$$\mathbb{Z}_k \times \mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_{km} \qquad (k,m)=1$$

$f: \mathbb{Z}_{km} \to \mathbb{Z}_k \times \mathbb{Z}_m$

$$[a]_{km} \longmapsto ([a]_k, [a]_m)$$

korektnost: $a \equiv b \pmod{k\cdot m} \Rightarrow \begin{matrix} a \equiv b \,(k) \\ a \equiv b \,(m) \end{matrix}$ ✓

jde o zobrazení

homomorfismus:

$f([a+b]) = f([a]) + f([b])$

$(a+b, a+b) = (a,a) \oplus (b,b)$ def. ✓

bijekce (stejná mohutnost $|\mathbb{Z}_{km}| = |\mathbb{Z}_k \times \mathbb{Z}_m| = k\cdot m$)

$f([a]) = f([b]) \Rightarrow a \equiv b \pmod k, a \equiv b \,(m)$

$\Rightarrow$ stačí injekce $\quad (k,m)=1 \Rightarrow a \equiv b \pmod{k\cdot m} \Rightarrow [a]_{km} = [b]_{km}$ ✓

$a \cdot H = \{a \cdot h ; h \in H\}$

$b \cdot H = \{b \cdot h ; h \in H\}$

$aH \overset{?}{=} bH \iff b^{-1} \cdot a \in H \iff a^{-1} \cdot b \in H$

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

$b^{-1} \cdot a \cdot a^{-1} \cdot b = e$

"$\subseteq$" "$\Leftarrow$"

$b^{-1} \cdot a \in H \Rightarrow \exists h \in H : b^{-1} a = h$

$\Rightarrow a = b \cdot h \in bH$

$\forall h_1 \in H$

$\Rightarrow a \cdot h_1 = b \cdot \underbrace{h \cdot h_1}_{\in H} \in bH \Rightarrow aH \subseteq bH$

symetrie $\Rightarrow bH \subseteq aH$

"$\Rightarrow$" $\forall h_1 \in H \; \exists h_2 \in H$

$a \cdot h_1 = b \cdot h_2 \Rightarrow b^{-1} \cdot a = h_2 \cdot h_1^{-1} \in H$

