^{k_n} : n \in \mathbb{N}, a_i \in X, k_i \in \mathbb{Z} \}$$

Speciální případy:

$$\langle a \rangle_G = \{ a^k : k \in \mathbb{Z} \} \quad \dots \text{tzv. } \underline{\text{CYKLICKÉ}} \text{ grupy}$$

$$G \text{ abelovská} \Rightarrow \langle u_1, \dots, u_n \rangle_G = \left\{ \sum_{i=1}^n k_i u_i : k_i \in \mathbb{Z} \right\}$$

Tvrzení: Bnd' G grupa, $a \in G$. Pak $\text{ord}_G(a) = |\langle a \rangle_G|$.

Lagrangeova věta: Bud' G grupa, H její podgrupa. Pak

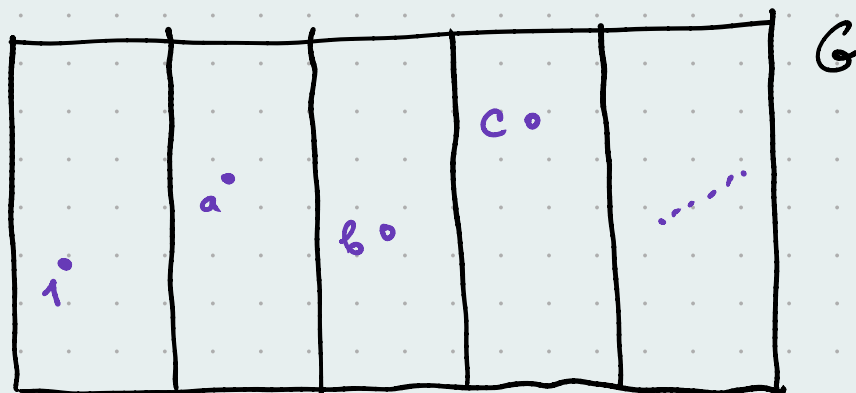
$$|G| = |H| \cdot [G:H].$$

tj. $|H|$ dělí $|G|$
v konečném případě

def: $aH = \{ah : h \in H\}$... (levé) rozkladové třídy

$T \subseteq G$ t.ž. $|T \cap aH| = 1 \quad \forall a \in G$... (levá) transverzála

$[G:H] = |\{aH : a \in G\}|$... (levý) index H v G



$$T = \{1, a, b, c, \dots\}$$

Lagrangeova věta: Bud' G grupa, H její podgrupa. Pak

$$|G| = |H| \cdot [G:H].$$

Lemma 1: $\forall a, b \in G \quad \begin{cases} aH = bH \\ aH \cap bH = \emptyset \end{cases}$

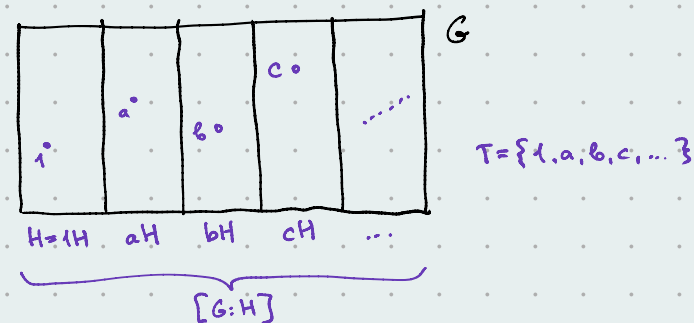
Lemma 2: $\forall a \in G \quad |aH| = |H|$

Lemma 3: $aH = bH \Leftrightarrow a^{-1}b \in H$

Pozn.: Mohli bychom definovat i pravé varianty.

l./p. rozkladové třídy mohou být různé, ale jejich počet je stejný.

def: $aH = \{ah : h \in H\}$... (levé) rozkladové třídy
 $T \subseteq G$ t.č. $|T \cap aH| = 1 \quad \forall a \in G$... (levá) transverzála
 $[G:H] = |\{aH : a \in G\}|$... (levý) index H v G

