$(S_3, \circ) \cong (D_6, \circ)$

G! $H = \{id, (1,2)\}$

$S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$\sigma \sim_H \tau :\Leftrightarrow \tau^{-1} \circ \sigma \in H$

Z: $(1,3) \not\sim_H (2,3) \Leftrightarrow (2,3)^{-1} \circ (1,3) = (2,3) \circ (1,3) = (1,2,3) \notin H$

S_3/H (Levý rozklad S_3 podle H)

id	$(1,3)$	$(2,3)$
$(1,2)$	$(1,2,3)$	$(1,3,2)$

$(1,3) \circ (1,2) = (1,2,3)$

$(2,3) \circ (1,2) = (1,3,2)$

3 13-16:00

$H \backslash S_3$ $H = \{id, (1,2)\}$

id	~~$(1,3)$~~	~~$(2,3)$~~
$(1,2)$	~~$(1,2,3)$~~	~~$(1,3,2)$~~

$(1,2) \circ (1,3) = (1,3,2)$

id	$(1,3)$	$(1,3,2)$
$(1,2)$	$(1,2,3)$	$(2,3)$

3 13-16:09

$a \in a \cdot H \cap H \cdot a$

$a \cdot H = H \cdot a$, dk: $\forall h \in H : a h \in Ha$

tj. $\forall h \in H : \exists h' \in H : a \cdot h = h' \cdot a \mid \cdot a^{-1}$

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

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

cvič 3 $G/H \to H\backslash G$

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

$b \cdot H \mapsto H \cdot b^{-1}$

$b^{-1} \mid a \cdot H = b \cdot H \overset{2)}{\Rightarrow} H \cdot a^{-1} = H \cdot b^{-1} \mid \cdot a$

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

Nelze $a \cdot H \mapsto Ha$, neboť

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

Je to surjekce, injekce $\Rightarrow$ bijekce

3 13-16:22

ad S. řády prvků $n \mid 6$, $|6| = p$:

řády 1, p, ..., p ($p-1$ generátorů)

$\Rightarrow G \cong (\mathbb{Z}_p, +)$

$g \mapsto [1]_p$

3 13-16:33

Rozklady podle podgrup | Normální podgrupy | Okruhy a tělesa | Dělitelnost a nerozložitelnost

Snadnými důsledky předchozího jsou následující věty:

Věta (Malá Fermatova)

Pro libovolné prvočíslo p a číslo $a \in \mathbb{Z}$ nedělitelné p platí

$a^{p-1} \equiv 1 \pmod{p}$. $(\mathbb{Z}_p^\times, \cdot)$

Věta (Eulerova)

Pro libovolné $m \in \mathbb{N}$ a každé $a \in \mathbb{Z}$ splňující $(a, m) = 1$ platí

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

$\mathbb{Z}_m^\times = \{a \in \mathbb{Z}; 1 \le a \le m, (a, m) = 1\}$ $(\mathbb{Z}_m^\times, \cdot)$