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

$H = \langle (1,2) \rangle = \{id, (1,2)\}$

$id \circ H = H$

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

$(1,3) \circ H = \{(1,3), (1,2,3)\}$

$(2,3) \circ H = \{(2,3), (1,3,2)\}$

$(1,2,3) \circ H = \{(1,2,3), (1,3)\}$

$(1,3,2) \circ H = \{(1,3,2), (2,3)\}$

$H = id \circ H \mid (1,3) \circ H \mid (2,3) \circ H$

G/H

$H \circ id = H$

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

$H \circ (1,3) = \{(1,3), (1,3,2)\}$

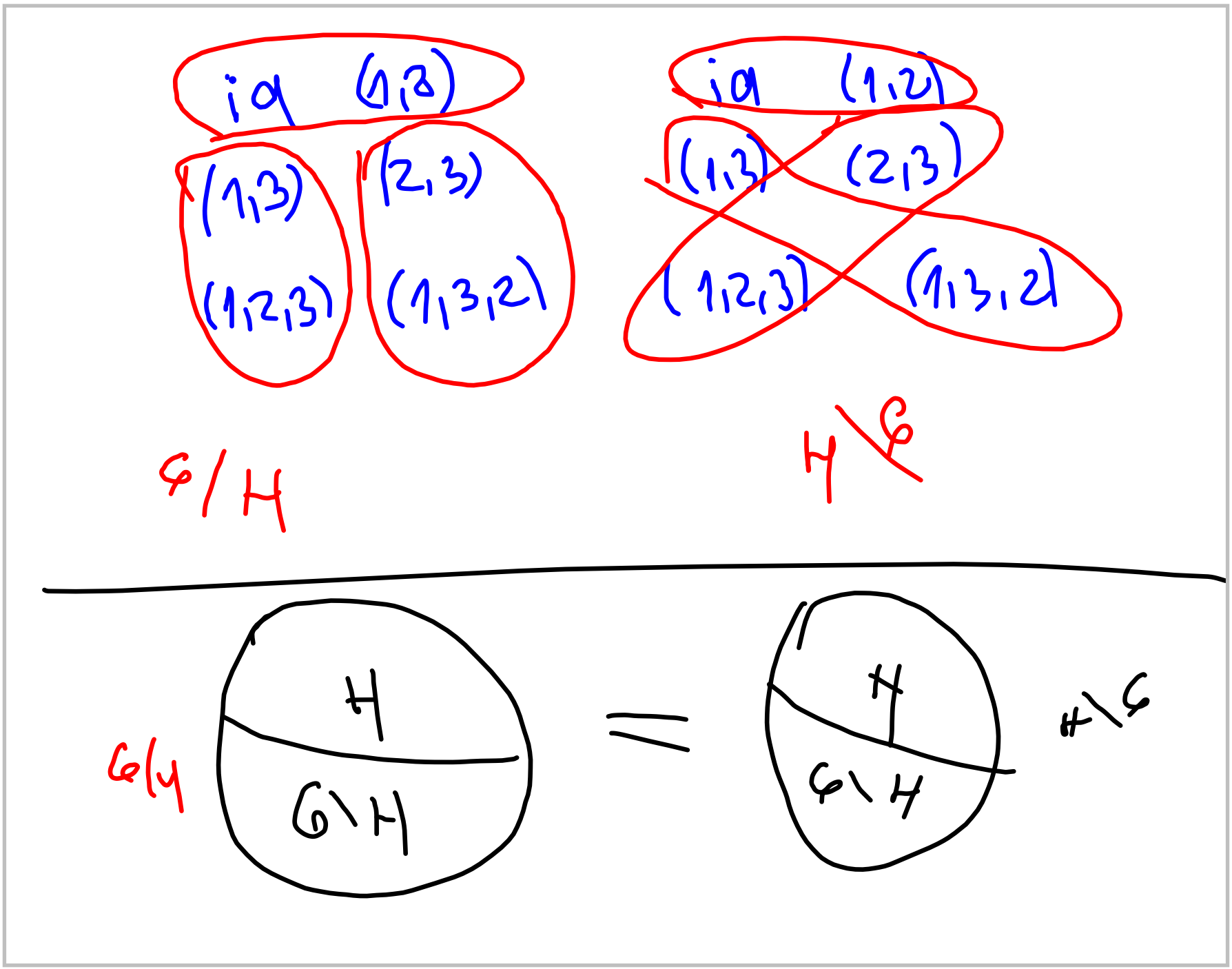
$H \circ (2,3) = \{(2,3), (1,2,3)\}$

$H \circ (1,2,3) = \{(1,2,3), (2,3)\}$

$H \circ (1,3,2) = \{(1,3,2), (1,3)\}$

$H \mid H \circ (1,3) \mid H \circ (2,3)$

$H \backslash G$


id (1,3)
(1,3)
(2,3)
(1,2,3)
(1,3,2)
G/H
id (1,2)
(1,3)
(2,3)
(1,2,3)
(1,3,2)
H\G
G/H
H
G\H
=
H
G\H
#G

Dk: ① $aH = Ha \Leftrightarrow \forall h \in H: aha^{-1} \in H$

$\Rightarrow$" $h \in H$ libl. pak $a \cdot h \in aH = Ha$

$\Rightarrow \exists h_1 \in H: a \cdot h = h_1 \cdot a \quad | \cdot a^{-1}$

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

$\Leftarrow$" $aha^{-1} \in H \Rightarrow \exists h_1 \in H: aha^{-1} = h_1 \quad | \cdot a$

$ah = h_1 a \in Ha$

$\Rightarrow \forall x \in H: ax \in Ha \Rightarrow aH \subseteq Ha$

$Ha \supseteq aH$ analogicky.

② $f_a: H \to aH$

$h \mapsto ah$

surjekce

$c \in aH$ libl.

$\Rightarrow c = ah_1 \quad \exists h_1$

$\Rightarrow h_1 \mapsto c$ ✓

je bijekce injekce: $ah_1 = ah_2 \quad | a^{-1}$

$h_1 = h_2$

③ $\varphi : aH \to Hb^{-1}$

je bijekce?

a) je to zobrazení
b) surjekce
c) injektivita

$Ha = Hb \Leftrightarrow ab^{-1} \in H$

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

$Ha^{-1} = Hb^{-1} \Leftrightarrow a^{-1}(b^{-1})^{-1} \in H \Leftrightarrow a^{-1}b \in H \Leftrightarrow$

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

$\Leftrightarrow aH = bH$

$\Rightarrow$ dokazuji c)

$\Leftarrow$ dokazuji a)

$(\mathbb{Z}_7^\times, \cdot)$ $\quad |\mathbb{Z}_7^\times| = 6$

$[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [1]$

$H = \langle [2] \rangle = \{[1], [2], [4]\} \Rightarrow |H| = 3$

$[2]$ řádu 3

$|G| = p \Rightarrow$ řády prvků 1 | p (pouze e | každý $g \in G$)

$G \to \mathbb{Z}_p$

$g \mapsto [1]_p \to G \cong (\mathbb{Z}_p, +)$

Snadnými důsledky předchozího jsou následující věty:

Věta (Malá Fermatova)

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

$$a^{p-1} \equiv 1 \pmod{p}.$$

Věta (Eulerova)

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

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

$(G/H, \circ)$ je grupa:

