M .... množina podgrup $(G,\cdot)$

$P := \bigcap_{H \in M} H$ je podgrupa G

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

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

$\Rightarrow a \circ b^{-1} \in P$

sjednocení $S = \bigcup_{H \in M} H$

$\forall a,b \in S, \exists H_1, H_2 \in M \; a \in H_1, b \in H_2$ ~~$a \circ b^{-1} \in S$~~

3 9-13:59

Př.: $2\mathbb{Z} = \{2 \cdot z ; z \in \mathbb{Z}\} \leq (\mathbb{Z},+)$

$3\mathbb{Z} = \{3 \cdot z ; z \in \mathbb{Z}\} \leq (\mathbb{Z},+)$

$2\mathbb{Z} \cap 3\mathbb{Z} = 6\cdot\mathbb{Z} \leq \mathbb{Z}$

$2\mathbb{Z} \cup 3\mathbb{Z} \not\leq \mathbb{Z}$ (např. $2,3 \in S$, $5 \notin S$)

S

3 9-14:11

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

$[1]+[1] = [2], \ldots$

$[a]_8 = \underbrace{[1]+\ldots+[1]}_{a}$ pro lib. $a \in \mathbb{Z}$

Obecně:

$[a]_m$ je v $(\mathbb{Z}_m,+)$ generátor

$\iff (a,m) = 1$

Bezoutova věta: $\exists k,l \in \mathbb{Z}: 1 = k\cdot a + l\cdot m$

$[a]_m + \ldots + [a]_m = [1 - l\cdot m]_m = [1]_m$

$k \cdot a \equiv 1 \pmod m$

3 9-14:19

$\mathbb{Z}_m^\times = \{[a]_m ; (a,m) = 1\}$

$\mathbb{Z}_7^\times = \mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{0\} = \{[1],[2],\ldots,[6]\}$

$(\mathbb{Z}_m^\times,\cdot)$ je grupa (komutativní)

$[a]_m \cdot [b]_m = [a\cdot b]_m$

$[2]_7 \cdot [4]_7 = [8]_7 = [1]_7$

generátory $\mathbb{Z}_7^\times$: ($a^k := \underbrace{a \cdot \ldots \cdot a}_{k}$, $a \in H$; $a^{-k} := \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k}$)

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \; (7)$ ne

$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6 \equiv -1, 3^4 \equiv -3, 3^5 \equiv 5, 3^6 \equiv 1 \; (7)$

Podobně generátor je i $[5]_7$

3 9-14:25

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

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

$\langle 3 \rangle = \{3, 3^2 \equiv 1\}$

$\langle 5 \rangle = \{5, 5^2 \equiv 1\}$

$\langle 7 \rangle = \{7, 7^2 \equiv 1\}$

NENÍ CYKLICKÁ:

$\Downarrow$

$x^2 = 1$ má v $\mathbb{Z}_8$ 4 řešení 1,3,5,7

$(\mathbb{Z}_p^\times,\cdot)$ je cyklická, (p prvočíslo) a má $\varphi(p-1)$ generátorů

3 9-14:32

ad 1) $f: (G,\cdot) \to (H,\circ)$, $e_G \mapsto e_H$

chci: $f(e_G) = e_H$

$f(e_G \cdot e_G) \overset{f \text{ homo}}{=} f(e_G) \circ f(e_G)$

e_G neutrální

$f(e_G)$

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

$e_H = f(e_G)$

3 9-14:35

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

Chci: $f(g^{-1}) \circ f(g) = f(g) \circ f(g^{-1}) = e_H$

$f(g^{-1}) \circ f(g) \overset{\text{hom.}}{=} f(g^{-1} \cdot g) = f(e_G) \overset{(2)}{=} e_H$

$f(g) \circ f(g^{-1}) = f(g \cdot g^{-1}) = f(e_G) = e_H$

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

Buďte $h_1, h_2 \in f(K)$ lib., dokažme, že $h_1 \circ h_2^{-1} \in f(K)$: $\exists k_1, k_2 \in K$:

$f(k_1) = h_1$, $f(k_2) = h_2 \Rightarrow f(k_1) \circ f(k_2)^{-1} =$

$\overset{(2)}{=} f(k_1) \circ f(k_2^{-1}) \overset{\text{hom.}}{=} f(\underbrace{k_1 k_2^{-1}}_{\in K}) \in f(K)$

$\Rightarrow f(K) \leq H$

3 9-14:44

ad 4) analogicky k 3)

ad 5) $f: G \to H$ hom., bijekce (izom.)

$\exists f^{-1}: H \to G$, chci: f^{-1} je hom.

