$(G,\cdot) \longrightarrow (H,\circ)$

$e_G \in G$, $e_H \in H$

f je hom. $\Rightarrow f(e_G) = e_H$

Dk, že $f(e_G)$ je neutrální prvek:

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

$\| f(e_G) \Rightarrow f(e_G) = f(e_G)\circ f(e_G) \;\big|\; \circ f(e_G)^{-1}$

$\underbrace{f(e_G)\circ f(e_G)^{-1}}_{e_H} = f(e_G)\circ \underbrace{f(e_G)\circ f(e_G)^{-1}}$

$e_H = f(e_G)\circ e_H$

$\underline{\underline{e_H = f(e_G)}}$

3 6-15:55

② obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.

$a \longmapsto f(a) = h$

nutně

$a^{-1} \longmapsto h^{-1}$

Dk, že $f(a^{-1})$ je inverzí $f(a)$.

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

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

3 6-16:09

ad 3 $f: G \to H$

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

Dk, že $f(K)$ je podgrupa: $\underline{h_1, h_2 \in f(K)} \overset{?}{\Rightarrow} h_1\circ h_2^{-1} \in f(K)$

$\exists g_1, g_2 \in K: h_1 = f(g_1), h_2 = f(g_2)$

$h_1\circ h_2^{-1} = f(g_1)\circ f(g_2)^{-1} \overset{(2)}{=}$

$= f(g_1)\circ f(g_2^{-1}) \overset{\text{hom.}}{=} \underbrace{f(\underbrace{g_1\cdot g_2^{-1}}_{\in K})}_{\in f(K)}$

3 6-16:11

ad 5 $f: G \to H$ bijektivní hom.

izomorfismus

$\Rightarrow f^{-1}$ je $\overset{(5)}{—}$ " —

$\boxed{f^{-1}(h) = g \iff f(g) = h}$

f^{-1} je hom.: $\forall h_1, h_2 \in H$:

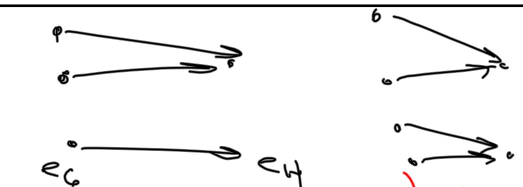
$\underline{f^{-1}(h_1\circ h_2) = \underset{g_1}{f^{-1}(h_1)}\cdot \underset{g_2}{f^{-1}(h_2)}}$

Pak $f(g_1\cdot g_2) = f(g_1)\circ f(g_2) =$

$= h_1\circ h_2$

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

3 6-16:16



obecné zobrazení hom.

ad 6) injektivní $\Rightarrow f^{-1}(\{e_H\}) = \{e_G\}$

„$\Leftarrow$" předp. že f není injektivní, tj.

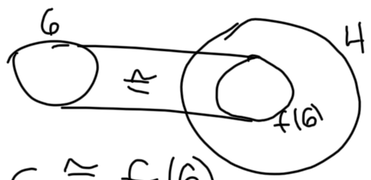
$\exists g_1, g_2 \in G, g_1 \neq g_2: f(g_1) = f(g_2)$

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

$f(g_1\cdot g_2^{-1}) = e_H$,

přičemž $g_1\cdot g_2^{-1} \neq e_G$

3 6-16:21



$G \cong f(G)$

3 6-16:26

$\langle a \rangle \le G$

$\| $

$\{a^0, a^1, a^{-1}, a^2, a^{-2}, \dots\}$

$a^k \cdot a^l = a^{k+l}$, $k,l \in \mathbb{Z}$

G konečná: $\exists k,l$: $k>l$ $a^k = a^l$ $/ \cdot (a^{-1})^l = a^{-l}$

$a^{k-l} = e$

3 6-16:27

$(\mathbb{Z}_8,+)$ generátory $[1]$, nebo $\langle [3] \rangle = \{3,6,1,4,7,2,5,0\}$

$(\mathbb{Z}_m,+)$ generátor $[1]$ nebo lib. $[a]_m$, kde $(a,m)=1$

z Bezoutovy věty $\exists k,l \in \mathbb{Z}$: $a \cdot k + m \cdot l = 1$

modulo: $[a]_m \cdot k = [1]_m$

$\underbrace{[a]+[a]+\dots+[a]}_{k\times} \Rightarrow [a]$ generátor je $(\mathbb{Z}_m,+)$

3 6-16:31

$(\mathbb{Z}_p^*, \cdot)$

Fakt: $\mathbb{Z}_p^*$ je cyklická!

