ALGEBRA 2, 23.3.2020

- PŘIPOMENUTÍ: $(G, \cdot, ^{-1}, 1)$ JE GRUPA, POKUD
  - $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$
  - $a \cdot 1 = a = 1 \cdot a \quad \forall a \in G$
  - $a \cdot (a^{-1}) = 1 = (a^{-1}) \cdot a \quad \forall a \in G$

- T 1.1: (1) KRÁCENÍ: $a \cdot c = b \cdot c \Rightarrow a = b$
  $c \cdot a = c \cdot b \Rightarrow a = b$

  (2) JEDNOZNAČNOST JEDNOTKY: $a \cdot u = a \Rightarrow u = 1$
  $u \cdot a = a \Rightarrow u = 1$

  (3) JEDNOZNAČNOST INVERZE: $a \cdot b = 1 \Rightarrow b = a^{-1}$
  $b \cdot a = 1 \Rightarrow b = a^{-1}$

  (4) $(a^{-1})^{-1} = a$

  (5) $(a b)^{-1} = b^{-1} \cdot a^{-1}$

- MOCNINY: $a \in G, n \in \mathbb{Z}$

$$a^n = \begin{cases} a \cdot a \cdot \ldots \cdot a & n\text{-KRÁT}, \ n > 0 \\ 1 & , \ n = 0 \\ a^{-1} \cdot a^{-1} \cdots a^{-1} & |n|\text{-KRÁT}, \ n < 0 \end{cases}$$

- BĚŽNÉ VLASTNOSTI MOCNIN PLATÍ: $a^k a^l = a^{k+l}$,
  $(a^k)^l = a^{k \cdot l}$,

- ADITIVNÍ ZNAČENÍ: $(G, +, -, 0)$
  - MÍSTO a^n PÍŠEME $n \cdot a$, IDENTITY VÝŠE MAJÍ TVAR $k \cdot a + l \cdot a = (k+l) \cdot a$ a $l \cdot (k \cdot a) = (k \cdot l) \cdot a$

- POZOR (!): OBECNĚ $(a \cdot b)^n \neq a^n \cdot b^n$
  - $n = 2$: $(a \cdot b)^2 = a \cdot b \cdot a \cdot b$, $a^2 b^2 = a \cdot a \cdot b \cdot b$
  - LEDA BY G BYLA KOMUTATIVNÍ (TÉŽ ABELOVSKÁ)

– PŘÍKLADY GRUP

– GRUPY PERMUTACÍ: $(S(X), \circ, {}^{-1}, id_X)$,
$S(X) = \{ f : X \to X \text{ BIJEKCE} \}$

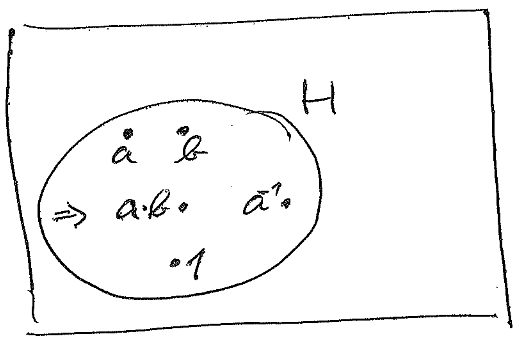
- $X = \{1, 2, \dots, n\} \rightsquigarrow (S_n, \circ, {}^{-1}, id)$

– MATICOVÉ GRUPY: $(GL_n(T), \cdot, {}^{-1}, I)$, T TĚLESO, $n \geq 1$

– $(R, +, -, \cdot, 0, 1)$ OKRUH S 1 $\rightsquigarrow$ $\left.\begin{matrix}(R, +, -, 0) \\ (R^*, \cdot, {}^{-1}, 1)\end{matrix}\right\}$ GRUPY

– PODGRUPY TĚCHTO:

G GRUPA

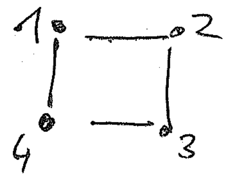


NAPŘ.: $A_n \leq S_n$ ALTERNUJÍCÍ GRUPA

~~PŘÍKLAD~~

– GRUPY AUTOMORFISMŮ MATEMATICKÝCH STRUKTUR

– např.: GRUPA AUTOMORFISMŮ GRAFU



$\rightsquigarrow$ 8 PRVKŮ: • id,

- ROTACE: $(1\,2\,3\,4)$, $(1\,4\,3\,2)$
  $90°$ $90°$

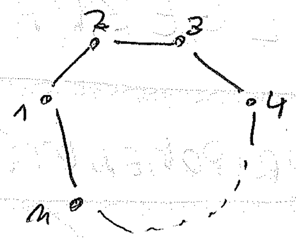
- STŘEDOVÁ SYMETRIE: $(1\,3)(2\,4)$

- ZRCADLENÍ (OSOVÉ SYMETRIE):