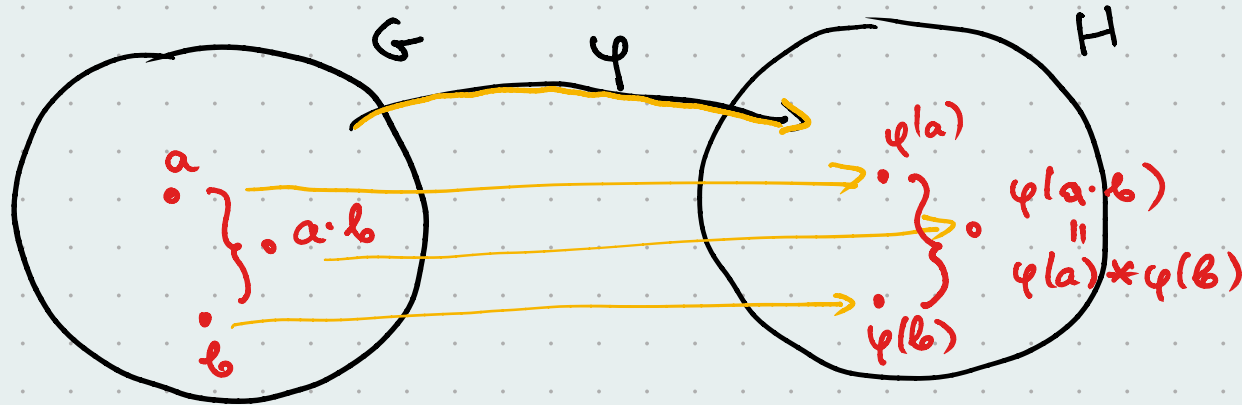


And' $G = (G, \cdot, ^{-1}, 1)$, $H = (H, *, ', e)$ grupy.

HOMOMORFISMEM rozumíme zobrazení $\varphi: G \rightarrow H$ splňující

$$\varphi(1) = e, \quad \varphi(a^{-1}) = \varphi(a)', \quad \boxed{\varphi(a \cdot b) = \varphi(a) * \varphi(b)} \quad \forall a, b \in G$$

Lemma: ta 3. identita implikuje 1. a 2.



def.: jádro φ : $\text{Ker } \varphi := \{a \in G : \varphi(a) = e\}$

$$\odot \text{Ker } \varphi \leq G$$

obraz φ : $\text{Im } \varphi := \{\varphi(a) : a \in G\}$

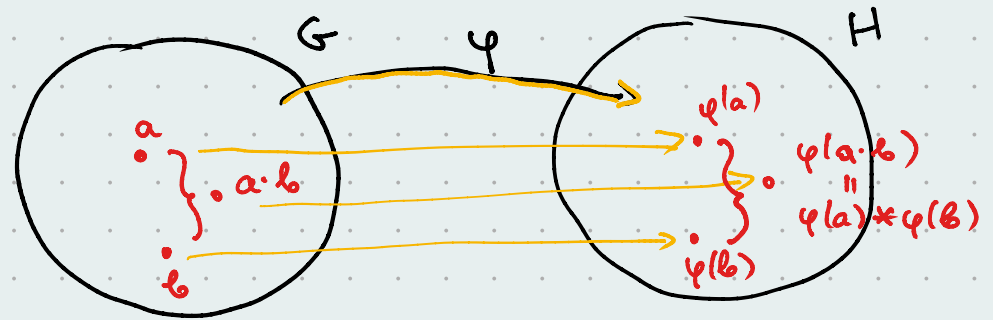
$$\odot \text{Im } \varphi \leq H$$

$\odot$ φ je prosté $\Leftrightarrow \text{Ker } \varphi = \{1\}$

Fakt: homomorfismy jsou určeny
hodnotami na generátorech

tj. $G = \langle X \rangle$, $\varphi: G \rightarrow H$ hom.

$$a \mapsto h_a \text{ pro } a \in X$$



$$\begin{aligned} \Rightarrow \varphi(g) &= \varphi(a_1^{k_1} \dots a_n^{k_n}) = \varphi(a_1)^{k_1} * \dots * \varphi(a_n)^{k_n} \\ &= h_{a_1}^{k_1} * \dots * h_{a_n}^{k_n} \end{aligned}$$