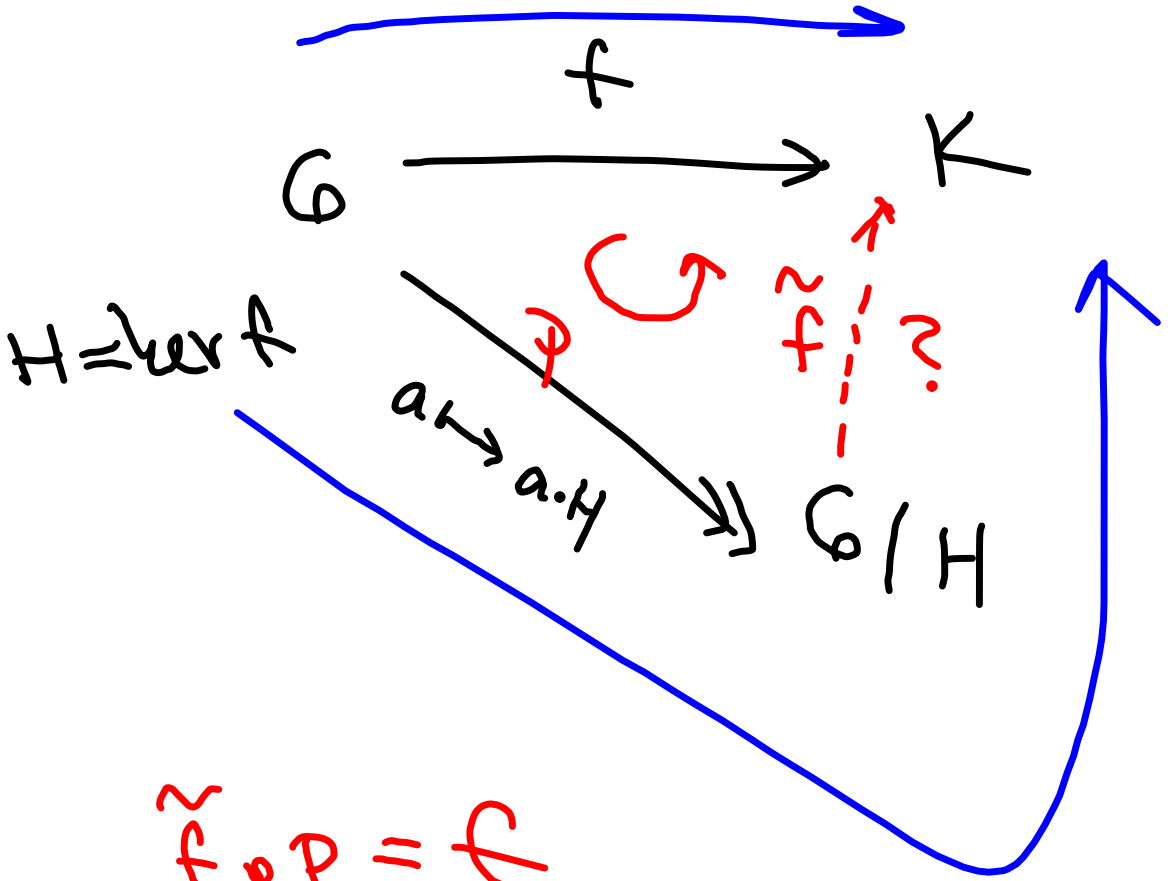
- $\circ$ je bin. operace: $(aH)\circ(bH) \in G/H$

$(aH)\circ(bH) = (a\cdot b)H \circ H$

- asociativní:

$$(aH \circ bH)\circ cH = (a\cdot b)H \circ cH =$$
$$= ((a\cdot b)\cdot c)H \overset{G \text{ asoc.}}{=} (a\cdot(b\cdot c))H =$$
$$= aH \circ (b\cdot c)H = aH \circ (bH \circ cH) \quad \checkmark$$

- neutrální prvek je $H = eH$
- inverzní k aH je $\bar{a}H$: $aH \circ \bar{a}^{-1}H =$
$= (a\cdot\bar{a}^{-1})H = eH = H$ ✓



$\tilde{f} \circ p = f$

$\tilde{f}(a \cdot H) = \tilde{f}(p(a)) = f(a)$

$G \to K$ surjektivní $\Rightarrow G/\ker f \cong K$

Řešení

Postupujme nejprve intuitivně (především je třeba si uvědomit, že zmíněná podgrupa je normální!): dělíme regulární matice řádu n matice do tříd podle toho, jaký dávají (nenulový) determinant. Zdá se tedy, že zmíněnou faktorgrupou by mohla být grupa nenulových reálných čísel $\mathbb{R}^\times$ s operací násobení (díky Cauchyově větě o determinantu součinu matic).

To, že je to skutečně ono, dokážeme pomocí konstrukce surjektivního homomorfismu z $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ do $(\mathbb{R}^\times, \cdot)$, jehož jádrem bude právě $\mathrm{SL}_n(\mathbb{R})$.

Nyní už by mělo být vidět, že přirozenou volbou pro takový homomorfismus je $A \mapsto \det(A)$.