L D: „⇐" ex. $e_H \in H$:

$H \neq \emptyset \Rightarrow \exists a \in H$: z ② ex. $\tilde{a}^{-1} \in H$

① $\Rightarrow a \circ \tilde{a}^{-1} = e_G \in H \Rightarrow e_H = e_G$.

$\forall a,b \in H: a \circ \tilde{b}^{-1} \in H$

① $\forall a,b \in H: a \circ b \in H$

② $\forall a \in H: \tilde{a}^{-1} \in H$

„⇒" zřejmé

„⇐"

- $a = b \Rightarrow e \in H$
- ② $\left.\begin{matrix} a := e \\ b := a \end{matrix}\right\} \Rightarrow e \circ \tilde{a}^{-1} = \tilde{a}^{-1} \in H$
- ③ $\left.\begin{matrix} a := a \\ b := \tilde{b}^{-1} \end{matrix}\right\} \Rightarrow a \circ (\tilde{b}^{-1})^{-1} = a \circ b \in H$ ($\tilde{b}^{-1} \in H$)

Př: $(\mathbb{Z}, +)$ stačí testovat $a - b \in H$

Příklad

1. $\mathbb{Z}$ je podgrupa aditivních grup $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. Všechny podgrupy $(\mathbb{Z}, +)$ jsou vyčerpány množinami $m\mathbb{Z}$.
3. $(R^+, \cdot) \leq (R^*, \cdot)$.
4. Množina A_n všech sudých permutací na n-prvkové množině je podgrupou Σ_n.
5. $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

$m\mathbb{Z} = \{m \cdot z ; z \in \mathbb{Z}\}$, $m \in \mathbb{N}_0$

$* \quad m \cdot z = (z + z + \dots + z)$, multiplikativně

$z^m = (z \cdot z \cdots z)$ (m krát)

a) $m\cdot\mathbb{Z} \leq \mathbb{Z}$ (podgrupa)

$\forall a,b \in m\cdot\mathbb{Z}: a-b \in m\mathbb{Z}$

$a = m\cdot z_1$, $b = m\cdot z_2$ $\Rightarrow a-b = m\cdot(z_1-z_2) \in m\cdot\mathbb{Z}$

$m\cdot\mathbb{Z}$ je podgrupa $\mathbb{Z}$ $\forall m \in \mathbb{N}_0$

b) buď $m = \min\{z \in \mathbb{N};\ z \in H\}$, kde H je podgrupa $\mathbb{Z}$ (existuje vždy, když $H \neq \{0\}$, pro $H = \{0\}$ je $H = 0\cdot\mathbb{Z}$).

Zřejmě pro lib. $z \in \mathbb{Z}$ je $m\cdot z \in H$, tj. $m\cdot\mathbb{Z} \subseteq H$, stačí dokázat, že $H \subseteq m\cdot\mathbb{Z}$. Kdyby $h \in H \setminus m\cdot\mathbb{Z}$, pak vydělíme: $h = \underset{\in H}{m}\cdot\underset{\in H}{q} + r$, kde $0 < r < m$, přitom $r \in H$ SPOR!

$4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z} \leq \mathbb{Z}$

$4\mathbb{Z} \cup 6\mathbb{Z} \not\leq \mathbb{Z}$

$\in$ $4, 6$ $\notin$ $10, 12$

$(\mathbb{Z}_m, +)$ $[a]$ je generátor $\Leftrightarrow$ $(a, m) = 1$

$1 \equiv a \cdot x = \underbrace{(a + a + \dots + a)}_{x}$ (modul)

Bezout: $1 = k \cdot a + l \cdot m \Rightarrow k \cdot a \equiv 1 \; (m)$

generátory $\mathbb{Z}_7^*$

$2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4, 2^6 = 1$

$2^{-1} = 4, 2^{-2} = 2, 2^{-3} = 1$

$\langle [2]_7 \rangle = \{ [1]_7, [2]_7, [4]_7 \}$

$3^1 \equiv 3, 3^2 = 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$

$\langle [3]_7 \rangle = \mathbb{Z}_7^*$

podobně

$\langle [5]_7 \rangle = \mathbb{Z}_7^*$

$(\mathbb{Z}_8^\times, \cdot)$

$\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ $\quad (\cong \mathbb{Z}_2 \times \mathbb{Z}_2)$

$3^1 \equiv 3, 3^2 \equiv 1, \dots$

$5^1 \equiv 5, 5^2 \equiv 1$

$7^1 = 7, 7^2 \equiv 1$

$(\mathbb{Z}_p^\times, \cdot)$ je vždy cyklická

ad 1) $f: G \to H$

$f(e_G) \overset{?}{=} e_H$

$f(e_G \circ e_G) \overset{\text{hom.}}{=} f(e_G) \circ f(e_G)$

$\| e_G$ jedn. G

$f(e_G)$ $\Rightarrow$ $f(e_G) = f(e_G) \circ f(e_G) \quad | \cdot f(e_G)^{-1}$

$e_H = f(e_G) \circ e_H$

$e_H = f(e_G)$

ad 2) $\forall a \in G: f(a^{-1}) \overset{?}{=} f(a)^{-1}$

tj. $f(a^{-1}) \cdot f(a) \overset{?}{=} e_H$, $f(a) \cdot f(a^{-1}) = e_H$ analogicky