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

- OBECNĚJI: D_{2n}, DIHEDRÁLNÍ GRUPA

  $:=$ GRUPA AUTOMORFISMŮ GRAFU



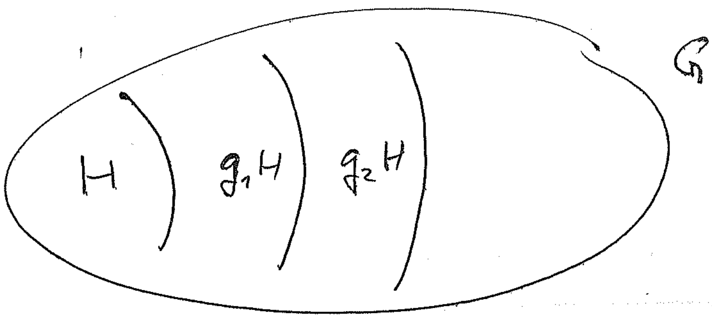
- Z MINULA:
- V: (LAGRANGEOVA) $(G, \cdot, ^{-1}, 1)$ GRUPA, H PODGRUPA

  PAK

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

JE-LI G KONEČNÁ, PAK $|H|$ DĚLÍ $|G|$.

- MYŠLENKA DŮKAZU



$g \cdot H = \{g \cdot h \mid h \in H\}$ LEVÁ ROZKLADOVÁ TŘÍDA PRVKU $g \in G$

- L 2.7: $a, b \in G$. PAK BUĎ $aH = bH$ NEBO $aH \cap bH = \emptyset$
- L 2.8: $\forall g$ EXISTUJE BIJEKCE $H \longrightarrow gH$

  $h \longmapsto g \cdot h$

- PAK $[G:H] :=$ POČET ROZKLADOVÝCH TŘÍD,
  (LEVÝ) INDEX PODGRUPY H V GRUPĚ G.

- POZN: SAMOZŘEJMĚ TOTÉŽ LZE PROVÉST
  S PRAVÝMI ROZKLADOVÝMI TŘÍDAMI

  $Hg = \{h \cdot g \mid h \in H\}$, KDE $g \in G$

- NORMÁLNÍ PODGRUPY — BUĎ $(G, \cdot, ^{-1}, 1)$ GRUPA, H PODGRUPA, $g \in G$

- OBECNĚ $g \cdot H \neq H \cdot g$

- PŘ: $S_3 =: G$, $\{id, (12)\} =: H$, $(13) =: g$

(str 16, zápis malých grup)

$$\Rightarrow \quad (13) \cdot H = \{(13), \underset{(13)\circ(12)}{\underset{\shortparallel}{(123)}}\}, \quad H \cdot (13) = \{(13), (132)\}$$

- NAOPAK $g \cdot H = H \cdot g$ VŽDY PRO G KOMUTATIVNÍ
- ALE TO NENÍ NUTNÉ, NAPŘ. $\pi \cdot A_n = A_n \pi \quad \forall \pi \in S_n$.

- DEF: G GRUPA. PODGRUPA $H \leq G$ JE NORMÁLNÍ, POKUD $g \cdot H = H \cdot g \quad \forall g \in G$.

- T (SKRIPTA, T18.7) $H \leq G$.
H JE NORMÁLNÍ $\iff (\forall h \in H)(\forall a \in G)(a h a^{-1} \in H)$

- Dk: $\Rightarrow$
  - BUĎ $h \in H$, $a \in G$
  - PAK $a \cdot h \in aH = Ha$
  - TJ. $a \cdot h = h_1 \cdot a$ PRO NĚJAKÉ $h_1 \in H$
  - JINÝMI SLOVY $a h a^{-1} = h_1 \in H$.

$\Leftarrow$:
  - BUĎ $ah \in aH$
  - PAK $ah = \underbrace{(a \cdot h \cdot a^{-1})}_{\in H} \cdot a \in Ha$
  - TJ. $aH \subseteq Ha$ A SYMETRICKY $H \cdot a \subseteq aH$

