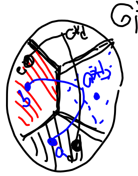


G^* H podgrupa G

$H \leq G$

$a \in G$:

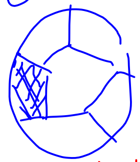
$a * H = \{a \cdot h \mid h \in H\}$

H normální

$\forall g \in G, \forall h \in H: g \cdot h \cdot g^{-1} \in H$

Faktorgrupa podle H

G $\quad H \leq G$



G/H

$a \cdot H = b \cdot H \Leftrightarrow$

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

$a \in b \cdot H$

$a \in a \cdot H$

Hlavní věta o faktorgr

$\varphi: G \to K$, $H \leq G$, $H \subseteq \ker \varphi$

$\Rightarrow \exists! f$ hom. $f: G/H \to K$

takový, že $\varphi = f \circ \pi$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & K \\ G/H \arrow[ur, "f"'] & \end{tikzcd}$$

$\boxed{\pi(a) = a \cdot H}$

- i) f je INJ $\Leftrightarrow$ $H = \ker \varphi$
- ii) f je SUR $\Leftrightarrow$ φ je surj.

G, H

$G \xrightarrow{\varphi} K$

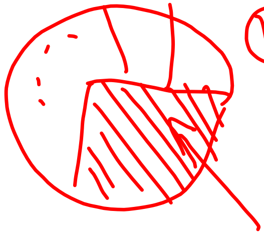
$\ker \varphi = H$,

φ surj

$\boxed{G/H \cong K}$

① $G = \mathbb{C}$

$H = \mathbb{R}$



$a, b \in \mathbb{C}$

$a + \mathbb{R} = b + \mathbb{R} \iff a - b \in \mathbb{R}$

$x_1 - x_2 + i(y_1 - y_2) \in \mathbb{R}$?

$a = x_1 + y_1 i$

$b = x_2 + y_2 i$

$y_1 = y_2$

$$\begin{tikzcd} \mathbb{C} \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & \mathbb{R} \\ & \mathbb{C}/\mathbb{R} \arrow[ur, "f"'] & \end{tikzcd}$$

$\varphi(a+bi) = b$

$\ker \varphi$

$\varphi(a+bi) = 0$

$b = 0$

$\ker \varphi = \mathbb{R}$

$a \in \mathbb{R}$ $\varphi(ai) = a$

$\mathbb{C}/\mathbb{R} \cong \mathbb{R}$

$$|G| = |G/H| \cdot |H|$$

(2) $\mathbb{C}^\times / \mathbb{R}^+$

$a \cdot H = b \cdot H \qquad a, b \in \mathbb{C}^\times$

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

$b = x + iy \quad \Rightarrow \quad \frac{x - iy}{x^2 + y^2} \cdot (\mu + \nu i) \in H$

$b^{-1} = \frac{x - iy}{x^2 + y^2}$

$a = \mu + \nu i$

$(x + iy)^{-1} = \frac{1}{x + iy} = \frac{x - iy}{x^2 + y^2}$

$$\mathbb{C}^\times \xrightarrow{\varphi} \{a + bi \mid a^2 + b^2 = 1\}$$

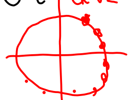
$\mathbb{C}^\times / \mathbb{R}^+$

$$\boxed{\varphi(a+bi) = \frac{a+bi}{\sqrt{a^2+b^2}}}$$

$\varphi(a+bi) = 1$

$\frac{a+bi}{\sqrt{a^2+b^2}} = 1 \Rightarrow b = 0$

$\frac{a}{\sqrt{a^2+b^2}} + i \underbrace{\frac{b}{\sqrt{a^2+b^2}}}_{=0} = 1 + 0i$



$\frac{a}{\sqrt{a^2}} = 1$

$\underbrace{\frac{a}{|a|} = 1}_{a \in \mathbb{R}^+}$

$\operatorname{Ker} \varphi = \mathbb{R}^+$

$a + bi \in K \Rightarrow \frac{a+bi}{\sqrt{a^2+b^2}} = a + bi$

$|a + bi| = 1 \qquad \varphi(a+bi) =$

③ $\mathbb{Z}\times\mathbb{Z}/\{(m,n)\in\mathbb{Z}\times\mathbb{Z} \mid 6 \mid 2m+n\}$

