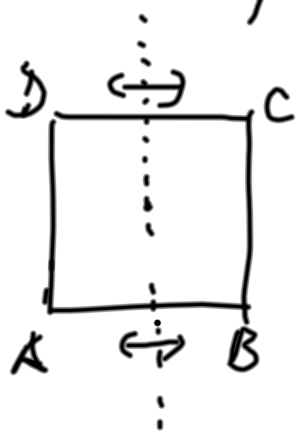
$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

$D_4 \; (D_8) \subset \Sigma_4$



$$[a]_m \mapsto ([a]_{m_1}, \dots, [a]_{m_k})$$

$$[\ ] = [a+b]_m \mapsto ([a+b]_{m_1}, \dots, [a+b]_{m_k})$$

$$[a]_m + [b]_m = \longmapsto ([a]_{m_1} + [b]_{m_1}, \dots, [a]_{m_k} + [b]_{m_k})$$

$$m = m_1 m_2 \cdots m_k$$

$$(m_1, m_2 \dots m_k)$$

3 16-14:13

$m_1 = 3 \qquad a_1 = 2$

$m_2 = 5 \qquad a_2 = 3$

$m_3 = 7 \qquad a_3 = 2$

$140 + 63 + 30 = 233$

$233 \equiv 23 \ (105)$

$(3, \underbrace{5 \cdot 7}_{35}) = 1 \quad , \quad \underbrace{-23 \cdot 3}_{\text{nezajímá}} + \underbrace{2 \cdot 35} = 1$

$2 \cdot 35 \equiv 1 \ (3)$

$140 = 2 \cdot 2 \cdot 35 \equiv 2 \ (3)$

$(5, \underbrace{3 \cdot 7}_{21}) = 1 \quad , \quad 1 \cdot 21 - 4 \cdot 5 = 1$

$21 \equiv 1 \ (5)$

$3 \cdot 21 = 63 \equiv 3 \ (5)$

$(7, 15) = 1 \qquad 1 \cdot 15 - 2 \cdot 7 = 1$

$15 \equiv 1 \ (7)$

$2 \cdot 15 = 30 \equiv 2 \ (7)$

$a \in G \qquad H \subset G$ podgrupa

$$a \cdot H = \{ah \mid h \in H\}$$

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

$$a^{-1} b \in H$$

$$c^{-1} \cdot a = \underbrace{c^{-1} \cdot b}_{\in} \cdot \underbrace{b^{-1} \cdot a}_{\in} \in H$$

$$\underset{\substack{\cup \\ a}}{a \cdot H} = b \cdot H \Rightarrow a = b \cdot h \Leftrightarrow b^{-1} a = h \in H$$

(1) $a \cdot H = Ha \iff \forall h \in H \; a \cdot h \cdot a^{-1} \in H$

„$\Rightarrow$" nechť $aH = Ha$ a $h \in H$ libovolné

$a \cdot h \in aH \Rightarrow \exists h_1 \in H : a \cdot h = h_1 \cdot a \Rightarrow$

$\Rightarrow a \cdot h \cdot a^{-1} = h_1 \in H$

„$\Leftarrow$" nechť $x \in Ha \Rightarrow x = h \cdot a = a \cdot \underbrace{a^{-1} \cdot h \cdot a}_{\in H}$

$\in aH$

---

(1) zobrazení $h \mapsto a \cdot h$ je izomorfismus množin H a aH. (Kdyby $a \cdot h_1 = a h_2 \Rightarrow h_1 = h_2$

3 16-14:43

$$\underbrace{|G|}_{n} = \underbrace{|G/H|}_{\text{počet tříd rozkladu}} \cdot |H|$$

$$\{a, a^1, a^2, \dots, a^k = e\}$$

$(\mathbb{Z}_p^*, \cdot)$

$(\mathbb{Z}_m^*, \cdot)$

④ $$a^n = \left(a^k\right)^{\frac{n}{k}} = (e)^{\frac{n}{k}} = e$$

⑤ nechť $g \in G$ takový, že $g \neq e$

$$\{g, g^2, \dots, g^{r-1}, g^r = e\} = G$$

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

$r \cdot \{id, r^2\} = \{r, r^3\}$

$r^3 \cdot \{id, r^2\} = \{r^3, r\}$

Nechť $aH = cH$, $bH = dH$, pak by mělo $(a \cdot b)H = (c \cdot d)H$

$c \in aH \Rightarrow c = ah$

$d \in bH \Rightarrow d = b \cdot h'$

$(c \cdot d)H = (a \cdot h \cdot b \cdot h')H = \overbrace{\underbrace{}_{\in H}}^{\in H}$

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

Uvažme Σ_3.

Podgrupy Σ_3: $\{id\}$, $\{id, (1,2)\}$, $\{id, (1,3)\}$, $\{id, (2,3)\}$, $\underline{\{id, (1,2,3), (1,3,2)\}}$ A_3 podgrupa sudých permutací.

$$\Sigma_3 / A_3 = \{A_3, \{(1,2), (1,3), (2,3)\}\}$$

$$\cong \mathbb{Z}_2$$

Neplatí že $\mathbb{Z}_2 \times A_3 \not\cong \Sigma_3$

$$\Sigma_3 / \{id, (1,2)\} = \Big\{ \{id, (1,2)\},\ \{(2,3), \underbrace{(2,3)\circ(1,2)}_{(1,3,2)}\},\ \{(1,3), \underbrace{(1,3)\circ(1,2)}_{(1,2,3)}\} \Big\}$$

$$\neq$$

$$\{id,(1,2)\} \backslash \Sigma_3 = \Big\{ \{id, (1,2)\},\ \{(2,3), \underbrace{(1,2)\circ(2,3)}_{(1,2,3)}\}\ \{(1,3), (1,3,2)\} \Big\}$$

Nechť $f: G \to H$ je hom. grupy.
Nechť K je jeho jádro, tzn. všechny $a \in G$ takové, že $f(a) = e$. Nechť $k \in K$ a $g \in G$ libovolné.

Pak
$$f(g^{-1} k g) = f(g^{-1}) \cdot \underbrace{f(k)}_{e} \cdot f(g) = f(g^{-1}) \cdot f(g) =$$
$$= f(g^{-1} \cdot g) = f(e) = e \Rightarrow g^{-1} k g \in K$$

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "p"'] & & K \\
& G/\ker f \arrow[ur, dotted, "\tilde{f}"'] &
\end{tikzcd}
\qquad f = \tilde{f} \cdot p$$

$SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$:

$$\det(G^{-1} \cdot A \cdot G) = \det(G^{-1}) \cdot \underbrace{\det(A)}_{1} \cdot \det(G) =$$

$$= 1$$

$$(GL(n, \mathbb{R}), \cdot) \xrightarrow{\det} (\mathbb{R}^*, \cdot)$$

$\ell = 4$