- NORMÁLNÍ GRUPY BUDOU NESMÍRNĚ DŮLEŽITÉ U FAKTORGRUP, TEĎ JE ALE NA CHVÍLI OPUSTÍME

– HOMOMORFISMY GRUP

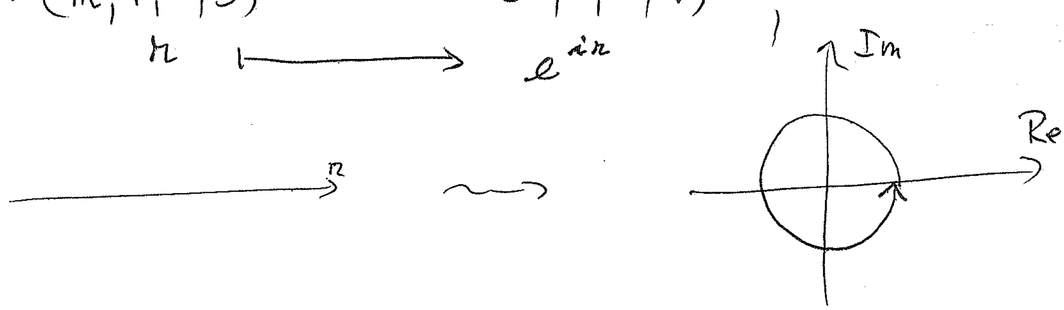
– MYŠLENKA: OBECNĚJŠÍ NEŽ ISOMORFISMUS, CHCEME POROVNÁVAT I RŮZNÉ GRUPY, NEMUSÍ BÝT BIJEKCE.

– DEF: BUĎ $(G, \cdot, ^{-1}, 1)$ A $(H, *, ', e)$ GRUPY.
HOMOMORFISMUS JE ZOBRAZENÍ $f: G \to H$ ZACHOVÁVAJÍCÍ OPERACE, TJ.:

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

– PODOBNĚ LZE DEFINOVAT NAPŘ. HOMOMORFISMUS OKRUHŮ, TĚLES, ...

– PŘ:
- $\exp: (\mathbb{R}, +, -, 0) \longrightarrow (\mathbb{C}^*, \cdot, ^{-1}, 1)$
  $r \longmapsto e^{ir}$



- T TĚLESO : $\det: GL_n(T) \longrightarrow T^*$

- $n \geq 1$: $\operatorname{sgn}: S_n \longrightarrow \mathbb{Z}^* \; (= \{\pm 1\})$

– KRITÉRIUM PRO HOMOMORFISMUS (SPECIÁLNÍ PRO GRUPY !!!)

– L 3.1: G, H ~~grupy~~ GRUPY, $f: G \to H$ ZOBRAZENÍ.
PAK f JE HOMOMORFISMUS $\iff f(a \cdot b) = f(a) * f(b) \; \forall a, b$

– DK: $\Rightarrow$: JASNÉ
$\Leftarrow$:
- $\cancel{f(1)} * e = f(1) = f(1 \cdot 1) = \cancel{f(1)} * f(1)$
  $\Rightarrow e = f(1)$

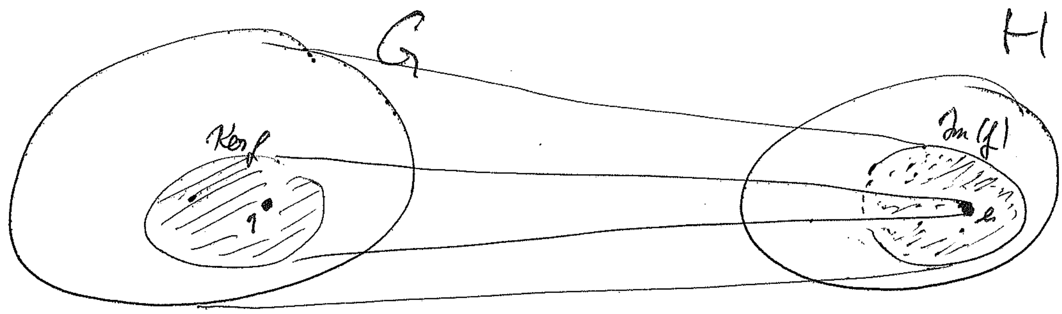
- $e = f(1) = f(a \cdot a^{-1}) = f(a) * f(a^{-1})$
  $\xRightarrow{\text{(JEDNOZAČNOST INVERZE)}} f(a^{-1}) = f(a)'$

- T3.2: G, H GRUPY, $f: G \to H$ ~~VNOŘENÍ~~ HOMOMORFISMUS.

(1) $Im(f) = \{ f(g) \mid g \in G \} \leq H$
(OBRAZ f)

(2) $Ker(f) = \{ g \in G \mid f(g) = e \} \leq G$ NORMÁLNÍ
(JÁDRO f)

(3) f PROSTÝ $\Leftrightarrow$ $Ker(f) = \{1\}$.