$\boxed{(a,b),(c,d)\in H}$

$6 \mid 2a-b$

$6 \mid 2c-d$

$(a+c,\ b+d)$

$\underbrace{2a+2c-b-d}=\underbrace{(2a-b)}_{6\mid}+\underbrace{(2c-d)}_{6}$

$(a,b)\in H \Rightarrow 6 \mid 2a-b$

$(-a,-b)$ $\quad -2a+b=-(2a-b)$

$\underbrace{(a,b)}+H=\underbrace{(c,d)}+H$

$(c,d)+(-a,-b)\in H$

$(c-a,\ d-b)\in H \Leftrightarrow$

$\underbrace{6 \mid 2c-2a-d+b}$

$$\begin{array}{ccc} \mathbb{Z}\times\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}_6 \\ \downarrow{\scriptstyle \nu} & & \\ \mathbb{Z}\times\mathbb{Z}/H & & \end{array}$$

$\varphi(a,b)=[2a-b]_6$

ověřit homo $\checkmark$

$\ker\varphi$

$\varphi(a,b)=[0]_6$

$[2a-b]_6=[0]_6 \Leftrightarrow$

$6 \mid 2a-b \Rightarrow \underbrace{H=\ker\varphi}$

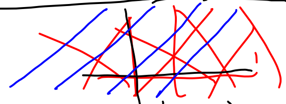
$(0,-1)\mapsto[1]_6$ $\quad [0,-3]\to[3]_6$ $\quad (0,-6)\to[0]_6$.

$(0,-2)\mapsto[2]_6$ $\quad [0,-4]\to[4]_6$

$(0,-5)\to[5]_6$

5) $G = \{ f: \mathbb{R}\to\mathbb{R} \mid f(x)=ax+b;\ a\in\mathbb{R}^*,\ b\in\mathbb{R}\}$

$H = \{f:\mathbb{R}\to\mathbb{R} \mid f(x)=x+b;\ b\in\mathbb{R}\}$



i) $H \le G$

- $f_1(x)=x+b$
- $f_2(x)=x+c$

$(f_1\circ f_2)(x) = f_1(f_2(x)) = f_1(x+c) =$
$= \underbrace{x+c+b}$

$f_1\circ f_2\in H$

$f\in H: f(x)=x+b$ $\quad f^{-1}\in H$

$y=x+b$
$x=y+b$ $\quad \boxed{y=x-b}$

NOR:

- $g\in G,\ h\in H$ $\quad g\circ h\circ g^{-1}$

$g(x)= ax+b$ $\quad g^{-1}: x=ay+b$, $\boxed{y=\frac{x-b}{a}}$

- $h(x)= x+c$

$(g\circ h\circ g^{-1})(x) = g(h(g^{-1}(x))) =$
$g\left(h\left(\frac{x-b}{a}\right)\right) = g\left(\frac{x-b}{a}+c\right) =$
$= \underbrace{x-b+ac+b} \in H$

$g\circ H \overset{=G}{=} g\circ H$

$\boxed{g^{-1}\circ h} \in H$

$g(x)=ax+b$
$g^{-1}(x)= \frac{x-b}{a}$
$h(x)= cx+d$

$g^{-1}(h(x))= g^{-1}(cx+d) =$
$= \frac{cx+d-b}{a} \in H$
$= \boxed{\frac{cx}{a} + \frac{d-b}{a}} \in H$
$\Rightarrow \boxed{c=a}$

$$\begin{tikzcd}
G \arrow[rr] \arrow[dr, "\pi"'] & & \mathbb{R}^\times \\
& G/H \arrow[ur] &
\end{tikzcd}$$

$g(x) = \boxed{a}x + b$

Homo?

$\exists\ \varphi(g) = a$

$\varphi(g) = 1$

$\operatorname{Ker} \varphi = H$

$g(x) = ax$

$\forall a \in \mathbb{R}^\times \quad j\ \boxed{\varphi(g) = a}$

$G = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| \; a, c \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}$

$H = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| \; a, c, b \in \mathbb{Q}, \underline{a, c} > 0 \right\}$

i) Podgrupa

$A \in H, B \in H \Rightarrow A \cdot B \in H$

$A^{-1} \in H$ ✓

ii) Norm.

$\underline{A \in G}, \underline{B \in H}$

$A \cdot B \cdot A^{-1} \in H$?