Je těžké generátor nalézt

$(\mathbb{Z}_{41}^\times, \cdot)$ je generováno $[6]$

$(\mathbb{Z}_7^\times, \cdot)$ $[2]$ je řádu 3, $[3]$ je řádu 6

$2^0=1,\ 2^1=2,\ 2^2=4,\ 2^3=1$

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

$3^0=1,\ 3^1=3,\ 3^2=2,\ 3^3=6,\ 3^4=-3,\ 3^5=-2,\ 3^6=1$

3 6-16:35

G konečná, cyklické, $|G|=k$

$\Rightarrow G \cong (\mathbb{Z}_k,+)$

$G = \langle g \rangle$

$f: G \to \mathbb{Z}_k$

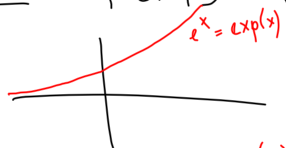
$g \mapsto [1]_k$

G nekonečná, $G = \langle g \rangle$

$G \cong (\mathbb{Z},+)$ $\quad g \mapsto 1$

3 6-16:40

Př 3: $\exp: (\mathbb{R},+) \to (\mathbb{R}^+, \cdot)$



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

$e^{a+b} = e^a \cdot e^b$

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

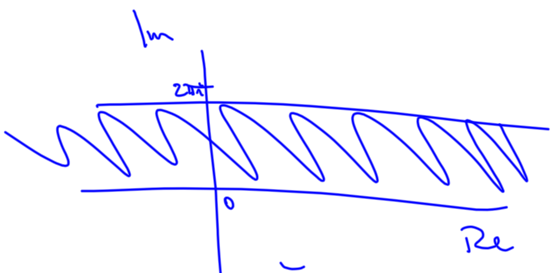
$e^{a+bi} = e^a \cdot (\cos b + i \sin b)$

hom: $e^{(a+bi)+(c+di)} \overset{?}{=} e^a(\cos b + i \sin b) \cdot e^c(\cos d + i \sin d)$

$\| $

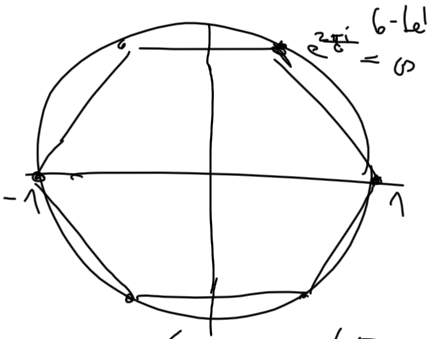
$e^{(a+c)+i(b+d)}$

3 6-16:45



$a+bi$, $b \in \langle 0, 2\pi)$

3 6-16:50



6-té odm. z 1

$e^{\frac{2\pi i}{6}} = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$

homom. $(\mathbb{Z}_k, +) \to (\mathbb{C}_k, \cdot)$

$f_1 : [1]_k \mapsto e^{\frac{2\pi i}{6}}$

$f_5 : [1]_k \mapsto e^{\frac{2\pi i}{6}\cdot 5}$

3 6-16:55

Homomorfismy Součiny Rozklady podle podgrup Normální podgrupy

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f. Označme $m = \prod_i m_i$ a pro libovolné $[a]_m \in \mathbb{Z}_m$ položme $f([a]_m) = ([a]_{m_1}, \ldots, [a]_{m_k})$. Snadno se ověří, že jde o injektivní homomorfismus (co je jádrem?).[2]

homom.

