def: <u>GRUPA</u> je algebraická struktura $(G, *, ', e)$ kde $*$ binární, $'$ unární

splňující

$$a*(b*c) = (a*b)*c$$
$$a*e = e*a = a \qquad \forall a,b,c \in G$$
$$a*a' = a'*a = e$$

Grupa se nazývá <u>ABELOVSKÁ</u> pokud $a*b = b*a \quad \forall a,b \in G$.

def: Buď $\mathbf{G} = (G, *, ', e)$ grupa, $H \subseteq G$ t.ž.

$$\left.\begin{array}{l} e \in H \\ a' \in H \\ a*b \in H \end{array}\right\} \forall a,b \in H.$$

Říkáme, že H je <u>uzavřená</u> na grupové operace, že <u>tvoří podgrupu</u>.
Struktura $\mathbf{H} = (H, *|_H, '|_H, e)$ se nazývá <u>podgrupa</u> grupy $\mathbf{G}$.
Píšeme $H \leq \mathbf{G}$, $\mathbf{H} \leq \mathbf{G}$

<u>Příklady</u>: - <u>permutační grupy</u>: $S_X = (\{\text{permutace na } X\}, \circ, ^{-1}, id)$ a její podgrupy

- grupy geometrických transformací
- <u>maticové grupy</u> $GL_n(T) = (\{\text{regulární matice } n \times n \text{ nad } T\}, \cdot, ^{-1}, I)$ a její podgrupy
- R komutativní okruh $\to (R, +, -, 0)$
  $\to (R^*, \cdot, ^{-1}, 1)$ ... invertibilní prvky

ATD.

def: <u>DIREKTNÍ SOUČIN</u> grup $G_1, \dots, G_n$, označme $G_i = (G_i, *_i, '^{i}, e_i)$:

$$\prod G_i = G_1 \times \dots \times G_n = (G_1 \times \dots \times G_n, *, ', (e_1, \dots, e_n))$$

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

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

def: G grupa, $a \in G$, $n \in \mathbb{Z}$ ... $a^n := \begin{cases} 1 & \text{pro } n = 0 \\ \underbrace{a \cdot \ldots \cdot a}_{n} & \text{pro } n > 0 \\ \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-n} & \text{pro } n < 0 \end{cases}$

<u>Tvrzení</u>: G grupa, $a, b \in G$, $k, l \in \mathbb{Z}$ $\Rightarrow$ $a^{k+l} = a^k \cdot a^l$

$a^{kl} = (a^k)^l = (a^l)^k$

G abelovská $\Rightarrow$ $(ab)^k = a^k b^k$

def: <u>ŘÁD grupy G</u> $= |G|$

<u>ŘÁD prvku a v G</u> $= \begin{cases} \text{nejmenší } n \in \mathbb{N} \text{ t.ž. } a^n = 1 & \text{pokud existuje} \\ \infty & \text{v opačném případě} \end{cases}$

__def__: Buď G grupa, $X \subseteq G$. __Podgrupa generovaná__ množinou X v grupě G je

$$\langle X \rangle_G := \text{nejmenší (v } \subseteq \text{) podgrupa } G \text{ obsahující } X = \bigcap_{X \subseteq H \leq G} H$$

__Tvrzení__: Buď G grupa, $\emptyset \neq X \subseteq G$. Pak $\boxed{\langle X \rangle_G = \{ a_1^{k_1} \cdots a_n^{k_n} : n \in \mathbb{N},\ a_i \in X,\ k_i \in \mathbb{Z} \}}$

__Důsledek__:
- $\langle a \rangle_G = \{ a^k : a \in \mathbb{Z} \}$
- G abelovská $\Rightarrow \langle u_1, \dots, u_n \rangle = \{ u_1^{k_1} \cdots u_n^{k_n} : k_i \in \mathbb{Z} \}$

__Tvrzení__: Buď G grupa, $a \in G$. Pak $\boxed{\mathrm{ord}_G(a) = |\langle a \rangle_G|}$.

def: Buď $H \leq G$. Pak

- $aH = \{ah : h \in H\}$, $a \in G$ … *rozkladové třídy* podgrupy H
- $T \subseteq G$ t.ž. $|T \cap aH| = 1$ $\forall a \in G$ … *transverzála* rozkladu G podle H
- $[G:H] = |\{aH : a \in G\}|$ … *index* H v G

Lagrangeova věta: $H \leq G \Rightarrow \boxed{|G| = |H| \cdot [G:H]}$

Lemma 1: $H \leq G$, $a, b \in G \Rightarrow aH = bH$ nebo $aH \cap bH = \emptyset$

Lemma 2: $H \leq G$, $a \in G \Rightarrow |aH| = |H|$

Tvrzení: $H \leq G$, $a, b \in G \Rightarrow$

- $aH = bH \Leftrightarrow a^{-1}b \in H$
- $Ha = Hb \Leftrightarrow ab^{-1} \in H$

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

<u>def</u>: $\varphi : G \to H$ je <u>homomorfismus</u>, pokud $\begin{cases} \varphi(a \cdot b) = \varphi(a) * \varphi(b) \\ \varphi(a^{-1}) = \varphi(a)' \\ \varphi(1) = e \end{cases} \quad \forall a, b \in G$

<u>Lemma</u>: První z těch tří rovností implikuje ostatní dvě.

<u>def</u>: $\mathrm{Im}(\varphi) := \{\varphi(a) : a \in G\}$ ... <u>obraz</u>

$\mathrm{Ker}(\varphi) := \{a \in G : \varphi(a) = e\}$ ... <u>jádro</u>

<u>Tvrzení</u>: (1) $\mathrm{Im}(\varphi) \leq H$, $\mathrm{Ker}(\varphi) \leq G$

(2) φ je prostý $\Leftrightarrow$ $\mathrm{Ker}(\varphi) = \{1\}$

<u>Tvrzení</u>: $\forall a \in G \quad \mathrm{ord}_H(\varphi(a)) \mid \mathrm{ord}_G(a)$ (rozumí se cokoliv $\mid \infty$)

Navíc, je-li φ prostý, pak $\mathrm{ord}_H(\varphi(a)) = \mathrm{ord}_G(a)$

<u>Tvrzení</u>: Je-li φ <u>na</u> H a $G = \langle X \rangle$, pak $H = \langle \varphi(X) \rangle$.

<u>Tvrzení</u>: (1) $\varphi : G \to H$, $\psi : H \to K$ homomorfismy $\Rightarrow$ $(\psi \circ \varphi) : G \to K$ je homomorfis

(2) $\varphi : G \to H$ hom., bijektivní $\Rightarrow$ $\varphi^{-1} : H \to G$ je homomorfismus

__def__: Bijektivní homomorfismy se nazývají __IZOMORFISMY__,
resp. __automorfismy__ pokud $G = H$.

__def__: Grupy G, H jsou __izomorfní__, píšeme $G \simeq H$, pokud $\exists \varphi: G \to H$ izomorfismus.

☺. relace $\simeq$ je ekvivalencí na třídě všech grup

__def__: __invariant__ izomorfismu je vlastnost V t.ž.
kdykoliv má grupa G vlastnost V a $H \simeq G$, pak H má vlastnost V

__Př.__: počet prvků daného řádu

__Př.__: minimální počet generátorů

__Př.__: existence odmocnin, např. "$\forall a \exists b \; a = b * b$"

__Př.__: obecně jakákoliv vlastnost definovatelná formulí 1. řádu