$A = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{b}{ac} & \frac{1}{c} \end{pmatrix}$

$B = \begin{pmatrix} e & 0 \\ f & g \end{pmatrix} \quad e, g > 0$

$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ f & g \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{a} & 0 \\ \frac{-b}{ac} & \frac{1}{c} \end{pmatrix} =$

$= \begin{pmatrix} ae & 0 \\ be+cf & cg \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{a} & 0 \\ \frac{-b}{ac} & \frac{1}{c} \end{pmatrix} =$

$= \begin{pmatrix} e & 0 \\ \frac{be+cf}{a} - \frac{cgb}{ac} & g \end{pmatrix} \in H$? ✓

iii) G/H

$A \cdot H = B \cdot H \quad A, B \in G$

$B^{-1} \cdot A \in H$

$A = \begin{pmatrix} e & 0 \\ f & g \end{pmatrix}$

$B = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \quad B^{-1} = \begin{pmatrix} \frac{1}{a} & 0 \\ \frac{-b}{ac} & \frac{1}{c} \end{pmatrix}$

$\begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{b}{ac} & \frac{1}{c} \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ f & g \end{pmatrix} =$

$\begin{pmatrix} \frac{e}{a} & 0 \\ \frac{-be}{ac} + \frac{f}{c} & \frac{g}{c} \end{pmatrix} \in H \; \vdots \; \frac{e}{a} > 0, \; \frac{g}{c} > 0$

$$
\begin{tikzcd}
G \arrow[rr] \arrow[dr] & & \mathbb{Z}_2 \times \mathbb{Z}_2 \\
& G/H \arrow[ur] &
\end{tikzcd}
$$

$$
\varphi\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{cases} \boxed{(0,0)} & a,c>0 \\ (0,1) & a>0,\ c<0 \\ (1,0) & a<0,\ c>0 \\ (1,1) & a<0,\ c<0 \end{cases}
$$

φ … homo OVĚŘIT

$$
\ker\varphi = \underbrace{\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G,\ a,c>0 \right\}}_{=H}
$$

Př 2.

1) G

$$H = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax\}$$

$g \in G$

$$g(x) = ax + b \qquad g^{-1}(x) = \frac{x-b}{a}$$

$h \in H$

$$h(x) = cx$$

$$(g \circ h \circ g^{-1})(x) = g(h(g^{-1}(x))) =$$

$$= g\left(h\left(\frac{x-b}{a}\right)\right) =$$

$$= g\left(\frac{cx-cb}{a}\right)$$

$$= cx \underbrace{-cb+b} \notin H$$

$c = 2,\ b = 1$

$G = S_4 = \Sigma_4$

$H = \{\pi \in S_4 \mid \pi(3) = 3\}$

$g \circ \pi \circ g^{-1}$

$g = (1,3,2)$

$g^{-1} = (1,2,3)$

$h = (1,2)$

$g \circ h \circ g^{-1} = (1,3,2) \circ (1,2) \circ (1,2,3) = \underline{(1,3)} \notin H$

4) 5^{6^7} po dělení 12

$(a,m)=1 \Rightarrow$

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

$\varphi(12)=\varphi(2^2\cdot 3)=4$

$(5,12)=1$ $\quad 5^4 \equiv 1\ (12)$

5^{6^7} $\quad \underbrace{(5\cdot 5\cdot \overset{1}{5}\cdot 5)(\dots)\cdot 5\cdot 5\cdot 5}_{6^7}$

$6^7 \equiv \cancel{x}\ (\mathrm{mod}\ 4)$

$2^7 \equiv x\ (\mathrm{mod}\ 4)$

$2^7 \equiv 0\ (4)$

$\boxed{5^{6^7} \equiv 1\ (12)}$

$7^{\overbrace{123456789}}$

$123456789 \equiv x\ (4)$

$x \equiv 1\ (4)$

$7^{123456789} \equiv 7\ (12)$

$17^{444} \equiv x\ (100)$

$\varphi(100)=40$

$17^{40} \equiv 1\ (100)$

$17^{440} \equiv 1\ (100)$

$17^{444} \equiv 17^4\ (100)$

$\equiv 289^2\ (100)$

$\equiv (-11)^2$

$\equiv 121\ (100)$

$\equiv 21\ (100)$