$f([a]+[b]) \overset{?}{=} f([a]) + f([b])$

$f([a+b]) \overset{?}{=} ([a]_{m_1}, \ldots, [a]_{m_k}) + ([b]_1, \ldots, [b]) =$

$= ([a+b]_1, [a+b]_{m_2}, \ldots, [a+b]_{m_k})$

[2] A nešlo by to ještě šikovněji? Pokud nám stačí existence izomorfismu, tak stačí využít toho, že injektivní zobrazení mezi množinami o stejném počtu prvků je automaticky bijekcí.

injektce? $[a] \in \ker f$

$\iff a \equiv 0 \; (m_1)$
$\quad a \equiv 0 \; (m_k)$ $\iff \prod m_i \mid a$

3 6-17:13

Chceme $a \in \mathbb{Z}$: $a \equiv a_1 (m_1), \ldots, a \equiv a_k (m_k)$

$\forall i: \; n_i := \frac{m}{m_i}, \quad m = \prod_{i=1}^{k} m_i$

$(m_i, n_i) = 1$

$\Rightarrow$ Bezout $\Rightarrow \exists \, u_i, v_i \in \mathbb{Z}$:

$u_i \cdot m_i + v_i \cdot n_i = 1$

mod m_i: $\quad v_i \cdot n_i \equiv 1 \; (m_i)$

Pak $a = \sum_{i=1}^{k} a_i v_i n_i$,

totiž

$a \equiv \sum_{j=1}^{k} a_j v_j n_j \equiv a_i v_i n_i \equiv 1 (m_i)$

3 6-16:58

Př: Najdi $a \in \mathbb{Z}$: $a \equiv 12 \; (17)$
$a \equiv 1 \; (5)$
$a \equiv 6 \; (13)$

$m_1 = 17, \; n_1 = 65, \; m_2 = 5, \; n_2 = 221$
$m_3 = 13, \; n_3 = 85$

$i=1$: $(65, 17) = 1$: $65 = 3\cdot 17 + 14$
$17 = 1 \cdot 14 + 3$
$14 = 4 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$

$1 = 3 - 2 = 3 - (14 - 4\cdot 3) = 5\cdot 3 - 14 = 5\cdot(17-14) - 14 =$
$= 5\cdot 17 - 6\cdot 14 = 5\cdot 17 - 6(65 - 3\cdot 17) =$
$= 23\cdot 17 - 6\cdot 65 \Rightarrow v_1 = -6$

$i=2$: $221 \cdot v_2 \equiv 1 \; (5)$
$1 \cdot v_2 \equiv 1 \; (5)$
$v_2 \equiv 1 \; (5)$

$i=3$: $85 \cdot v_3 \equiv 1 \; (13)$
$7 \cdot v_3 \equiv 1 \; (13)$
$7 \cdot v_3 \equiv 14 \; (13)$
$v_3 = 2 \; (13)$

Pak $a = \sum a_i v_i n_i =$
$= 12\cdot(-6)\cdot 65 + 1\cdot 1\cdot 221 + 6\cdot 2\cdot 85$

3 6-17:21

Lze i jinak: $a \equiv 12 \; (17)$
$a \equiv 1 \; (5)$
$a \equiv 6 \; (13)$

$a = 12 + 17k, \; k \in \mathbb{Z}$

Dosadíme: $12 + 17k \equiv 1 \; (5)$
$17k \equiv -11 \; (5)$
$2k \equiv 4 \; (5)$
$k \equiv 2 \; (5)$

$k = 2 + 5l, \; l \in \mathbb{Z}$, dosadit zpět za a:

$a = 12 + 17(2 + 5l) = 46 + 17\cdot 5l$

Dosadíme: $46 + 17\cdot 5l \equiv 6 \; (13)$
$17\cdot 5l \equiv -40 \; (13)$
$\cancel{3}l \equiv -1 \; (13)$
$7l \equiv -14 \; (13) \mid :7$
$l \equiv -2 \; (13)$

$l = -2 + 13t, \; t \in \mathbb{Z}$, dosadíme do výrazu pro a:

$a = 46 + 17\cdot 5(-2 + 13t) =$
$= -124 + 5\cdot 13\cdot 17\cdot t, \; t \in \mathbb{Z}$

Tedy $a \equiv -124 \; (5\cdot 13\cdot 17)$

3 6-17:32