$\overset{\text{def.}}{\Longrightarrow}$

$\overset{\text{hom.}}{=}$ $f(a^{-1} \circ a)$

$=$ $f(e_G)$

ad 3) $K \leq G \Rightarrow f(K) \leq H$

$a, b \in f(K)$ lib., chceme $a \cdot b^{-1} \in f(K)$

$\exists k, l \in K: a = f(k)$, $b = f(l)$

$a \cdot b^{-1} = f(k) \cdot f(l)^{-1} \overset{②}{=} f(k) \cdot f(l^{-1}) \overset{\text{hom.}}{=} f(k \circ l^{-1}) \in f(K)$ ✓

$k \leq G$, $k \circ l^{-1} \in K$

adl4 anal.

adl5 $f: G \to H$ hom., bijekce

$\overset{?}{\Rightarrow}$ f^{-1} je homomorfismus

$\forall a,b \in H: f^{-1}(a \cdot b) = f^{-1}(a) \circ f^{-1}(b)$

buď $g = f^{-1}(a)$, $h = f^{-1}(b)$ $\Rightarrow f(g \circ h) = f(g) \cdot f(h)$

$f(f^{-1}(a) \circ f^{-1}(b)) = a \cdot b$ /apl. f^{-1}

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

adl6 $\Rightarrow$ triv.

$\Leftarrow$ obměnou: $\exists a,b \in G, a \neq b: f(a) = f(b)$

f není injekce $\Rightarrow f^{-1}(e_H) \neq \{e_G\}$

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

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

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

$\wedge\ a \cdot b^{-1} \neq e_G$

$\exp: (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$

$\exp(a) = e^a$

$e^{a+b} = e^a \cdot e^b$ $\quad (\exp(a+b) = \exp(a) \cdot \exp(b))$

je to bijekce, tedy izomorfismus

$\exp^{-1} =: \log$

$\log(a \cdot b) = \log(a) + \log(b)$

$$\exp : (\mathbb{C}, +) \to (\mathbb{C} \setminus \{0\}, \cdot)$$

$$e^{a+bi} = z$$

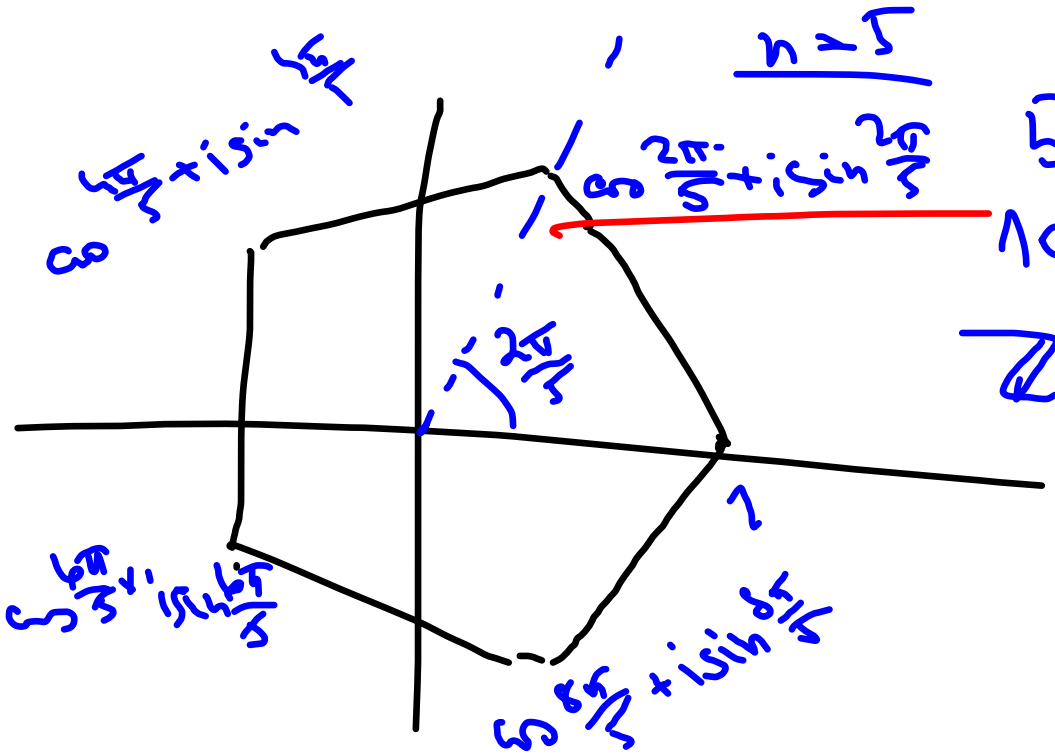
a) $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$

b) $e^{i\pi} = -1$

$$\Rightarrow e^{a+bi} = e^a (\cos b + i \sin b)$$

$$\Rightarrow e^{a+2k\pi i} = 1 \cdot (\cos 2k\pi + i \sin 2k\pi) =$$

$$= 1$$



5 otočení

10 symetrií

$\mathbb{Z}_5 \leq D_{10}$

obecně $\sqrt[k]{1} = \{ \cos \frac{l \cdot 2\pi}{k} + i \sin \frac{l \cdot 2\pi}{k} ;$
$l = 0, \ldots, k-1 \}$