Dk Věty: ⇒ 1) H je uzavřená vůči $\circ$

$(H,\circ)$ (přesněji $(H, \circ|_{H\times H})$) je grupa

$\circ: G\times G \to G$

$\circ|_{H\times H}: H\times H \to G$ (díky 1)) $\to H$

$\circ$ je asociativní na H

· ex. neutrální prvek v H: $\forall a\in H$: $\underbrace{a\circ a^{-1}}_{\boxed{e_G}} \in H$

· $\forall a\in H$ ex. $a^{-1}\in H$ (přímo 2)

„Snadno se vidí": „⇒" zřejmé

„⇐" Nechť $\forall a,b\in H$: $a\circ b^{-1}\in H$, pak $a\circ a^{-1} = e\in H$.

Dosadíme: $a \leftarrow e$, $b\leftarrow a$:

$e\circ a^{-1} = a^{-1}\in H$ (to je ②)

$a\leftarrow a$, $b\leftarrow b^{-1}$

$a\circ (b^{-1})^{-1} = a\circ b \in H$ (to je ①)

$*$ $(b^{-1})^{-1} = c$: $c\circ b^{-1} = e$

$b^{-1}\circ c = e$

lze volit $c = b$.

Pozn: $(a\circ b)^{-1} = b^{-1}\circ a^{-1}$: $(a\circ b)\circ(b^{-1}\circ a^{-1})$

$a\circ \underbrace{(b\circ b^{-1})}_{e}\circ a^{-1}$

$(a\circ e)\circ a^{-1}$

$\underbrace{a\circ a^{-1}}_{e}$

2 27-15:49

① $(\mathbb{Z},+) \le (\mathbb{Q},+) \le (\mathbb{R},+) \le (\mathbb{C},+)$

$(\mathbb{Z},+)$ je podgrupa $(\mathbb{R},+)$ ⇔ $\forall a,b\in\mathbb{Z}$: $a+(-b) = a-b\in\mathbb{Z}$

② $m\cdot\mathbb{Z} = \{m\cdot z;\ z\in\mathbb{Z}\}$; $m\in\mathbb{Z}$

$0\cdot\mathbb{Z} = \{0\} \le \mathbb{Z}$

$1\cdot\mathbb{Z} = \mathbb{Z} \le \mathbb{Z}$

$2\cdot\mathbb{Z} = \{z;\ 2|z\} \le \mathbb{Z}$

a) $m\cdot\mathbb{Z}$ je podgrupa: $\forall a,b\in m\cdot\mathbb{Z}$ chceme $a-b\in m\cdot\mathbb{Z}$

$\exists \alpha,\beta\in\mathbb{Z}$: $\left.\begin{matrix} a = m\cdot\alpha \\ b = m\cdot\beta\end{matrix}\right\} \Rightarrow a-b = m(\alpha-\beta) \in m\cdot\mathbb{Z}$

b) Uvažme podgrupu $H\le\mathbb{Z}$ a položme $m = \min(H\cap\mathbb{N})$, m ex. vždy, když $H\ne\{0\}$

$\mathbb{N}$ je dobře uspořádaná

Dokážeme, že $H = m\cdot\mathbb{Z}$:

a) $m\mathbb{Z}\subseteq H$ zřejmé, neboť H je podgrupa

b) $H\subseteq m\mathbb{Z}$, sporem: kdyby ex. $h\in H\setminus m\cdot\mathbb{Z}$

dělíme se zbytkem: $h = q\cdot m + r$, $0\le r< m$

$h\in H$, $q\cdot m\in m\mathbb{Z}\subseteq H \Rightarrow -q\cdot m\in H \Rightarrow$

