

$(S_3, \circ) \cong (D_6, \circ)$   
 $G = H = \{id, (1,2)\}$   
 $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$   
 $\sigma \sim_H \tau \iff \exists \alpha \in H: \sigma = \alpha \tau$   
 $?(1,3) \not\sim_H (2,3) \iff (2,3)^{-1} \circ (1,3) = (2,3) \circ (1,3) = (1,2,3) \notin H$   
 $S_3/H$  (Lent' vosled  $S_3$  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

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

id	<del>(1,3)</del>	<del>(2,3)</del>
(1,2)	<del>(1,2,3)</del>	<del>(1,3,2)</del>

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

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

3 13-16:09

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

---

$a \in G/H \rightarrow H \cdot a$   
 $a \cdot H \rightarrow H \cdot a^{-1}$   
 $b \cdot H \rightarrow H \cdot b^{-1}$   
 $b \cdot a \cdot H = b \cdot H \cdot a \Rightarrow H \cdot b^{-1} \cdot a^{-1} = H \cdot b^{-1} \cdot a^{-1}$

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

Nelze  $a \cdot H \rightarrow H \cdot a$  nebo  
 $H \cdot a = H \cdot b \iff a \cdot b^{-1} \in H$

Je to surjektiv, injektiv  $\Rightarrow$  bijektiv

3 13-16:22

ad S. Fady prvku  $n \in G, |G| = p$ :  
 Fady  $1, P, P^2, \dots, P^{p-1}$   
 $\Rightarrow G \cong (\mathbb{Z}_p, +)$   
 $g \mapsto [1]_p$

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  
 $a^{p-1} \equiv 1 \pmod{p}$  ( $\mathbb{Z}_p^*$ )

**Věta (Eulerova)**  
 Pro libovolné  $m \in \mathbb{N}$  a každé  $a \in \mathbb{Z}$  splňující  $(a, m) = 1$  platí  
 $a^{\phi(m)} \equiv 1 \pmod{m}$

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}; 1 \leq a \leq m, (a, m) = 1\} = (\mathbb{Z}_m^*, \cdot)$   
 $|\mathbb{Z}_m^*| = \phi(m)$

3 13-16:36

$H = \{id, (1,2)\} \triangleleft S_3$   
 $A_3 \triangleleft S_3$   
 $\{id, (1,2,3), (1,3,2)\}$

$S_3/A_3$

$A_3$	$\bar{A}_3$
3	3

$A_3/S_3$

$A_3$	$\bar{A}_3$
2	3

3 13-16:39

**Příklad**

- Dihedrál ní grupa  $D_{2n}$  má vždy normální podgrupu izomorfní  $Z_n$ . Levý (i pravý) rozklad podle této podgrupy je dvojprvková množina  $\{Z_n, s \cdot Z_n\}$ .
- $\langle r^2 \rangle = \{id, r^2\}$  je normální podgrupa v  $D_8$ . Levý rozklad podle této podgrupy je čtyřprvková množina  $\{id, r^2, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}\}$ .

$\langle r^2 \rangle \triangleleft D_8$   
 $\forall a \in D_8 \forall h \in \langle r^2 \rangle: ah \in \langle r^2 \rangle$

$D_8 = \{id, r, r^2, r^3, s, sr, sr^2, sr^3\}$   
 $h = r^2: r \cdot r^2 = r^3 \in \langle r^2 \rangle$   
 $s \cdot r^2 = s \cdot r^2 = s \cdot r^2 \cdot s = s \cdot r \cdot r \cdot s = s \cdot r \cdot s = r^{-1} = r^3 \in \langle r^2 \rangle$   
 $r \cdot s = s \cdot r^{-1} = s \cdot r^3 = s \cdot r \cdot r^2 = s \cdot r \cdot r^2 = s \cdot r^5 = s \cdot r \cdot r^3 = s \cdot r^4 = r^2 \in \langle r^2 \rangle$   
 $\Rightarrow \langle r^2 \rangle$  je normální v  $D_8$

3 13-16:45

- $\langle r^2 \rangle = \{id, r^2\}$  je normální podgrupa v  $D_8$ . Levý rozklad podle této podgrupy je čtyřprvková množina  $\{E, R, S, T\}$   
 $\{id, r^2, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}\}$ .

	E	R	S	T	
E	E	R	S	T	řádky 1 2 2 2
R	R	E	T	S	
S	S	T	E	R	
T	T	S	R	E	

$s \circ r \circ s \cdot r = id \Rightarrow Z_2 \times Z_2$

3 13-16:56

$(a \cdot h \cdot b \cdot h') \cdot H = ((a \cdot b) \cdot \boxed{b^{-1} \cdot h \cdot b}) \cdot H = (a \cdot b) \cdot H$

$a, a \cdot h \in a \cdot H$   
 $b, b \cdot h' \in b \cdot H$  (nezalží na volbě reprezentantů)  
 $a \cdot b \sim_H a \cdot h \cdot b \cdot h'$   
 nebo  $(a \cdot b) \cdot H = (a \cdot h \cdot b \cdot h') \cdot H$

Zřejmě  $D_{2n}/Z_n \cong (Z_2, +)$   
 $D_8/\langle r^2 \rangle \cong ?$  ( $Z_2$  nebo  $Z_2 \times Z_2$ )

3 13-16:50

$GL_n(\mathbb{R})/SL_n(\mathbb{R})$   
 $G$   $H$

$A \sim_H B \Leftrightarrow B^{-1} \cdot A \in H$   
 $\Leftrightarrow (B^{-1} \cdot A) = 1$   
 $\Leftrightarrow (B^{-1} \cdot A) = 1 \Leftrightarrow |A| = |B|$

3 13-17:09

$0 \cdot c = 0$   
 $(a-a) \cdot c = (a+(-a)) \cdot c =$   
 $= a \cdot c + \underbrace{(-a) \cdot c}_{-(a \cdot c)} = 0$

podíl v  $(Z_{n+1})$  není jednorázový  
 $a=2, b=2$   
 $c=1, c'=3$   
 $b \cdot c = 2 \cdot 1 = a \quad b \cdot c' = [2 \cdot 3] = [2] = a$   
 $[c] \neq [c'] \in Z_n$

3 13-17:19

$a \cdot x \equiv 1 \pmod{p}$   
 $(a, p) = 1 \Rightarrow$  má právě 1 řešení  
 To je hledání inverze  
 $n(Z_{p+1})$

3 13-17:27

$R$  těleso  $\Rightarrow R$  je OI  
 $a \cdot b = 0 \mid a \neq 0$   
 $\underline{b = 0}$   
 $R$  je konečný OI  $\Rightarrow R$  těleso  
Důk: buď  $a \in R \setminus \{0\}$  | ukážeme, že  
ma' invert.  
 $f_a: R \rightarrow R$   
 $x \mapsto a \cdot x$   
 $f_a$  je injektiv:  $a \cdot x = a \cdot y$   
 $a \cdot (x - y) = 0 \Rightarrow x - y = 0$   
 $\Rightarrow x = y$   
 $\Rightarrow$  surjektiv (končnat)  
 $\Rightarrow \exists b \in R: f_a(b) = a \cdot b = 1$   
 $\Rightarrow b = a^{-1}$

3 13-17:30