- Dk: (1) $e = f(1) \in Im(f)$

$f(a), f(b) \in Im(f) \Rightarrow f(a) * f(b) = f(a \cdot b) \in Im\, f$

$f(a)' = f(a^{-1}) \in Im\, f$

(2) $k \in Ker(f)$, $a \in G$

$\Rightarrow f(aka^{-1}) = f(a) * e * f(a)' = f(a) * f(a)' = e$

$\Rightarrow aka^{-1} \in Ker(f)$

(3) $\Rightarrow$: JASNÉ

$\Leftarrow$: - ŘEKNĚME, ŽE $f(a) = f(b)$

- TJ. $f(ab^{-1}) = f(a) * f(b)' = e$

$\Rightarrow ab^{-1} \in Ker(f)$

$\Rightarrow ab^{-1} = 1$

$\Rightarrow a = b$

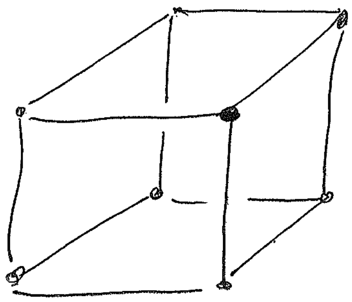
- T3.3: G, H, K GRUPY, $f_1: G \to H$, $f_2: H \to K$ HOMOMORFISMY

(1) $f_2 \circ f_1 : G \to K$ HOMOMORFISMUS

(2) JE-LI f_1 BIJEKCE, JE I $f_1^{-1}: H \to G$ HOMOMORFISMUS

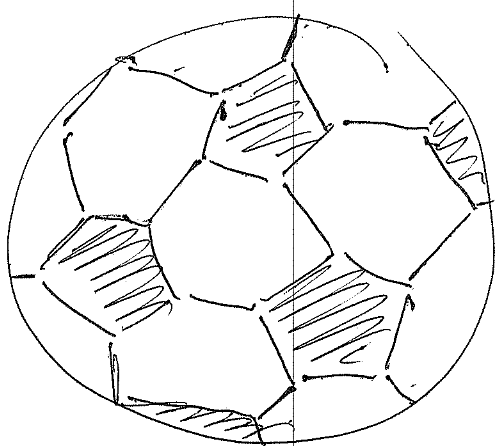
– ISOMORFISMY A NEISOMORFISMY

– PŘ 1: SYMETRIE KRYCHLE V $\mathbb{R}^3$



$$G \cong S_4$$
$$G \leq \mathrm{Iso}(\mathbb{R}^3)$$

– PŘ 2: SYMETRIE FOTBALOVÉHO MÍČE V $\mathbb{R}^3$



$$G \cong A_5$$
$$G \leq \mathrm{Iso}(\mathbb{R}^3)$$

– TABULKA MALÝCH GRUP AŽ NA ISO

$\lvert G \rvert$	G
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2\times\mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_2\times\mathbb{Z}_4$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, D_8, Q

(!) $\mathbb{Z}_6 \cong \mathbb{Z}_2\times\mathbb{Z}_3$, ČV

KVATERNIONY

$Q = \{\pm 1, \pm i, \pm j, \pm k$
$\subseteq (\mathbb{H}^*, \cdot, {}^{-1}, 0)$

CAYLEYOVA REPREZENTACE

- V (SKRIPTA, V 14.7)

KAŽDÁ GRUPA G JE ISOMORFNÍ ~~PERMU~~ PODGRUPĚ PERMUTAČNÍ GRUPY

- Dk: - ZKONSTRUUJEME PROSTÝ HOMOMORFISMUS

$$\lambda : G \longrightarrow S(G)$$

$$\Big((G, \cdot, {}^{-1}, 1) \longrightarrow (S(G), \circ, {}^{-1}, id_G) \Big)$$

- KONKRÉTNĚ $\quad \lambda(g) : G \longrightarrow G$

$$a \longmapsto g \cdot a$$

(TZV. LEVÁ TRANSLACE)

- $\lambda(g)$ JE BIJEKCE, PROTOŽE $\lambda(g^{-1})$ JE INVERZ:

$$\lambda(g) \circ \lambda(g^{-1})\,(a) = g\,(g^{-1} \cdot a) = a$$

$$\lambda(g^{-1}) \circ \lambda(g)\,(a) = g^{-1}(g \cdot a) = a$$

- λ JE HOMOMORFISMUS, PROTOŽE

$$\lambda(g \cdot h)\,(a) = (g \cdot h \cdot a) = g \cdot (h \cdot a) =$$

$$\lambda(g)\,(h \cdot a) = \lambda(g)\,\big(\lambda(h)\,(a)\big) =$$

$$= \big(\lambda(g) \circ \lambda(h)\big)\,(a), \quad \text{TJ.}$$

$$\boxed{\lambda(g \cdot h) = \lambda(g) \circ \lambda(h)}$$

- $Ker(\lambda) = 1$, PROTOŽE

$$\lambda(g) = id_G \implies \lambda(g)\,(1) = 1$$

$$\implies g \cdot 1 = 1$$

$$\implies g = 1$$