ALE ne každá volba h_a lze rozšířit do homomorfismu

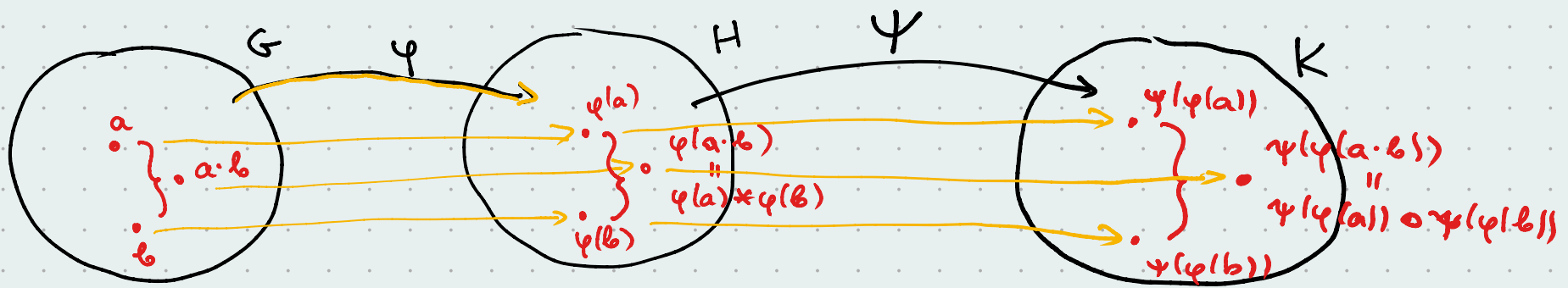
Trvzení: Bnd' $\varphi: G \rightarrow H$ homomorfismus grup.

Paž $\text{ord}_H(\varphi(a)) \mid \text{ord}_G(a) \quad \forall a \in G. \quad (\text{cokoliv } \mid \infty)$

Je-li φ prostý, paž nastává rovnost.

Trvzení: Bnd' $\varphi: G \rightarrow H$ homomorfismus grup na H .

Je-li $G = \langle X \rangle$, paž $H = \langle \varphi(X) \rangle$.



Tvzení: Složený homomorfismus je homomorfismus.
 Inverzní bijektivní homomorfismus je homomorfismus.

def.: **IZOMORFISMUS**

Řekneme, že grupy G, H jsou izomorfní, píšeme $G \cong H$
 pokud $\exists \varphi: G \rightarrow H$ izomorfismus.

Důsledek: $\cong$ je ekvivalence na grupách

Jak dokázat, že $G \neq H$?

Idea **INVARIANTU**: vlastnost V t.ž. $G \cong H$
 $G \text{ má } V$ $\} \Rightarrow H \text{ má } V$

- Příklady:
- řád grupy
 - počet prvků daného řádu
 - minimální počet generátorů
 - existence "odmocnin" $\forall a \exists b \quad b * b = a$
a jiné formule 1. řádu

Trvzení: Bud' $\varphi: G \rightarrow H$ **prvstí** homomorfismus grup.
Pak $\text{ord}_H(\varphi(a)) = \text{ord}_G(a) \quad \forall a \in G$.

Trvzení: Bud' $\varphi: G \rightarrow H$ homomorfismus grup na H .
Je-li $G = \langle x \rangle$, pak $H = \langle \varphi(x) \rangle$.

Klasifikační věty

Věta: Bud' X algebraická struktura splňující
Pak $X \cong |\text{XXXX}|$, pro nějaký parametr

matr. klasifikace konečných těles

Věta: (klasifikace cyklických grup)

Bud' G cyklická grupa. Pak $\begin{cases} G \text{ je nekonečná a } G \cong \mathbb{Z} \\ G \text{ je konečná a } G \cong \mathbb{Z}_n \text{ pro nějaké } n \in \mathbb{N}. \end{cases}$

Důsledek: (klasifikace grup prvočíselného řádu)

Bud' G grupa t.č. $|G| = p$ prvočíslo. Pak $G \cong \mathbb{Z}_p$.

Věta: (klasifikace konečně generovaných abelovských grup)

Bud' G konečně generovaná abelovská grupa. Pak

$$G \cong \mathbb{Z}^m \times \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_m^{k_m}}$$

pro nějaká $m, n \in \mathbb{N}$, $p_i^{k_i}$ mocniny prvočísel.