$h + (-q\cdot m) = h - qm = r\in H$

$\wedge\ r < m = \min(H\cap\mathbb{N})$

$\Rightarrow r = 0 \Rightarrow h = q\cdot m\in m\cdot\mathbb{Z}$, SPOR

Př: $H = \{-6, -3, 0, 3, 6, 9, 28, \dots\}$, $m=3$

$H\le\mathbb{Z}$: mutně $3\cdot 9 = 27\in H$

$1 = 28-27\in H$

2 27-16:19

③ $(\mathbb{R}^+,\cdot) \le (\mathbb{R}^*,\cdot)$

$\forall a,b\in\mathbb{R}^+ \Rightarrow a\cdot b^{-1}\in\mathbb{R}^+$

$\{1\}\le\mathbb{R}^*$ $\mathbb{R}^*\le\mathbb{R}^*$

$\{-1,1\}\le\mathbb{R}^*$

④ $(A_n,\circ) \le (S_n,\circ)$

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

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

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

$A_3 = \{id, (1,2,3), (1,3,2)\} \cong (\mathbb{Z}_3,+)$

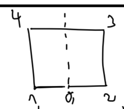
$A_3 \le S_3$

2 27-16:40

4b $|S_4| = 24$

$D_8\le S_4$

dihedrální grupa



r… rotace o 90° v kladném smyslu

$r = (1,2,3,4)$, r^2, r^3

$\sigma_| = (1,2)(3,4)$

$\sigma_- = (1,4)(2,3)$, $\sigma_\backslash = (1,3)$, $\sigma_/ = (2,4)$

$r^4 = id = ()$

$D_8 = \{r, r^2, r^3, r^4 = id, \sigma_-; \sigma_\backslash; \sigma_/; \sigma_|\}$

$s := \sigma_|$

$D_8 = \{id, r, r^2, r^3, s, \underset{\text{sor}^3}{\overset{\sigma_\backslash}{r\circ s}}, \underset{\text{sor}^2}{\overset{\sigma_-}{r^2\circ s}}, \underset{\sigma_/}{r^3\circ s} = r^{-1}\circ s\}$, $\text{sor} = r^3\circ s$

$D_8 = \langle s, r \mid s^2 = id, r^4 = id, rsrs^{-1} = id\rangle$

$r\circ s = s\circ r^3 \mid r$

$r\circ s\circ r = s$

Příklady podgrup D_8:

$\{id\}$, $\{id, s\}$, $\{id, r, r^2, r^3\}$

V_4 = Klein viergroup $= \{(1,3), (2,4), (1,3)(2,4); id\}$ $\cong \mathbb{Z}_2\times\mathbb{Z}_2$

2 27-16:49

⑤ $GL_n(\mathbb{R})$ … general linear group

= matice řádu n nad $\mathbb{R}$, které jsou regulární

$SL_n(\mathbb{R})$ … special linear group

matice řádu n nad $\mathbb{R}$ s $\det = 1$

$A,B\in SL_n(\mathbb{R}) \overset{?}{\Rightarrow} A\cdot B^{-1}\in SL_n(\mathbb{R})$

$\left.\begin{matrix}\det(A) = 1\\ \det(B) = 1\end{matrix}\right\} \overset{?}{\Rightarrow} \det(A\cdot B^{-1}) = 1$

$\det(A)\cdot\det(B)^{-1} = 1$ ✓

2 27-17:04

$(\mathbb{Z}_8,+)$

$\mathbb{Z}_8 = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$

$\langle[3]\rangle = \{3,6,1,4,7,2,5,0\}$

$\langle[5]\rangle = \{5,2,7,4,1,6,3,0\}$

$\langle[7]\rangle = \mathbb{Z}_8$

$[-1]$

2 27-17:13

$R^\times$ ... množina prvků z R mající (multiplikativní) inverzi

$\mathbb{Z}_7^\times = \mathbb{Z}_7 \setminus \{[0]_7\} = \mathbb{Z}_7^*$

$\mathbb{Z}_8^\times \neq \mathbb{Z}_8 \setminus \{0\} = \mathbb{Z}_8^*$

$\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$

$a \in \mathbb{Z}_m^\times \Leftrightarrow (a, m) = 1$

2 27-17:21

$(\mathbb{Z}_7^\times, \cdot) = \langle [3] \rangle$

$\langle 3 \rangle = \{3, 3^2 = 2, \underset{3^3}{[6]} = [-1], \underset{3^4}{4}, 3^5 = 5, 3^6 = 1\}$

$\langle 5 \rangle$ obdobně

$\langle 2 \rangle = \{2, 4, 1\} \subsetneq \mathbb{Z}_7^\times$

$\langle -1 \rangle = \{-1, 1\} \subsetneq \mathbb{Z}_7^\times$

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

$\langle 1 \rangle = \{1\}$ $\langle 5 \rangle = \{5, 1\}$

$\langle 3 \rangle = \{3, 1\}$ $\langle 7 \rangle = \{7, 1\}$

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

2 27-17:24