$[f^{-1}(h) = g \Leftrightarrow f(g) = h]$

stačí: $\forall h_1, h_2 \in H$: $f^{-1}(h_1 \circ h_2) = f^{-1}(h_1) \cdot f^{-1}(h_2)$

Nechť $g_1 = f^{-1}(h_1)$, $g_2 = f^{-1}(h_2)$, f je hom. $\Rightarrow$

$f(g_1 \cdot g_2) = f(g_1) \circ f(g_2) = f(f^{-1}(h_1)) \circ f(f^{-1}(h_2))$

$= h_1 \circ h_2$

$\Rightarrow f^{-1}(f(g_1 g_2)) = f^{-1}(h_1 \circ h_2)$

$g_1 \cdot g_2 = f^{-1}(h_1) \cdot f^{-1}(h_2)$ □

3 9-14:50

ad 6) f je injekce $\Leftrightarrow f^{-1}(e_H) = \{e_G\}$

"$\Rightarrow$" triviální

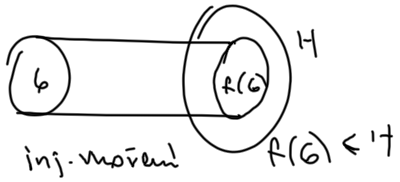
"$\Leftarrow$" sporem: $a, b \in G$, $a \neq b$: $f(a) = f(b)$

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

$f(a \cdot b^{-1})$, přitom když $a \cdot b^{-1} = e_G$

$a = b$ ↯

3 9-14:56



3 9-15:02

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

$x \mapsto e^x$

homo: $\exp(x+y) \overset{?}{=} \exp(x) \cdot \exp(y)$

$e^{x+y} = e^x \cdot e^y$

izomorfismus

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

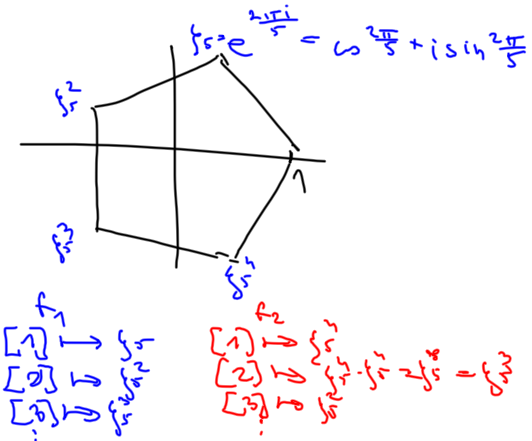
$a, b \in \mathbb{R}^+$: $a \mapsto \ln a$

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

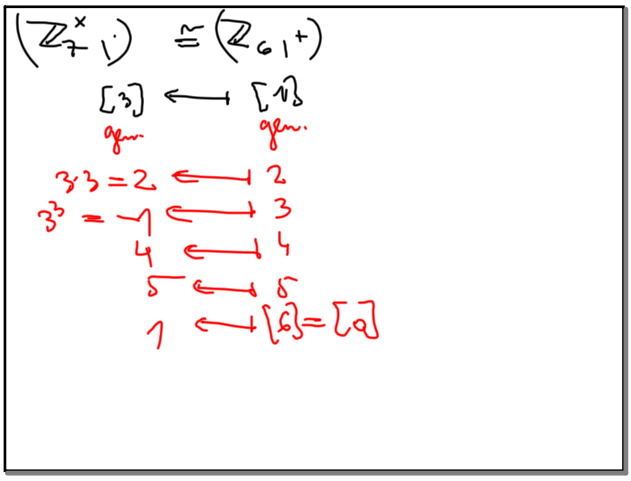
G: $e^{a+bi} = e^a(\cos b + i \sin b) = 1$

$\Leftrightarrow b = 2k\pi$, $a = 0$

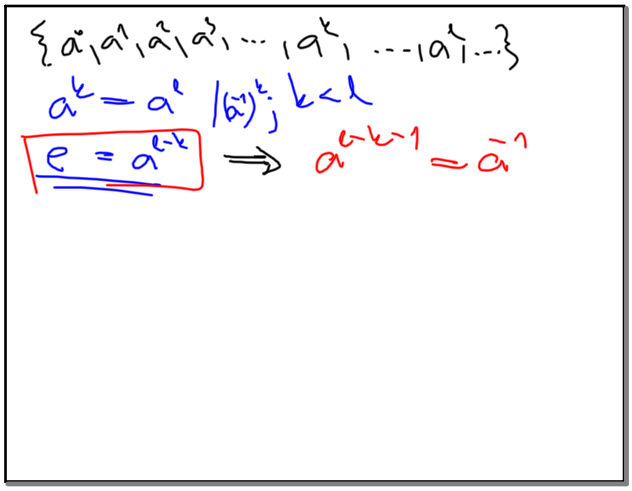
3 9-15:07



3 9-15:14



3 9-15:18



3 9-15:21