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

3 13-16:36

$H = \{id, (1,2)\} \not\lhd S_3$

$A_3 \lhd S_3$

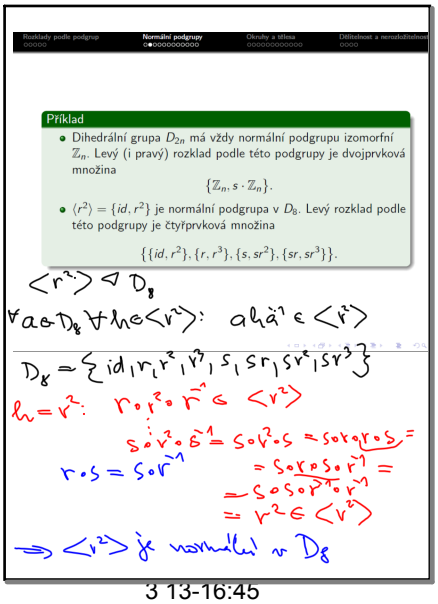
$\{id, (1,2,3), (1,3,2)\}$

S_3/A_3 | $A_3 \backslash S_3$

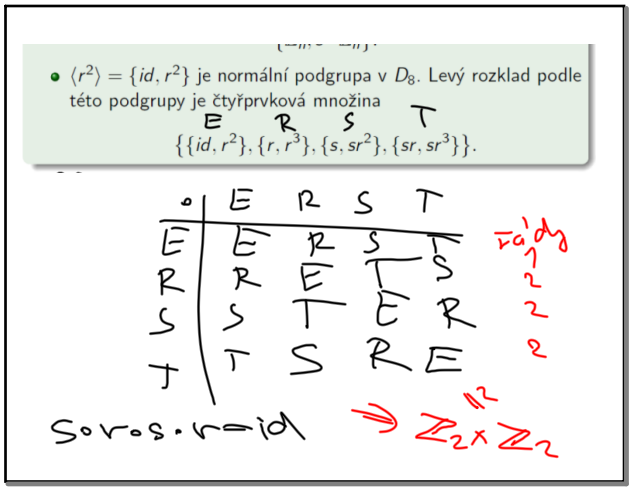
A_3	$\overline{A_3}$
3	3

A_3	$\overline{A_3}$
2	

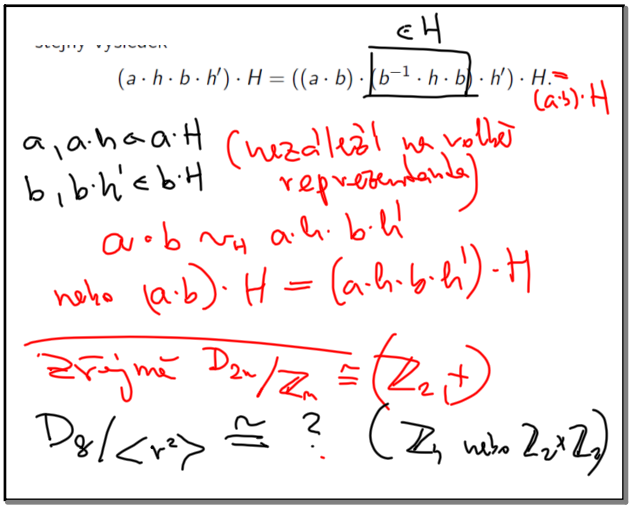
3 13-16:39



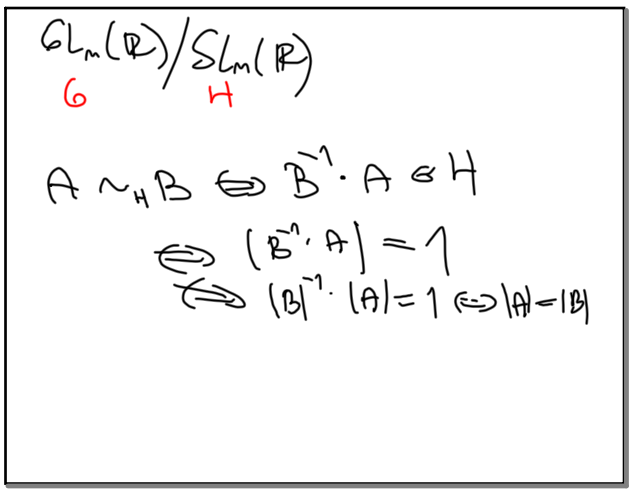
3 13-16:45



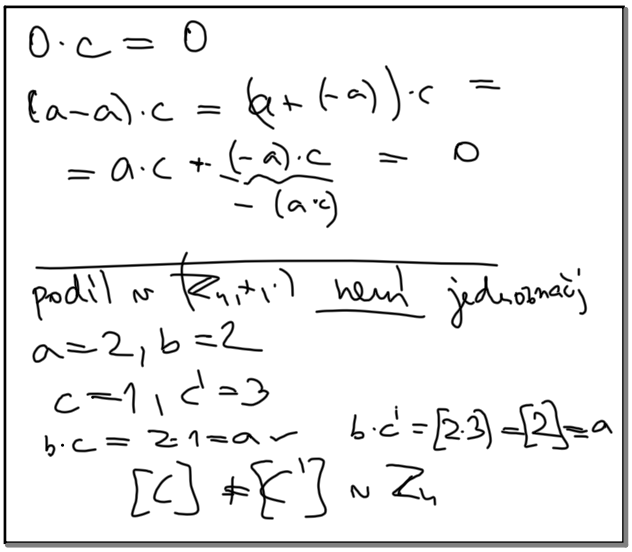
3 13-16:56



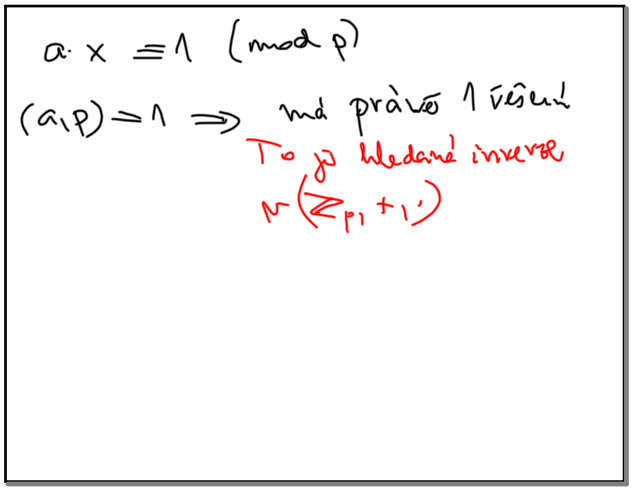
3 13-16:50



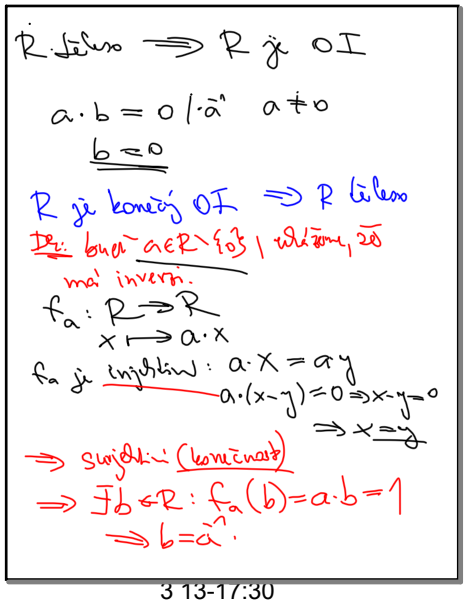
3 13-17:09



3 13-17:19



3 13-17:27


R těleso ⇒ R je OI
a·b = 0 /·a⁻¹ a ≠ 0
b = 0
R je konečný OI ⇒ R těleso
Dk: buď a∈R\{0} | vlastnosti, ZO
má inverzní.
f_a : R → R
x ↦ a·x
f_a je injektivní: a·x = a·y
a·(x−y) = 0 ⇒ x−y = 0
⇒ x = y
⇒ surjektivní (konečnost)
⇒ ∃b∈R : f_a(b) = a·b = 1
⇒ b = a⁻¹.

3 13-17:30